ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ & ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

" Το Πρόβλημα του Διακριτού Λογαρίθμου"

Τριανταφύλλου Σταμάτιος

Εξεταστική Επιτροπή

Α. Παπαϊωάννου, Αναπληρωτής Καθηγητής ΕΜΠ (επιβλέπων)

Χ. Κουκουβίνος, Καθηγητής ΕΜΠ

Π. Στεφανέας, Λέκτορας ΕΜΠ

ΑΘΗΝΑ, 2013

Περιεχόμενα

Κεφάλαιο 1 : *Εισαγωγή στις βασικές αρχές της κρυπτογραφίας*

Κεφάλαιο 2 : *Στοιχεία θεωρίας αριθμών*

Κεφάλαιο 3 : *Το πρόβλημα του διακριτού λογαρίθμου*

Κεφάλαιο 4 : *Βασική θεωρία ελλειπτικών καμπυλών*

Κεφάλαιο 5 : *Ελλειπτικές Καμπύλες πάνω σε Πεπερασμένα Σώματα*

Κεφάλαιο 6 : *Το Πρόβλημα Διακριτού Λογαρίθμου στις Ελλειπτικές Καμπύλες (ECDLP).*

Κεφάλαιο 1:

Εισαγωγή στις βασικές αρχές της κρυπτογραφίας.

1.1 Βασικές έννοιες

Κρυπτολογία:

Η κρυπτολογία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας . Κύριος στόχος είναι να παρέχει μηχανισμούς επικοινωνίας μεταξύ δύο ή περισσότερων μελών χωρίς κάποιος άλλος – ανεπιθύμητος να είναι ικανός να κατανοήσει το περιεχόμενο των μηνυμάτων που ανταλλάσσονται, να υποκλέψει, όπως λέγεται, τις διακινούμενες πληροφορίες. Με άλλα λόγια να κατασκευάζει κρυπτοσυστήματα.

Η κρυπτολογία αποτελείται από δύο ενότητες: την κρυπτογραφία και την κρυπτανάλυση.

Κρυπτογραφία: είναι ο κλάδος που ασχολείται με τους μαθηματικούς μετασχηματισμούς, που είναι απαραίτητοι για την ασφαλή μεταφορά της πληροφορίας.

Κρυπτανάλυση: είναι ο κλάδος που ασχολείται με την ανάλυση και το "σπάσιμο" των κρυπτοσυστημάτων, ώστε να γίνουν κατανοητές οι πληροφορίες που μεταδίδονται.

1.2 Ιστορικά στοιχεία

Ιστορικά η κρυπτογράφηση μηνυμάτων σήμαινε την μετατροπή της πληροφορίας από μια κατανοητή γλώσσα σε ένα γρίφο, για την κατανόηση του οποίου απαιτούνταν κάποιος κρυφός μετασχηματισμός.. Το χαρακτηριστικό των παλιότερων κρυπτοσυστημάτων ήταν η επεξεργασία της γλωσσικής δομής του κειμένου- μηνύματος. Στα νεότερα κρυπτοσυστήματα γίνεται μετατροπή του κειμένου- μηνύματος σε αριθμητικό ισοδύναμο. Το βάρος από κει και πέρα πέφτει σε διάφορα μαθηματικά πεδία, όπως τα διακριτά μαθηματικά, η θεωρία αριθμών, η θεωρία πληροφορίας, η υπολογιστική πολυπλοκότητα, η στατιστική και συνδυαστική ανάλυση, ώστε να είναι αδύνατο, σε πραγματικό χρόνο, να "σπάσει" το κρυπτοσύστημα, και να ανακαλυφθεί τελικά το αρχικό μήνυμα.

Η ιστορία της κρυπτογραφίας ξεκινά από την εποχή των αρχαίων Αιγυπτίων περίπου 4000 χρόνια πριν. Μέχρι και τις αρχές του 20ου αιώνα οι μέθοδοι κρυπτογράφησης και αποκρυπτογράφησης χρησιμοποιούσαν χαρτί, μολύβι και στην καλύτερη περίπτωση απλούς μηχανισμούς κρυπτογράφησης και αποκρυπτογράφησης (κλασσική κρυπτογραφία). Στις αρχές του 20ου αιώνα εφευρέθηκαν πολύπλοκες μηχανές, όπως η μηχανή Enigma και Purple Machine οι οποίες χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο από τους Γερμανούς και τους Ιάπωνες αντίστοιχα. Αργότερα η εμφάνιση των ηλεκτρονικών συστημάτων και των υπολογιστών επέτρεψε την υλοποίηση εξαιρετικά πολύπλοκων κρυπτογραφικών συστημάτων.

Η εξέλιξη της κρυπτογραφίας συμβαδίζει με την εξέλιξη της κρυπτανάλυσης. Η ανακάλυψη και εφαρμογή μεθόδων ανάλυσης της συχνότητας εμφάνισης κάθε χαρακτήρα σε κρυπτοκείμενα, έφερε το "σπάσιμο" των κωδικών και κάποτε ανέτρεψε τη ροή της ιστορίας. Είναι γνωστό ότι η αποκρυπτογάφηση του "τηλεγραφήματος Zimmermann", έφερε την εμπλοκή των ΗΠΑ στον πρώτο παγκόσμιο πόλεμο και η αποκρυπτογράφηση μηνυμάτων των χιτλερικών στρατευμάτων, από τους συμμάχους, έφερε το τέλος του δευτέρου παγκοσμίου πολέμου δυο χρόνια περίπου νωρίτερα

Μέχρι τη δεκαετία του 1970 η κρυπτογραφία ήταν προνόμιο και αποκλειστικότητα των κυβερνήσεων. Από και πέρα δύο πράγματα αλλάζουν τη χρήση της. Πρώτο είναι η δημιουργία ενός ανοικτού προτύπου κρυπτογραφίας (DES) και δεύτερο η εφεύρεση της κρυπτογραφίας "δημοσίου κλειδιού".

1.3 Περιγραφή του μοντέλου κρυπτογράφησης:

Ο αντικειμενικός σκοπός της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω την Alice και τον Bob, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο ανεπιθύμητο πρόσωπο, μη εξουσιοδοτημένο (αντίπαλος), **να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.**

Το σύστημα λειτουργεί με τον ακόλουθο τρόπο:

Α) Ο αποστολέας επιλέγει ένα κλειδί.

Β) Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.

Γ) Δημιουργεί ένα μήνυμα.

Δ) Κρυπτογραφείται το μήνυμα. Με τη συνάρτηση κρυπτογράφησης και δεδομένα το κλειδί και το μήνυμα, παράγεται το κρυπτογραφημένο μήνυμα, δηλαδή μια ακολουθία συμβόλων, ένας γρίφος.

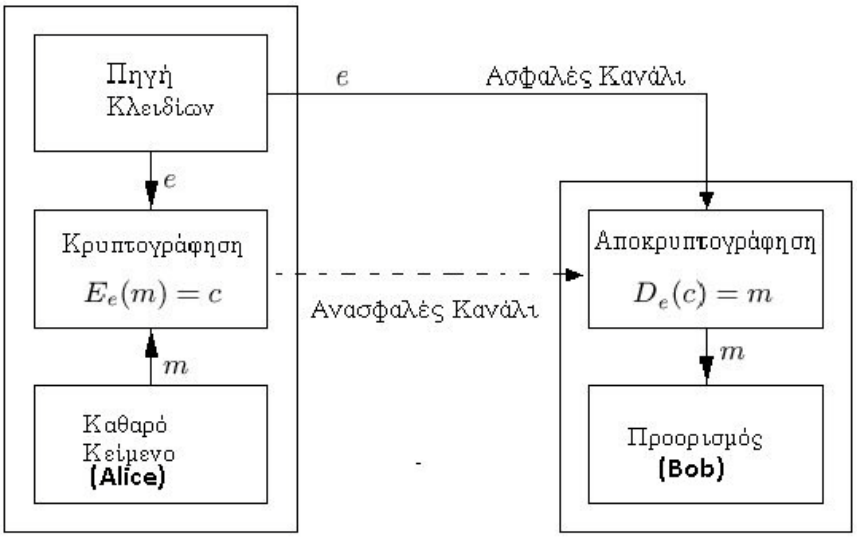
Ε) Το κρυπτογραφημένο μήνυμα αποστέλλεται μέσω ενός μη ασφαλούς καναλιού.

ΣΤ) Ο παραλήπτης με τη συνάρτηση αποκρυπτογράφησης και δεδομένα το κλειδί και το κρυπτογραφημένο μήνυμα, παράγει την ακολουθία του μηνύματος.

Η χρήση των ηλεκτρονικών υπολογιστών μαζί με τις μεθόδους κρυπτανάλυσης έχουν ουσιαστικά αχρηστεύσει την κλασσική κρυπτογραφία, έτσι στο εξής θα ασχοληθούμε με τη μοντέρνα κρυπτογραφία. Η κρυπτογραφία σήμερα διακρίνεται σε κατηγορίες, την συμμετρική και την ασύμμετρη κρυπτογραφία.

1.4 Συμμετρική κρυπτογραφία:

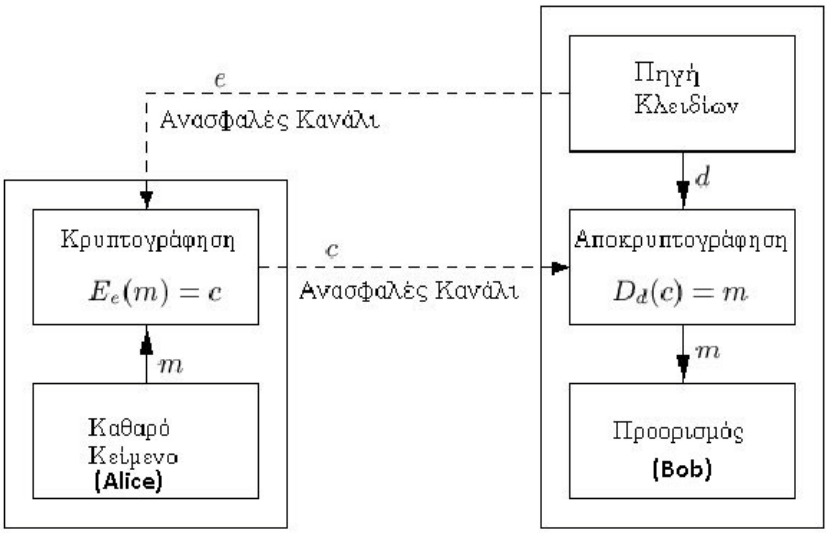
Οι αλγόριθμοι συμμετρικού κλειδιού είναι μια κατηγορία κρυπτογραφικών αλγορίθμων, στους οποίους το κλειδί κρυπτογράφησης σχετίζεται με απλό τρόπο με το κλειδί αποκρυπτογράφησης e. Αυτό σημαίνει είτε ότι τα δύο κλειδιά ταυτίζονται, είτε ότι από το ένα προκύπτει το άλλο με κάποιο απλό μετασχηματισμό.



Σχήμα 1.1
Σχηματική Παράσταση Συμμετρικής Κρυπτογραφίας

1.5 Ασύμμετρη κρυπτογραφία:

Η κρυπτογραφία δημοσίου κλειδιού, είναι μια μορφή κρυπτογραφίας που επιτρέπει στους χρήστες να επικοινωνούν με ασφάλεια χωρίς να έχουν πρότερη κατοχή ενός κοινού μυστικού κλειδιού. Αυτό επιτυγχάνεται με τη χρήση ενός ζεύγους κρυπτογραφικών κλειδιών d, e που αναφέρονται ως δημόσιο και ιδιωτικό κλειδί αντίστοιχα και σχετίζονται με μαθηματικό τρόπο.



Σχήμα 1.2
Σχηματική Παράσταση Ασύμμετρης Κρυπτογραφίας

Η θεμελιώδης μαθηματική ιδέα πίσω από την κρυπτογραφία δημοσίου κλειδιού είναι η αξιοποίηση πολύ δύσκολων μαθηματικών προβλημάτων, όπως είναι το πρόβλημα της **παραγοντοποίησης** και το πρόβλημα του **διακριτού λογαρίθμου**.

Αυτή γίνεται με τη χρήση μίας **"μονόδρομης"** συνάρτησης για τη διαδικασία της κρυπτογράφησης. Το δύσκολο μαθηματικό πρόβλημα έγκειται στη δυσκολία αντιστροφής αυτής της συνάρτησης, η οποία αν είναι σωστά σχεδιασμένος ο αλγόριθμος γίνεται μόνο με την εισαγωγή μίας επιπρόσθετης τεχνικής προϋπόθεσης, ενός μηχανισμού **"καταπακτής"** όπως λέγεται. Τότε το δύσκολο μαθηματικό πρόβλημα θα μπορούσε να χρησιμοποιηθεί για την κατασκευή ενός αλγόριθμου δημοσίου κλειδιού ή ενός αλγόριθμου ψηφιακής υπογραφής.

Ο όρος ασύμμετρη κρυπτογραφία είναι συνώνυμος της κρυπτογραφίας δημοσίου κλειδιού αν και παραπλανητικός. Υπάρχουν αλγόριθμοι ασύμμετροι που δεν χρησιμοποιούν δημόσιο κλειδί. Στην κρυπτογραφία δημοσίου κλειδιού το ιδιωτικό κλειδί διατηρείται μυστικό ενώ το δημόσιο κλειδί κοινοποιείται. Κατά μία έννοια το ένα κλειδί κλειδώνει μία κλειδαριά ενώ το άλλο την ξεκλειδώνει. Πρέπει να είναι εξασφαλισμένο, ότι δεν γίνεται να προκύψει το ιδιωτικό κλειδί ενός ζεύγους

από το δημόσιο αντίστοιχό του. Στους σωστά σχεδιασμένους αλγόριθμους αυτό ισχύει.

Υπάρχουν διάφορες μορφές κρυπτογραφίας δημοσίου κλειδιού:

- Κρυπτογράφηση δημοσίου κλειδιού, δηλαδή διατήρηση ενός μηνύματος μυστικού από οποιονδήποτε δε διαθέτει το κατάλληλο ιδιωτικό κλειδί.
- Ψηφιακή υπογραφή δημοσίου κλειδιού – παροχή δυνατότητας να εξακριβωθεί ότι ένα μήνυμα έχει δημιουργηθεί με ένα συγκεκριμένο ιδιωτικό κλειδί.
- Διαπραγμάτευση κλειδιού- παροχή δυνατότητας σε δύο μέρη, που δεν κατέχουν εκ των προτέρων μυστικό κλειδί να συμφωνήσουν σε κάποιο.
- Τυπικά οι τεχνικές δημοσίου κλειδιού είναι πολύ πιο απαιτητικές σε επεξεργαστική ισχύ από αυτές των συμμετρικών αλγορίθμων αλλά η σωστή χρήση των πρώτων καθιστά εφικτές ένα σύνολο από εφαρμογές.

- **Εξέλιξη:**

Κατά τη διάρκεια σχεδόν όλης της ιστορίας της κρυπτογραφίας το κλειδί έπρεπε να είναι απολύτως απόρρητο και προσυμφωνημένο με ασφαλή και κρυπτογραφικό τρόπο. Λόγω πρακτικών δυσκολιών στη διανομή των κλειδιών με αυτήν τη προσέγγιση επινοήθηκε η κρυπτογραφία δημοσίου κλειδιού. Με την κρυπτογραφία δημοσίου κλειδιού οι χρήστες μπορούν να επικοινωνήσουν ασφαλώς πάνω από ένα μη ασφαλές μέσο, χωρίς να έχουν προσυμφωνήσει για το κλειδί.

Ασύμμετρο κρυπτογράφημα εμφανίστηκε για πρώτη φορά το 1976 από τον Whitfield Diffie και τον Martin Hellmann που κατοχύρωσαν μία μέθοδο για διαπραγμάτευση κλειδιού. Αυτή η μέθοδος ήταν η πρώτη διαπιστωμένη για διαπραγμάτευση κοινού μυστικού κλειδιού πάνω από ένα μη προστατευμένο κανάλι επικοινωνίας.

Το 1977 οι Rivest, Shammir και Adleman από το MIT επινόησαν τον αλγόριθμο που έγινε γνωστός ως RSA. Αυτός χρησιμοποιεί εκθετοποίηση και modular αριθμητική (αριθμητική υπολοίπων διαίρεσης) με το γινόμενο δύο μεγάλων πρώτων αριθμών για την κρυπτογράφηση και αποκρυπτογράφηση παρέχοντας και κρυπτογράφηση δημοσίου κλειδιού και ψηφιακή υπογραφή. Η ασφάλεια του απορρέει από τη δεδομένη δυσκολία παραγοντοποίησης μεγάλων ακεραίων, ένα πρόβλημα για το οποίο δεν υπάρχει αποτελεσματική (γρήγορη) επίλυση.

Από τη δεκαετία του 1970 ένα σύνολο από κρυπτογραφήσεις, ψηφιακές υπογραφές και άλλες τεχνικές αναπτύχθηκαν στο πεδίο της κρυπτογραφίας δημοσίου κλειδιού. Το κρυπτοσύστημα ElGamal επαφίεται στη δυσκολία του προβλήματος του διακριτού λογαρίθμου, το ίδιο και αυτό του DSA. Η εισαγωγή δε των ελλειπτικών καμπύλων από τον Neal Koblitz στα μέσα της δεκαετίας του 1980 προκάλεσε την δημιουργία μιας οικογένειας αντίστοιχων αλγορίθμων δημοσίου κλειδιού. Οι ελλειπτικές καμπύλες παρότι πιο πολύπλοκες παρέχουν

αποτελεσματικότερο τρόπο εκμετάλλευσης του προβλήματος του διακριτού λογαρίθμου, ειδικά σε ότι αφορά τα μεγέθη των κλειδιών για την επίτευξη αντίστοιχων επιπέδων ασφάλειας.

- Ασφάλεια:

Αλγόριθμοι ασύμμετρης κρυπτογραφίας υπάρχουν διάφοροι, είναι δημοφιλείς και μη δημοφιλείς, παραβιασμένοι και απαραβίαστοι, προς το παρόν. Η δημοτικότητα, βέβαια, δε συμβαδίζει με την αξιοπιστία. Έχουν δικλείδες ασφαλείας με διάφορα χαρακτηριστικά και διάφορα επίπεδα δυσκολίας. Η δυσκολία τους αντιστοιχεί στη δυσκολία επίλυσης των δημοφιλών μαθηματικών προβλημάτων, που είναι ακόμη άλυτα, όπως αυτό της εύρεσης διακριτών λογαρίθμων.

- Παραλληλισμός συμμετρικής και ασύμμετρης κρυπτογραφίας:

Ένας παραλληλισμός που μπορεί να φωτίσει τις διαφορές ανάμεσα στη συμμετρική και ασύμμετρη κρυπτογραφία είναι ο παρακάτω. Στο γνωστό σενάριο Alice - Bob η Alice έχει το μυστικό μήνυμα που θέλει να στείλει στον Bob και αυτός να επιστρέψει μια μυστική απάντηση.

Με το συμμετρικό κρυπτοσύστημα η Alice πρώτα βάζει το μυστικό μήνυμα σε ένα κουτί, το οποίο κλειδώνει με ένα λουκέτο για το οποίο φυσικά έχει το κλειδί και έπειτα στέλνει το κουτί στον Bob . Όταν ο Bob παραλάβει το κουτί το ανοίγει με το πανομοιότυπο κλειδί που διαθέτει και διαβάζει το μήνυμα. Στη συνέχεια ο Bob μπορεί να χρησιμοποιήσει το ίδιο λουκέτο για να στείλει την μυστικά απάντηση στην Alice.

Με ένα ασύμμετρο σύστημα ο Bob και η Alice έχουν διαφορετικά λουκέτα και αντίστοιχα κλειδιά ο καθένας μόνο για το λουκέτο του. Πρώτα η Alice ζητάει από τον Bob να της στείλει το λουκέτο του ανοιχτό και χωρίς το κλειδί. Όταν το παραλάβει, κλειδώνει το κουτί μέσα στο οποίο έβαλε το μυστικό μήνυμα και το δικό της λουκέτο ανοιχτό και το στέλνει στον Bob. Ο Bob παραλαμβάνει το κουτί, ανοίγει το λουκέτο, του οποίου έχει το κλειδί και διαβάζει το μυστικό μήνυμα. Στη συνέχεια ο Bob ενεργεί παρόμοια για να απαντήσει.

Συμπέρασμα: Στην ασύμμετρη κρυπτογραφία ο Bob και η Alice για να επικοινωνήσουν δεν χρειάζονται να στείλουν αντίγραφα κλειδιών ο ένας στον άλλο. Αυτό αποτελεί το κυριότερο πλεονέκτημα της ασύμμετρης κρυπτογραφίας. Δεν τίθεται θέμα κλοπής του κλειδιού κατά την μεταφορά και επομένως υποκλοπής των μηνυμάτων. Ακόμα και στην περίπτωση κλοπής του κλειδιού του Bob το μήνυμα της Alice φτάνει με ασφάλεια σε κάθε άλλο παραλήπτη.

- Αλγόριθμοι:

Στους αλγόριθμους ασύμμετρης κρυπτογραφίας συνηθίζεται η Alice και ο Bob να έχουν δύο κλειδιά ο καθένας, ένα για κρυπτογράφηση (το δημόσιο κλειδί) και ένα για αποκρυπτογράφηση (το ιδιωτικό κλειδί). Το κλειδί κρυπτογράφησης μπορεί να δημοσιευτεί, γι' αυτόν το λόγο λέγεται και δημόσιο κλειδί, χωρίς να θυσιάζεται η ασφάλεια των κρυπτογραφημένων μηνυμάτων. Δημοσιεύονται δηλαδή, από τον Bob, οι οδηγίες κατασκευής ενός λουκέτου (δημόσιο κλειδί) χωρίς να δημοσιεύονται ούτε να είναι δυνατό να προκύψει ο τρόπος κατασκευής του κλειδιού που ανοίγει το λουκέτο (ιδιωτικό κλειδί). Αυτοί που θέλουν να επικοινωνήσουν με τον Bob κρυπτογραφούν (κλειδώνουν) το μήνυμά τους με το δημόσιο κλειδί του (λουκέτο) και ο Bob το αποκρυπτογραφεί με το ιδιωτικό του κλειδί.

- Αδυναμίες:

Φυσικά υπάρχει πιθανότητα παραβίασης του λουκέτου. Η ασφάλεια των αλγορίθμων ασύμμετρων κλειδιών βασίζεται σε εκτιμήσεις δυσκολίας που συνεπάγεται το υπόβαθρο μαθηματικό πρόβλημα. Τέτοιες εκτιμήσεις μεταβάλλονται λόγω της σταδιακής αύξησης της επεξεργαστικής ισχύος, είτε λόγω αλγοριθμικών επινοήσεων και μαθηματικών ανακαλύψεων.

Μια άλλη πιθανή αδυναμία, που αφορά το σύστημα δημοσίου κλειδιού είναι η πιθανότητα μιας **επίθεσης μεσολαβητή (man in the middle)**. Σε αυτήν την περίπτωση η ανταλλαγή των δημοσίων κλειδιών αναχαιτίζεται από κάποιον μη φίλιο και μεταβάλλεται με τέτοιο τρόπο που τα δύο μέλη τελικά λαμβάνουν αντί για τα σωστά δημόσια κλειδιά, δύο δημόσια κλειδιά που ανήκουν στο μεσολαβητή. Η κρυπτογραφημένη απόκριση αναχαιτίζεται επίσης, αποκρυπτογραφείται και επανακρυπτογραφείται με το κατάλληλο δημόσιο κλειδί όμως, για να μη κινηθούν υποψίες . Αυτό καθιστά τη μέθοδο δύσκολα υλοποιήσιμη. Η επίθεση όμως δεν είναι αδύνατη και κάποιος μπορεί να την εφαρμόσει . Αυτού του είδους οι επιθέσεις αντιμετωπίζονται καθώς εξελίσσονται οι μηχανισμοί διανομής των κλειδιών, με δυνατότητες πιστοποίησης του αποστολέα και ακεραιότητας του μηνύματος πάνω από μη ασφαλή κανάλια επικοινωνίας .

- **Επεξεργαστικό κόστος:**

Πρέπει να τονιστεί ότι οι περισσότεροι αλγόριθμοι δημοσίου κλειδιού είναι σχετικά απαιτητικοί σε επεξεργαστική ισχύ αν τους συγκρίνουμε με συμμετρικούς αλγόριθμους αντίστοιχης ασφάλειας . Το γεγονός έχει σημαντικές προεκτάσεις σε ότι αφορά την πρακτική τους αξία. Οι περισσότεροι χρησιμοποιούνται σε υβριδικά συστήματα για λόγους αποδοτικότητας . Σε αυτά το μυστικό κλειδί παράγεται από κάποιο μέλος και αυτό κρυπτογραφείται με το δημόσιο κλειδί κάθε παραλήπτη. Κάθε ένας από αυτούς μετά το αποκρυπτογραφεί με το ιδιωτικό κλειδί του . Μόλις όλα τα μέλη αποκτήσουν το μυστικό κλειδί μπορούν να χρησιμοποιήσουν έναν πολύ γρηγορότερο συμμετρικό αλγόριθμο για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων.

1.6 Ψηφιακές υπογραφές:

Η διαδικασία της υπογραφής ενός μηνύματος πιστοποιεί την αυθεντικότητα και την προέλευση του μηνύματος. Πιο συγκεκριμένα οι ψηφιακές υπογραφές χρησιμοποιούνται για να εξασφαλίσουν την πιστοποίηση του αποστολέα , και την ακεραιότητα του μηνύματος .

Λειτουργικά μια ψηφιακή υπογραφή διαφοροποιείται από την κρυπτογράφηση, στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού. Για να υπογραφεί ένα μήνυμα δημιουργείται η σύνοψή του και στη συνέχεια κρυπτογραφείται με χρήση του ιδιωτικού κλειδιού του υπογραφόμενου. Το μήνυμα μαζί με την κρυπτογραφημένη σύνοψη τοποθετούνται μαζί. Ο παραλήπτης θα δημιουργήσει εκ νέου τη σύνοψη και θα αποκρυπτογραφήσει, χρησιμοποιώντας το δημόσιο κλειδί, την κρυπτογραφημένη σύνοψη. Τέλος θα ελεγχθεί η ομοιότητα των δύο συνόψεων.

Μια ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του.

Κεφάλαιο 2:

Στοιχεία θεωρίας αριθμών

Σε αυτό το κεφάλαιο αναφερόμαστε σε στοιχεία της θεωρίας αριθμών τα οποία θα χρησιμεύσουν στο υπόλοιπο της εργασίας.

2.1 Πρώτοι αριθμοί

Θεώρημα

Οι πρώτοι αριθμοί έχουν άπειρο πλήθος.

Θεώρημα (Θεώρημα Πρώτων Αριθμών)

Αν **p(x)** το πλήθος των πρώτων αριθμών που είναι μικρότεροι απο **x**. Τότε **p(x)** $\approx \frac{x}{\ln x}$, με την έννοια ότι ο λόγος **p(x)/(x/ln *x*) → 1** όταν **x**→∞.

Θεώρημα (Θεμελιώδες Θεώρημα της Αριθμητικής)

Για κάθε ακέραιο $n > 1$ υπάρχουν πρώτοι $p_1 \leq p_2 \leq \ldots \leq p_r$ τέτοιοι ώστε p1

$$n = p_1 \cdot p_2 \ldots p_r.$$

Η παραγοντοποίηση αυτή είναι μοναδική.

2.2 Μέγιστος κοινός διαιρέτης

Ορισμός

Ένας ακέραιος **d** ονομάζεται **μέγιστος κοινός διαιρέτης** δύο ακεραίων **a** και **b** και συμβολίζεται ως **ΜΚΔ(a,b)** ή **(a,b)** αν**:**

i. **d> 0**
ii. **d** διαιρεί και τον **a** και τον **b** και
iii. κάθε ακέραιος **f** που είναι κοινός διαιρέτης των **a, b** είναι και διαιρέτης του **d**.

Θα λέμε ότι οι **a** και **b** ειναι **πρώτοι μεταξύ τους** αν **ΜΚΔ(a,b)= 1.**

Θεώρημα (Θεώρημα διαίρεσης του Ευκλείδη)

Για κάθε ζεύγος ακεραίων k με k >0 και j υπάρχουν μοναδικοί ακέραιοι q και r με $0 \le r \le k$ και $j = qk + r$.

Θεώρημα

Αν a, b ακέραιοι όχι και οι δύο μηδέν, τότε ΜΚΔ(a,b) υπάρχει και είναι μοναδικός.

Θεώρημα(Bezout)

Αν a, b ακέραιοι όχι και οι δυο μηδενικοί και d= ΜΚΔ(a,b) τότε υπάρχουν ακέραιοι x, y με ax +by= d.

Θεώρημα

Υπάρχουν ακέραιοι x, y που ικανοποιούν την εξίσωση ax +by= c αν και μόνο αν d= ΜΚΔ(a,b) και d|c.

Αλγόριθμος του Ευκλείδη (Εύρεση ΜΚΔ)

Υποθέτουμε ότι $a \ge b$. Αν δεν ισχύει αυτό αντιμεταθέτω τα a και b. Το πρώτο βήμα είναι να διαιρέσουμε το a με το b και έτσι:

$$\mathbf{a= q_1b +r_1.}$$

Αν $r_1= 0$, τότε b|a και ο ΜΚΔ είναι ο b. Αν $r_1 \neq 0$ τότε συνεχίζουμε αναπαριστώντας τον b στη μορφή: $\mathbf{b= q_2r_1 +r_2}$

Συνεχίζοντας με αυτόν τον τρόπο μέχρι να βρούμε υπόλοιπο **0** έχουμε:

$$\mathbf{r_{1=} q_3r_2 +r_3}$$

. . .

. . .

$$\mathbf{r_{k-2=} q_kr_{k-1} +r_k}$$

$$\mathbf{r_{k-1}= q_{k+1}r_k}$$

Το συμπέρασμα είναι ότι **ΜΚΔ(a,b)= r_k**.

Πολυπλοκότητα χρόνου : $O(\log a \cdot \log b)$

Παράδειγμα

i	1	2	3
r_i	30	5	0
q_i	2	1	6

Άρα ΜΚΔ(a,b) = $r_2 = 5$. □

Επεκταμένος Ευκλείδειος Αλγόριθμος

Έστω a, b ακέραιοι και d=ΜΚΔ(a,b). Από το θεώρημα *Bezout* ξέρουμε ότι υπάρχουν ακέραιοι x, y με ax +by= d. Ο Επεκταμένος Ευκλείδειος Αλγόριθμος μας επιτρέπει να υπολογίσουμε αποδοτικά τους x, y.
Υποθέτουμε ότι ξεκινάμε διαιρώντας τον a με τον b έτσι ώστε b= q_1a +r_1 και συνεχίζουμε όπως στον Ευκλείδειο αλγόριθμο. Έστω ότι τα διαδοχικά πηλίκα είναι $q_1, q_2, \dots, q_n$.
Ορίζουμε τις παρακάτω ακολουθίες:

$$\mathbf{x_0= 0, x_1= 1, x_j = -q_{j-1}x_{j-1} +x_{j-2}}$$

$$\mathbf{y_0= 1, y_1= 0, y_j = -q_{j-1}y_{j-1} +y_{j-2}}$$

Τελικά έχουμε:

$$\mathbf{ax_n +by_n= MK\Delta(a,b)}$$

Παράδειγμα

Έστω a=341, b=527. Κάνοντας τους υπολογισμούς έχουμε:

$$x_0= 0, x_1= 1, x_2= -1, x_3= 2, x_4= -3.$$

Παρομοίως βρίσκουμε $y_4= 2$ και έτσι βλέπουμε ότι

$$ΜΚΔ(341,527)= 31= 2\cdot527 -3\cdot341.$$

Πολυπλοκότητα χρόνου : $O(\log a \cdot \log b)$

2.3 Ισοδυναμίες

Μια απο τις πιο βασικές και χρήσιμες έννοιες στη θεωρία αριθμών είναι οι ισοδυναμίες.

Ορισμός

Έστω a, b, n ακέραιοι με ≠ 0. Λέμε ότι ο a είναι **ισοδύναμος με τον b modulo n** και γράφουμε a≡b (modn) ή a=b (modn) αν η διαφορά a-b είναι ακέραιο πολλαπλάσιο του n. Δηλαδή a -b= kn για κάποιον ακέραιο k.

Παραδείγματα

32= 7 (mod5) , 40= 1 (mod13) , -9= 11 (mod10)

Ιδιότητες

Αν a, b, c, n ακέραιοι με n≠ 0 τότε ισχύουν τα παρακάτω:

1. a= 0 (modn) αν και μόνο αν n|a.
2. a= a (modn). (αυτοπαθής)
3. a= b (modn) αν και μόνο αν b= a (modn). (συμμετρική)
4. Άν a= b (modn) και b= c (modn) τότε και a= c (modn). (μεταβατική)

Η ισοδυναμία, όντας μια σχέση αυτοπαθής, συμμετρική και μεταβατική είναι μία **σχέση ισοδυναμίας.**

Στην πράξη χρησιμοποιούμε συχνά τους ακέραιους mod n, που συμβολίζονται ως $\mathbb{Z}_n$. Αυτοί μπορούν να θεωρηθούν ως το σύνολο {0, 1, 2, ..., n-1} με πρόσθεση, αφαίρεση και πολλαπλασιασμό mod n. Αν ο a είναι ένας ακέραιος, μπορούμε να διαιρέσουμε τον a με n και να πάρουμε το υπόλοιπο που ανήκει στο παραπάνω σύνολο:

a= nq +r με **0≤ r <n**

Έτσι ο a= r (modn), άρα και κάθε ακέραιος a θα είναι ισοδύναμος modn με κάποιο ακέραιο r όπου 0≤ r <n.

Θεώρημα

Έστω a, b, c, d, n ακέραιοι με n≠ 0, και υποθέτουμε ότι a= b modn και c= d modn. Τότε:

$a \pm c = b \pm d \bmod n$ και
$ac = bd \bmod n$.

Θεώρημα

Έστω a, b, c, n ακέραιοι με n≠ 0 και ΜΚΔ(a,n)= 1. Τότε αν ab= ac modn, έπεται ότι b= c modn.

Δηλαδή μπορούμε να διαιρέσουμε και τα δύο μέλη μιας ισοδυναμίας modn με τον ακέραιο a αν και μόνο αν οι a, n είναι πρώτοι μεταξύ τους.

Θεώρημα

Αν ΜΚΔ(a,n)= 1 τότε υπάρχει μοναδικός ακέραιος που συμβολίζουμε με a^{-1} τέτοιος ώστε $aa^{-1} = 1 \bmod n$ και ονομάζεται **αντίστροφος του a (modn).**

Επίλυση της ax= b modn

Παρατηρούμε ότι αν υπάρχει x_0 που ικανοποιεί την ισοδυναμία ax= b modn τότε υπάρχουν άπειρες λύσεις της μορφής $x_0 + kn$ (k ακέραιος) που είναι όμως όλες ισοδύναμες modn. Όντως $a(x_0 + kn) = ax_0 + akn = ax_0 = b \bmod n$

Έστω τώρα ότι ΜΚΔ(a,n)= d.

1η Περίπτωση: Αν **d∤b** τότε η ισοδυναμία δεν έχει λύση**.**

2η Περίπτωση: Αν **d|b** τότε η ισοδυναμία έχει d μη ισοδύναμες λύσεις. Αν x_0 μια λύση τότε βρίσκουμε τις υπόλοιπες από τον τύπο $x = x_0 + t\frac{n}{d}$ με t ακέραιο. Για να βρούμε τις d μη ισοδύναμες λύσεις δίνουμε στο t τις τιμές 0, 1, …, d-1.

Ορισμός

Το σύνολο των ακεραίων $\{r_1, r_2, ..., r_s\}$ ονομάζεται **περιορισμένο σύνολο υπολοίπων modm** αν

i) ΜΚΔ(r_i,m)=1 για κάθε i
ii) $r_i \neq r_j$ για $i \neq j$
iii) Για κάθε ακέραιο n με ΜΚΔ(n,m)=1 αντιστοιχεί r_i : n= r_i modm.

Κινέζικο Θεώρημα Υπολοίπων (ΚΘΥ)

Έστω οι s φυσικοί m_1, m_2, ..., m_s που είναι όλοι πρώτοι προς αλλήλους και M= $m_1 \cdot m_2 \cdots m_s$. Έστω επιπλέον οι s το πλήθος ακέραιοι a_i όπου $1 \leq i \leq s$ με ΜΚΔ(a_i,m_i)= 1 για κάθε i. Τότε το παρακάτω σύστημα ισοδυναμιών έχει μια λύση μοναδική modM:

$a_1x = b_1 \, mod m_1$, $a_2x = b_2 \, mod m_2$, …, $a_sx = b_s \, mod m_s$

Ορισμός

Η **συνάρτηση φ(n) του Euler** μας δίνει το πλήθος των θετικών ακεραίων μικρότερων του n που είναι πρώτοι προς τον n.

Μικρό θεώρημα του Fermat

Έστω p πρώτος και $a \in \mathbb{Z}$, τότε

i) $a^p = a \, mod p$

ii) $a^{p^k} = a \, mod p$

iii) Αν $p \nmid a \Rightarrow a^{p-1} = 1 \, mod p$

Θεώρημα (Euler)

Αν $n \in \mathbb{N}$, $a \in \mathbb{Z}$ τέτοιοι ώστε ΜΚΔ(a,n)= 1, τότε $a^{\varphi(n)} = 1$ modn.

2.4 Πρωταρχικές ρίζες

Ορισμός

Αν h είναι ο μικρότερος θετικός ακέραιος τέτοιος ώστε $a^h=1$ modm τότε λέμε ότι ο a **ανήκει στον εκθέτη h modulo m.**

Αλλιώς λέμε ότι ο a **έχει τάξη h modulo m** .

Θεώρημα

Μια ικανή και αναγκαία συνθήκη για να ισχύει $a^b=1$ modm για κάποιον ακέραιο b είναι η ΜΚΔ(a,m)=1

Θεώρημα

Έστω a έχει τάξη h modulo m και $a^r=1$ modm, τότε h/r.

Ορισμός

Αν ένας ακέραιος g έχει τάξη φ(m) modm τότε ονομάζεται **αρχική ή πρωταρχική ρίζα modm.**

Θεώρημα

Αν ο g είναι πρωταρχική ρίζα modm τότε οι δυνάμεις του g δηλαδή $g,g^2,..,g^{\varphi(m)}$ είναι όλες μη ισοδύναμες modm και αποτελούν ένα περιορισμένο σύνολο υπολοίπων modm.

Θεώρημα

Αν a έχει τάξη h modm και ΜΚΔ(k,h)=d τότε ο a^k έχει τάξη h/d modm.

Θεώρημα

Αν g είναι πρωταρχική ρίζα modm τότε η g^r είναι επίσης μία πρωταρχική ρίζα modm αν και μόνο αν ΜΚΔ(r,φ(m))=1.

Θεώρημα

Αν υπάρχει μία πρωταρχική ρίζα modm τότε το πλήθος των αμοιβαία μη ισοδύναμων πρωταρχικών ριζών είναι φ(φ(m)).

Θεώρημα

Για κάθε πρώτο p, υπάρχουν πρωταρχικές ρίζες modp.

Παρατήρηση

Όταν p πρώτος, μια g πρωταρχική ρίζα modp είναι ένας αριθμός που οι δυνάμεις του g, g^2,…, g^{p-1} είναι όλες μη ισοδύναμες modp και μας δίνουν όλα τα μη μηδενικά υπόλοιπα modp. Δηλαδή η g πρωταρχική ρίζα είναι **γεννήτορας** της πολλαπλασιαστικής ομάδας $\mathbb{Z}_p^*$.

2.5 Υπολογισμός δυνάμεων modm

Μία αποδοτική μέθοδος για τον υπολογισμό μεγάλων δυνάμεων x^n είναι η μέθοδος **“square and multiply”,** εκφράζεται αναδρομικά έτσι:

$$\Delta\acute{\upsilon}\nu\alpha\mu\eta(x,n)=\begin{cases}1, & \alpha\nu\ n=0\\ x\cdot\Delta\acute{\upsilon}\nu\alpha\mu\eta(x,n-1), & \alpha\nu\ n=\pi\varepsilon\rho\iota\tau\tau\acute{o}\varsigma\\ \Delta\acute{\upsilon}\nu\alpha\mu\eta(x,n/2)^2, & \alpha\nu\ n=\acute{\alpha}\rho\tau\iota\circ\varsigma\end{cases}$$

Η πολυπλοκότητα της μεθόδου προφανώς είναι $O(\log n)$ λόγω των διαδοχικών διαιρέσεων με το 2.

Αν θέλουμε να υπολογίσουμε τις δυνάμεις ενός ακεραίου modm σε κάθε βήμα υπολογίζουμε $\Delta\acute{\upsilon}\nu\alpha\mu\eta(x,n) \bmod m$.

Παράδειγμα
Θέλουμε να υπολογίσουμε το 2^5mod3 τότε υπολογίζουμε:

2=2mod3, 2^2=4=1mod3, $\left(2^2\right)^2=2^4$=16=1mod3 άρα

$2^5=2^4\cdot2=1\cdot2$mod3=2mod3.

Κεφάλαιο 3:

Το πρόβλημα του διακριτού λογαρίθμου

3.1 Εισαγωγικές έννοιες και ορισμοί

- **Ορισμός :**

Έστω G πεπερασμένη κυκλική ομάδα τάξης n, g ένας γεννήτορας της G $\left(G = \langle g \rangle\right)$ και b ∈ G. **Διακριτός λογάριθμος** του b στη βάση g (συμβολίζεται $\log_g b$) είναι ο μοναδικός ακέραιος x , $0 \le x \le n-1$, με $g^x = b$.
(χρησιμοποιώ πολλαπλασιαστικό συμβολισμό για την πράξη της ομάδας, αν χρησιμοποιήσουμε προσθετικό συμβολισμό θα έγραφα $b = xg$)

- **Ιδιότητες διακριτού λογαρίθμου**

Έστω G κυκλική πολλαπλασιαστική ομάδα τάξης n, g,g΄ γεννήτορες της G, b,a ∈G, s∈ℤ

i. $\log_{g(}ab) \equiv (\log_g b + \log_g a) \bmod n$
ii. $\log_g(b^s) \equiv s \log_g b \bmod n$
iii. $\log_{g'} b \equiv (\log_g b)(\log_g g')^{-1} \bmod n$

Παρατήρηση:

Η χρησιμότητα του προβλήματος του διακριτού λογαρίθμου, από την άποψη της κρυπτογραφίας έγκειται στο ότι η συνάρτηση $b = g^x$ ανήκει πιθανότατα στην κατηγορία των μονόδρομων συναρτήσεων (one-way function).
Δηλαδή, ενώ είναι αλγοριθμικά εύκολος ο υπολογισμός της τιμής $b = g^x$ σε σχετικά μικρό χρόνο για κάθε x (π.χ. ο αλγόριθμος square and multiply υπολογίζει το α^x σε χρόνο $O(k^2)$, όπου k ο αριθμός των bits του x),ο υπολογισμός της τιμής της αντίστροφης συνάρτησης $x = \log_g b$ σε κατάλληλα[1] επιλεγμένες ομάδες G είναι υπολογιστικά δυσπρόσιτος. Δεν υπάρχει, δηλαδή, μέχρι σήμερα αποδοτικός αλγόριθμος για τον υπολογισμό του x δοθέντων των g,b.

[1] π.χ. αν θέλω να επιλύσω την εξίσωση στο Z_p ,για p πρώτο με τουλάχιστον 150 ψηφία και με το p-1 να έχει τουλάχιστον ένα μεγάλο πρώτο παράγοντα

Οι πιο σημαντικές ομάδες στην κρυπτογραφία είναι οι πολλαπλασιαστικές ομάδες F_q^* του πεπερασμένου σώματος F_q. Ειδική περίπτωση αυτών των ομάδων είναι η πολλαπλασιαστική ομάδα Z_p^* των ακεραίων modulo p (όπου p : πρώτος) η οποία είναι κυκλική ομάδα τάξης p-1.

Πρόβλημα 3.1 : Γενικευμένο Πρόβλημα του διακριτού λογαρίθμου (GDLP)

Δίνονται : πεπερασμένη κυκλική ομάδα G τάξης n, g ένας γεννήτορας της G και $b \in G$.

Ζητείται : Να βρεθεί ακέραιος x , με $0 \leq x \leq n-1$, τέτοιος ώστε $g^x \equiv b \pmod p$.

Μια πιο γενική μορφή του παραπάνω προβλήματος είναι η εξής :

- Με δεδομένα: G πεπερασμένη ομάδα και στοιχεία $g,b \in G$, να βρεθεί ένας ακέραιος x τέτοιος ώστε $g^x=b$, υποθέτοντας ότι ένας τέτοιος ακέραιος υπάρχει.

Σε αυτή την παραλλαγή δεν απαιτείται η G να είναι κυκλική, ακόμη όμως κι αν είναι δεν απαιτείται ο g να είναι γεννήτορας της G.

Στην περίπτωση όπου η G είναι κυκλική, και η τάξη του g είναι γνωστή μπορούμε εύκολα να παρατηρήσουμε εάν ένας τέτοιος ακέραιος x υπάρχει, λόγω της παρακάτω πρότασης:

Πρόταση

Αν G κυκλική ομάδα, g ένα στοιχείο της G τάξης n και $b \in G$, τότε υπάρχει ένας $x \in Z$ τέτοιος ώστε $g^x=b$ αν και μόνο αν $b^n = 1$.

Πρόβλημα 3.2 : Πρόβλημα του διακριτού λογαρίθμου (DLP)

Δίνονται : Ένας πρώτος αριθμός p, ένας γεννήτορας g του Z_p^* και ένα στοιχείο $b \in Z_p^*$

Ζητείται : Να βρεθεί ακέραιος x , με $0 \leq x \leq p-2$, τέτοιος ώστε $g^x \equiv b \pmod p$.

(*Στο εξής η ισοδυναμία $x \equiv y \pmod p$ θα συμβολίζεται με $x=y \bmod p$)

Παρατήρηση :

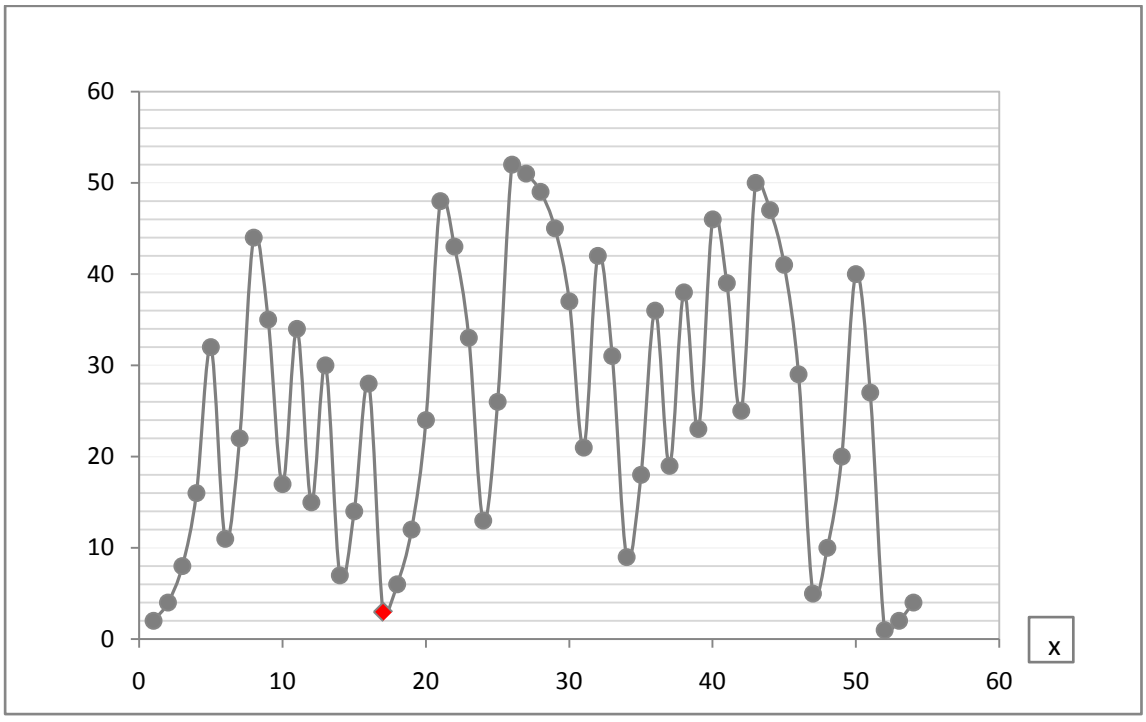
Η δυσκολία του DLP είναι ανεξάρτητη της επιλογής του γεννήτορα g του Z_p^* λόγω της ιδιότητας (iii) του διακριτού λογαρίθμου. Αυτό συμβαίνει γιατί εάν βρούμε το διακριτό λογάριθμο του b με βάση g, τότε βρίσκουμε και το διακριτό λογάριθμο οποιουδήποτε γεννήτορα g΄.

$$\log_{g'} b \equiv (\log_g b)(\log_g g')^{-1} \bmod n$$

Παράδειγμα 3.1:

Για p=53 , η Z_{53}^* είναι κυκλική ομάδα τάξης n=52. Ένας γεννήτορας της Z_{53}^* είναι ο g=2. Έστω b=3.Αφού $2^{17}=3 \bmod 53$ έχουμε ότι $\log_2 3=17$ στο Z_{53}^* .

Παρακάτω βλέπουμε το γράφημα του διακριτού λογαρίθμου
(Z_{53}^* , γεννήτορας 2) , $0 \le 2^x \bmod 53 \le 51$



Σχήμα 3.1
Γράφημα διακριτού λογαρίθμου (Z_{53}^* , γεννήτορας 2)

- **Πρόβλημα των Diffie-Hellman (DHP)**

Ένα άλλο πρόβλημα με σημαντικές εφαρμογές σε κρυπτοσυστήματα και πρωτόκολλα ανταλλαγής δεδομένων είναι το ***Πρόβλημα των Diffie-Hellman (DHP)***. Διατυπώθηκε από τους Whitfield Diffie και Martn E. Hellman το 1976 σε μία δημοσίευση με τίτλο "New Directions in Crytptography" που αποτέλεσε σταθμό στην ιστορία της σύγχρονης κρυπτογραφίας. Στην ίδια δημοσίευση οι συγγραφείς περιγράφουν και το ομώνυμο πρωτόκολλο ανταλλαγής κλειδιού που θα συζητήσουμε παρακάτω. Η ασφάλεια του προβλήματος βασίζεται στο πρόβλημα του διακριτού λογαρίθμου.

Συνήθως συναντούμε το πρόβλημα στις δύο ακόλουθες μορφές :

Πρόβλημα 3.3 : Υπολογιστικό Diffie-Hellman (DHP ή CDH)

Δίνονται : Ένας πρώτος αριθμός p, ένας γεννήτορας g του Z_p^* και δύο στοιχεία α,b $\in Z_p^*$.

Επειδή g γεννήτορας θα ισχύει $\alpha=g^x \bmod p$ και $b=g^y \bmod p$ για κάποια $x, y \in Z$

Ζητείται : Να βρεθεί το $c=g^{xy} \bmod p$

Ισοδύναμα , να βρεθεί $c \in Z_p^*$,τέτοιο ώστε

$$z = \log_g c = \log_g \alpha \cdot \log_g b \bmod(p-1)$$

Πρόβλημα 3.4 : Diffie-Hellman απόφασης (DDH)

Δίνονται : Ένας πρώτος αριθμός p, ένας γεννήτορας g του Z_p^* και τρία στοιχεία α,b,c $\in Z_p^*$.

Ζητείται : Να ελεγχθεί αν υπάρχουν $x, y \in Z$ τέτοιοι ώστε $g^x \bmod p=\alpha$, $g^y \bmod p=b$ και $c=g^{xy} \bmod p$.

Παρατήρηση

Εύκολα διαπιστώνει κανείς ότι το DDH είναι τουλάχιστον το ίδιο δύσκολο με το DHP και το DLP είναι τουλάχιστον το ίδιο δύσκολο με το DHP.

Πιο επίσημα, από τη σκοπιά της επιστήμης υπολογιστών τα DDH,DHP, DLP ανάγονται πολυωνυμικά το ένα στο άλλο με τη σειρά

$$DDH \propto_p DHP \propto_p DLP$$

Οι εν λόγω αναγωγές αποδεικνύονται εύκολα. Συγκεκριμένα έχουμε :

$DDH \propto_p DHP$ **:** Δοθέντων των g,a,b,c της DDH, χρησιμοποιώ έναν αλγόριθμο που επιλύει το CDH, βρίσκω μία τιμή c' τέτοια ώστε

$$\log_g c' = \log_g \alpha \cdot \log_g b \bmod(p-1).$$

και τέλος ελέγχω αν c=c΄.

$DHP \propto_p DLP$: Δοθέντων των g,a,b της DHP, χρησιμοποιούμε έναν αλγόριθμο που επιλύει το DLP, βρίσκω $x=\log_g\alpha$ και $y=\log_g b$ και τέλος υπολογίζω $z=xy \bmod(p-1)$ και $c=g^z \bmod p$.

Παρατήρηση (Εύρεση γεννήτορα της Z_p^*)

Δεν υπάρχει αποδοτικός αλγόριθμος για την εύρεση γεννήτορα της Z_p^* εκτός εάν έχω την παραγοντοποίηση του p-1 σε πρώτους. Το πρόβλημα της παραγοντοποίησης θεωρείται υπολογιστικά δύσκολο. Οπότε στην πράξη παράγω έναν τυχαίο παραγοντοποιημένο αριθμό n και ελέγχω τον n+1 για πρώτο, επαναλαμβάνω μέχρι να βρω n+1 πρώτο και στη συνέχεια εύκολα βρίσκω έναν γεννήτορα g. *(βλέπε [Shoup],11.1)*

Στη συνέχεια δουλεύουμε κυρίως στην κυκλική πολλαπλασιαστική ομάδα Z_p^* **,** με p πρώτο. Η μελέτη γενικεύεται εύκολα σε οποιαδήποτε πεπερασμένη κυκλική ομάδα.
Στη θέση του γεννήτορα g χρησιμοποιούμε το **πρωταρχικό στοιχείο modp** , γιατί στις κυκλικές ομάδες Z_p^* οι έννοιες γεννήτορας και πρωταρχικό στοιχείο modp συμπίπτουν.

3.2 Μέθοδοι επίλυσης του προβλήματος του διακριτού λογαρίθμου

3.2.1 Στοιχειώδεις μέθοδοι

(Υποθέτω ότι για να υπολογίσω ένα γινόμενο δύο στοιχείων της Z_p^* ,απαιτείται O(1) σταθερός χρόνος.)

- Ο στοιχειώδης αλγόριθμος εδώ είναι η **εξαντλητική μέθοδος αναζήτησης** στο Z_p^* και απαιτεί O(p) χρόνο και O(1) χώρο.
  Υπολογίζω δηλαδή τα g, g^2,g^3,... (υπολογίζοντας κάθε φορά $g^i=g^{i-1}\cdot g$ O(1) χρόνος)
  μέχρι να βρεθεί $b=g^x$.

- Μία άλλη προσέγγιση είναι η εξής:

  - Υπολογίζω εκ των προτέρων όλες τις δυνατές τιμές g^i , $0 \le i \le p-2$
    Χρόνος : O(p)
  - Ταξινομώ τη λίστα διατεταγμένων ζευγών (i, g^i) ως προς τη δεύτερη συντεταγμένη g^i ,χρησιμοποιώντας έναν αποδοτικό αλγόριθμο (π.χ. Mergesort)
    Χρόνος [2] : O(plogp) =O(p) .
  - Αναζητώ στην ταξινομημένη λίστα το ζευγάρι με $g^i=b$.
    Χρόνος : O(logp)=O(1) χρησιμοποιώντας δυαδική αναζήτηση

  Τελικά λύνω το πρόβλημα σε O(1) χρόνο με O(p) προκαταρτικούς υπολογισμούς και χρησιμοποιώντας O(p) μνήμη.

3.2.2 Μέθοδος του Shanks (ή Baby step/Giant step)

Παρατήρηση :

Έστω $x= \log_g b$, έχω:

$$0 \le x \le p-2 \qquad (1)$$

[2] Εδώ αγνοώ τον λογαριθμικό παράγοντα στην πολυπλοκότητα, όπως συνήθως γίνεται στην ανάλυση αυτών των αλγορίθμων.

Αν διαιρέσω τον x με κάποιο $m \in \square$ παίρνω

$$x = m\,j + i \qquad (2)$$

όπου $0 \le i \le m-1$ και από

$$(1),(2) \Rightarrow 0 \le j \le \frac{x}{m} \le \frac{p-2}{m} \qquad (3)$$

Η ιδέα είναι, για σταθερό m να ψάξω όλα τα πιθανά j,i μέχρι να βρω $x = mj + i$

Παίρνω m με $m^2 \ge p\text{-}1$, π.χ. το $m = \left\lceil \sqrt{p-1} \right\rceil$ (4)

$$(1),(2),(4) \Rightarrow m\,j + i = x \le p-1-1 \le m^2 - 1 = (m+1)(m-1) \Leftrightarrow$$
$$\Leftrightarrow m\,j + i \le m(m-1) + (m+1)$$

Άρα έχω $0 \le i \le m-1$ και $0 \le j \le m-1$

Ο παρακάτω αλγόριθμος είναι μια βελτίωση του προηγούμενου βασισμένος στην παραπάνω παρατήρηση

Αλγόριθμος 3.1 : Shanks (Baby step/Giant step)

1. $m \leftarrow \left\lceil \sqrt{p-1} \right\rceil$

2. Για j=0 έως m-1, υπολογίζουμε το $g^{m\,j}$ mod p .

3. Ταξινομούμε τα m διατεταγμένα ζεύγη (j, $g^{m\,j}$ mod p) βάσει της δεύτερης συντεταγμένης (δηλαδή του $g^{m\,j}$ mod p), ώστε να προκύψει μία ταξινομημένη λίστα L_1 .

4. Για i=0 έως m-1, υπολογίζουμε το bg^{-i} mod p .

5. Ταξινομούμε τα m διατεταγμένα ζεύγη (i, bg^{-i} mod p) βάσει της δεύτερης συντεταγμένης (δηλαδή του bg^{-i} mod p) , ώστε να προκύψει μία ταξινομημένη λίστα L_2 .

6. Αναζητούμε ζεύγος (j, y) ΞL_1 τέτοιο ώστε (i, y) ΞL_2, δηλαδή δύο ζεύγη που να έχουν την ίδια τεταγμένη.

7. $(\log_g b =) x := m\,j + i \mod (p-1)$.

1. **Πράγματι** ισχύει $\log_g b = x = m\,j + i \bmod(p-1)$ γιατί:

Αν (j, y) $\Xi\, L_1$ και (i, y) $\Xi\, L_2$ τότε:

$$g^{m\,j} = y = bg^{-i} \Rightarrow g^{m\,j+i} = b \Rightarrow g^{x} = b \Rightarrow$$
$$\Rightarrow x = \log_g b$$

Τέλος, για να πέσω σε μια κλάση ισοδυναμίας της $\mathbf{Z}_p^*$ παίρνω το mod(p-1).

2. Αντί για τα βήματα 4,5,6 μπορούμε κάθε φορά που υπολογίζουμε ένα στοιχείο $bg^{-m\,j} \bmod p$ να το αναζητούμε στην L_1.

3. Τελικά από την ανάλυση του αλγορίθμου έχουμε:

Πολυπλοκότητα χώρου $O(\mathrm{m}) = O\left(\sqrt{p}\right)$

(για τα ταξινομημένα διανύσματα)

Πολυπλοκότητα χρόνου $O(\mathrm{m}) = O\left(\sqrt{p}\right)$

(για τις αναζητήσεις)

4. Ανήκει στην κατηγορία των αλγορίθμων ανταλλαγής χρόνου-μνήμης (time-memory trade-off algorithms) : επιλέγοντας μικρότερο m παίρνουμε λίστα μεγέθους O(m) (μνήμη), αλλά επειδή $0 \le j \le \frac{x}{m} \le \frac{p-2}{m}$ ο χρόνος εκτέλεσης θα είναι ανάλογος του O(p/m).

5. Ο αλγόριθμος στην πράξη δουλεύει για πρώτους μέχρι και λίγο πάνω από 20 ψηφία.

Παράδειγμα 3.2 :

Έστω ότι p= 809 και θέλουμε να υπολογίσουμε τον $\log_3 525$ ($g = 3, b = 525$). Το $m := \left\lceil \sqrt{808} \right\rceil = 29$.Επίσης έχω

$$3^{29} \bmod 809 = 99$$

Πρώτα υπολογίζουμε τα διατεταγμένα ζεύγη ($j, 99^j \bmod 809$), για $0 \le j \le 28$ δημιουργώντας έτσι τη λίστα :

(0,1)	(5,329)	**(10,644)**	(15,727)	(20,528)	(25,586)
(1,99)	(6,211)	(11,654)	(16,781)	(21,496)	(26,575)
(2,93)	(7,664)	(12,26)	(17,464)	(22,564)	(27,295)
(3,308)	(8,207)	(13,147)	(18,632)	(23,15)	(28,81)
(4,559)	(9,268)	(14,800)	(19,275)	(24,676)	

από την οποία με ταξινόμηση θα προκύψει η L_1 .

Στη συνέχεια δημιουργούμε μία λίστα από τα διατεταγμένα ζεύγη $(i, 525 \cdot 3^{-i} \bmod 809)$, $0 \le i \le 28$ (υπολογίζοντας το 3^{-1} =270 με επεκταμένο Ευκλείδειο αλγόριθμο:

(0,525)	(5,132)	(10,440)	(15,388)	(20,754)	(25,356)
(1,175)	(6,44)	(11,686)	(16,399)	(21,521)	(26,658)
(2,328)	(7,554)	(12,768)	(17,133)	(22,713)	(27,489)
(3,379)	(8,724)	(13,256)	(18,314)	(23,777)	(28,163)
(4,396)	(9,511)	(14,355)	**(19,644)**	(24,259)	

από την οποία με ταξινόμηση θα προκύψει η L_2 .

Πρακτικά μόλις βρούμε τη σύμπτωση (στη θέση 19) σταματάμε τον αλγόριθμο. Έτσι θα βρούμε τα στοιχεία $(10, 644) \in L_1$ και $(19, 644) \in L_2$.Υπολογίζουμε το

$$x = \log_3 525 = 29 \cdot 10 + 19 = 309 \ .$$

Πράγματι μπορούμε εύκολα να επαληθεύσουμε ότι $3^{309} = 525 (\bmod 809)$. W

3.2.3 Μέθοδος των Pohlig-Hellman

Υπενθυμίζουμε δύο θεωρήματα που θα χρησιμοποιήσουμε :

(Θ. 1): Αν g πρωταρχική ρίζα της $\mathbb{Z}_p^*$ και $g^r = 1 \bmod m$ τότε: $p-1 \mid r$

(Θ. 2): Αν g πρωταρχική ρίζα της $\mathbb{Z}_p^*$ και ΜΚΔ(k,p-1)=d τότε ο g^k ανήκει στον εκθέτη $p-1/d$ modulo m

Παρατήρηση :

-Έστω ο πρώτος p και g μία πρωταρχική ρίζα modp, δηλαδή ο φ(p)=p-1 είναι ο μικρότερος θετικός ακέραιος n με $g^n=1$ modp. Τότε χρησιμοποιώντας το **(Θ. 1)** έχω

$$g^{m_1} = g^{m_2} \bmod p \Rightarrow g^{m_1-m_2} = 1 \bmod p \Rightarrow$$
$$\overset{(\Theta.1)}{\Rightarrow} (p-1) \mid (m_1 - m_2) \Leftrightarrow m_1 - m_2 = k(p-1) \Leftrightarrow$$
$$\Leftrightarrow m_1 = m_2 \bmod (p-1)$$

-Έστω $b=g^x$ με $0 \le x \le p-2$, θέλουμε να υπολογίσουμε το x , δηλαδή θέλουμε να επιλύσουμε το DLP.

-Υπολογίζω εύκολα το $x \bmod 2$:

Είναι $\text{ΜΚΔ}\left(p-1, \frac{p-1}{2}\right) = \frac{p-1}{2}$

Άρα από **(Θ. 2)** $\Rightarrow g^{\frac{p-1}{2}}$ ανήκει στον εκθέτη $\frac{p-1}{\frac{p-1}{2}} = 2 \bmod p \Rightarrow$

$\Rightarrow (g^{\frac{p-1}{2}})^2 = 1 \bmod p \Rightarrow g^{\frac{p-1}{2}} = \pm 1 \bmod p.$

Όμως p-1 είναι ο μικρότερος εκθέτης n με $g^n=1$ modp άρα:

$g^{\frac{p-1}{2}} = -1 \bmod p.$

Υψώνω τώρα την $b=g^x$ στην δύναμη $\frac{p-1}{2}$:

$$b = g^x \Rightarrow b^{\frac{p-1}{2}} = g^{x\left(\frac{p-1}{2}\right)} = \left(g^{\left(\frac{p-1}{2}\right)}\right)^x = (-1)^x \bmod p.$$

Άρα
$b^{\frac{p-1}{2}} = 1$ αν x άρτιος
$b^{\frac{p-1}{2}} = -1$ αν x, περιττός

Βασική ιδέα του αλγορίθμου :

-Έστω $x = \log_g b$ και $p-1 = \prod_i q_i^{e_i}$ τότε:

-Υπολογίζω τα $x \bmod q_i^{e_i} \quad \forall i$

-Συνδυάζω τις απαντήσεις μέσω του Κινέζικου θεωρήματος υπολοίπων (ΚΘΥ) και βρίσκω μια μοναδική λύση mod(p-1).Δηλαδή επιλύω το DLP.
(Το ΚΘΥ προφανώς εφαρμόζεται γιατί ΜΚΔ($q_i^{e_i}$, $q_j^{e_j}$)=1 $\forall i \neq j$)

Αναλύουμε τώρα τη μέθοδο υπολογισμού του $x \bmod q_i^{e_i} \quad \forall i$:

Έστω q ένας πρώτος από τους q_i .Θέτω $x = x_0 + x_1 q + x_2 q^2 + \ldots$ (*)
με $0 \le x_i \le p-1$,θα υπολογίσω τα x_i άρα και το x .

Βήμα 1.

Υπολογισμός του x_0 :

- Παρατηρώ:

$$x\left(\frac{p-1}{q}\right) \overset{(*)}{=} x_0\left(\frac{p-1}{q}\right) + (p-1)(x_1 + x_2 q + x_3 q^2 + \ldots) \Rightarrow$$

$$\Rightarrow x\left(\frac{p-1}{q}\right) = x_0\left(\frac{p-1}{q}\right) + n(p-1) \qquad , n \in \mathbf{Z}$$

-Υψώνω την $b=g^x$ στον ακέραιο $\frac{p-1}{q}$,οπότε:

$$\left.\begin{array}{l} b^{\frac{p-1}{q}} = g^{x\left(\frac{p-1}{q}\right)} = g^{x_0\left(\frac{p-1}{q}\right)}\left(g^{p-1}\right)^n \\ (**) : g^{p-1} \equiv 1 \bmod p \quad (\text{Θεώρημα Fermat}) \end{array}\right\} \Rightarrow b^{\frac{p-1}{q}} = g^{x_0\left(\frac{p-1}{q}\right)} \cdot 1 \bmod p$$

-Για να βρώ το x_0 εξετάζω τις δυνάμεις $g^{k\left(\frac{p-1}{q}\right)}$, k=0,1,..,q-1 μέχρι να πάρω : $g^{k\left(\frac{p-1}{q}\right)} = b^{\frac{p-1}{q}}$.Τότε x_0=k. (Η μοναδικότητα του k εξασφαλίζεται από τη σχέση

$g^{m_1} = g^{m_2} \bmod p \Leftrightarrow m_1 = m_2 \bmod(p-1)$ και το γεγονός ότι οι εκθέτες $\frac{k(p-1)}{q}$ είναι διαφορετικοί mod(p-1) .

Βήμα 2.

Υπολογισμός του x_1 :

-Ελέγχω αν $q^2 \mid p-1$, έστω ότι ισχύει

-Θέτω $b_1 = bg^{-x_0} = g^{x-x_0} \overset{(*)}{=} g^{(x_1 q + x_2 q^2 + \ldots)} \bmod p$ ψώνω στον ακέραιο $\frac{p-1}{q^2}$

Έχουμε:

$$b_1^{\frac{p-1}{q^2}} = g^{\frac{p-1}{q}(x_1 + x_2 q + \ldots)} = g^{x_1 \frac{p-1}{q}} \left(g^{p-1}\right)^{x_2 + x_3 q + \ldots} \overset{(**)}{=} g^{x_1 \frac{p-1}{q}} \bmod p$$

-Ομοίως με το βήμα 1 ψάχνω $k \in \{0,1,\ldots,q-1\}$ με $g^{k\left(\frac{p-1}{q}\right)} = b^{\frac{p-1}{q^2}}$

Οπότε υπολογίζω $x_1 = k$ μοναδική λύση.

Βήμα 3.

Υπολογισμός του x_2 :

-Ελέγχω αν $q^3 \mid p-1$, έστω ότι ισχύει.

- Θέτω $b_2 = b_1 g^{-x_1 \cdot q}$, υψώνω στον ακέραιο $\frac{p-1}{q^3}$ και υπολογίζω το x_2 .

Βήμα n.

Υπολογισμός του x_{n-1} :

-Ελέγχω αν $q^n \mid p-1$, έστω ότι ισχύει.

- Θέτω $b_{n-1} = b_{n-2} g^{-x_{n-2} \cdot q^{n-2}}$ (όπου b_0=b) , υψώνω στον ακέραιο[3] $\frac{p-1}{q^n}$ και υπολογίζω το x_{n-1}.

Συνεχίζουμε έως ότου βρούμε $q^{r+1} \nmid p-1$ οπότε σταματάμε
Έχουμε υπολογίσει τα $x_1, x_2, ..., x_{r-1}$ άρα και το x $\bmod p^r$.

Επαναλαμβάνω τα βήματα 1 έως r_i+1 για όλους τους πρώτους παράγοντες $q_i^{r_i}$ (για όλα τα i) .
Τέλος το ΚΘΥ μας επιτρέπει να συνενώσουμε όλες τις ισοδυναμίες σε μία ισοδυναμία x $\bmod (p-1)$.Αφού $0 \le x \le p-1$ υπολογίσαμε τον εκθέτη x άρα λύσαμε το DLP.

Παρατήρηση :

1. Η δυσκολία υπολογισμού του x προσδιορίζεται από το μέγεθος του μεγαλύτερου πρώτου που διαιρεί το p-1 (επειδή σε κάθε βήμα ψάχνουμε ένα $k \in \{0,1,...,q-1\}$).
Έτσι στην πράξη ο αλγόριθμος επιλύει το DLP όταν ο p-1 έχει μόνο μικρούς πρώτους παράγοντες.

2. (Πολυπλοκότητα του αλγορίθμου)

- Πρώτη ματιά: Αν $q = \max\{q_i\}$, κάνω q βήματα στο ψάξιμο του k ,αν έχω q^r το κάνω r φορές Άρα έχω πολυπλοκότητα $O(r \cdot q)$.

- Όμως η εύρεση του k μπορεί να θεωρηθεί σαν ένα πρόβλημα διακριτού λογαρίθμου αφού έχω :

$$\delta = g^{k\left(\frac{p-1}{q}\right)} \Leftrightarrow k = \log_{g^{\frac{p-1}{q}}} \delta .$$

[3] Ο $\frac{p-1}{q^n}$ είναι πάντα ακέραιος λόγω της $q^n \mid p-1$

Κάθε στοιχείο $g^{\left(\frac{p-1}{q}\right)}$ έχει τάξη[4] q και επομένως κάθε k μπορεί να υπολογιστεί (π.χ. με αλγόριθμο του Shanks) σε χρόνο $O(\sqrt{q})$.

Επομένως έχω $O(r\cdot\sqrt{q})$ όπου η χειρότερη περίπτωση για το r είναι όταν ισχύει $p-1=2^r \Leftrightarrow r=\log_2 p$.
Άρα έχουμε $O\left(\log p\cdot\sqrt{q}\right)$ και αγνοώντας λογαριθμικούς παράγοντες τελικά έχουμε:

Πολυπλοκότητα χρόνου : $O\left(\sqrt{q}\right)$

Παραθέτουμε τον αλγόριθμο που περιγράψαμε παραπάνω:

Αλγόριθμος 3.2: Pohlig-Hellman

1. $p-1=\prod_i q_i^{e_i}$
2. Για κάθε i επιλύω την εξίσωση $b=g^x \bmod q_i^{r_i}$:
   3. Θεωρώ $x=x_0+x_1q_i+x_2{q_i}^2+\ldots+x_{r_i-1}{q_i}^{r_i-1}$
   4. j:=0
   5. b_j:=b
   6. Όσο ισχύει $j \le r_i-1$ κάνε
      7. Βρες k τέτοιο ώστε $b_j^{\frac{p-1}{q_i^{j+1}}}=g^{\frac{k(p-1)}{q_i}} \bmod p$
      8. x_j:=k
      9. $b_{j+1}:=b_j g^{-x_j q_i^j}$.
      10. j:= j+1
11. Με ΚΘΥ ενώνω τις ισοδυναμίες και βρίσκω τη λύση x .

[4] Γιατί προφανώς το q είναι ο μικρότερος εκθέτης που μας δίνει $\left(g^{\frac{p-1}{q}}\right)^q = g^{p-1}=1$.

Παράδειγμα 3.2 :

Έστω p=41, g=7, b=12 και θέλουμε να λύσουμε την 7^x=12 mod41.

Επειδή 41-1=40=2^3·5 θα εξετάσουμε τις περιπτώσεις των παραγόντων q=2 και q=5,για την ακρίβεια $q=2^3$ και q=5.

Έστω q=2 και θα βρούμε τον $x \bmod 2^3 = x \bmod 8$. Θέτουμε :

$$x = x_0 + 2x_1 + 4x_2 \bmod 8, \ με \ \ x_0 \ , x_1, x_2 \in \{0,1\}$$

Αρχίζουμε με $\beta^{\frac{p-1}{2}} = 12^{20} = 40 = -1 \bmod 41$. Πράγματι:

$12^1 = 12$

$12^2 = 21$

$12^3 = 6$

$12^4 = 31$

$12^5 = 3$

$g^{\frac{p-1}{2}} = 7^{20} = 40 = -1 \bmod 41$, αφού

$7^1 = 7 \bmod 41$	$7^6 = 20$
$7^2 = 49 = 8 \bmod 41$	$7^7 = 17$
$7^3 = 7\cdot 8 = 56 = 15 \bmod 41$	$7^8 = 37$
$7^4 = 105 = 23 \bmod 41$	$7^9 = 13$
$7^5 = 38$	$7^{10} = 9$

άρα $7^{20} = 9\cdot 9 = 81 = -1 \bmod 41$.

Άρα $\beta^{\frac{p-1}{2}} = \left(g^{\frac{p-1}{2}} \right)^{x_0} \bmod p \Rightarrow -1 = (-1)^{x_0} \bmod 41 \Rightarrow x_o = 1$.

Ακολούθως $b_1 = bg^{-x_o} = 12\cdot 7^{-1} = 12\cdot 6 = 72 = 31 \bmod 41$.

[Πράγματι $6\cdot 7 = 42 = 1 \bmod 41 \Rightarrow 7^{-1} = 6$]

Επίσης $b_1^{\frac{p-1}{2}} = 31^{10} = 1 \bmod 41$, πράγματι $31^5 = -1$ και $b_1^{\frac{p-1}{2^2}} = \left(g^{\frac{p-1}{2}} \right)^{x_1} \bmod 41 \Rightarrow$

$\Rightarrow 1 = (-1)^{x_1} \bmod 41 \Rightarrow x_1 = 0.$

Ομοίως έχουμε:

$b_2 = b_1 g^{-2x_1} = 31 \cdot 7^0 = 31 \bmod 41$, οπότε

$q^3 \mid p-1$ και $b_1^{\frac{p-1}{2^3}} = -1 = \left(g^{\frac{p-1}{2}} \right)^{x_2} \bmod 41 \Rightarrow x_2 = 1$. Πήραμε λοιπόν :

$$x = x_0 + 2x_1 + 4x_2 = 1 + 2 \cdot 0 + 4 \cdot 1 = 5 \bmod 8.$$

Τώρα παίρνω $q = 5$ και θα βρω το $x \bmod 5$. Έχουμε:

$b^{\frac{p-1}{5}} = 12^8 = 12^5 \cdot 12^3 = 3 \cdot 6 = 18 \bmod 41$ και $g^{\frac{p-1}{q}} = 7^8 = 37 \bmod 41.$

Δοκιμάζοντας τις δυνάμεις του k έχω:

$37^0 = 1 \bmod 41$

$37^1 = 37 \bmod 41$

$37^2 = 16 \bmod 41 \qquad 18 = 37^k \bmod 41 \Rightarrow k = 3$

$37^3 = \boxed{18} \bmod 41$

$37^4 = 10 \bmod 41$

Άρα έχω τη λύση $x = 3 \bmod 5.$

Πρέπει λοιπόν να συνδυάσω τις λύσεις :

$x = 5 \bmod 8 \Rightarrow x = \left\{ 5, \boxed{13}, 21, 29, 37, 45, \boxed{53}, \ldots \right\}$ και

$x = 3 \bmod 5 \Rightarrow x = \left\{ 3, 8, \boxed{13}, 18, 23, 28, 33, 38, 43, 48, \boxed{53}, \ldots \right\}$ με το ΚΘΥ .

Άρα $x = 13 \bmod 40 \Rightarrow x = 13$

Πράγματι ελέγχω:

$$7^{13} = 12 \bmod 41$$

$$7^{13} = 7^{10} \cdot 7^3 = 9 \cdot 15 = 12 \bmod 41$$

άρα λύθηκε το DLP $7^x = 12 \bmod 41$.

3.2.4 Μέθοδος Λογισμού – Δεικτών (Index Calculus)

Οι αλγόριθμοι που παρουσιάσαμε παραπάνω (3.2.1 έως 3.2.4) μπορούν να εφαρμοστούν σε οποιαδήποτε πεπερασμένη κυκλική ομάδα για την επίλυση του προβλήματος του διακριτού λογαρίθμου, ονομάζονται **γενετικοί αλγόριθμοι.**

Στις διάφορες παραλλαγές τους οι αλγόριθμοι Index Calculus εφαρμόζονται αποδοτικά στις ειδικές περιπτώσεις των πεπερασμένων κυκλικών ομάδων $\mathbf{Z}_p^*$ (p πρώτος) και $\mathbf{F}_{2^m}^*$ (πεπερασμένου σώματος χαρακτηριστικής 2) και γενικά της πολλαπλασιαστικής ομάδας $\mathbf{F}_q^*$ του πεπερασμένου σώματος $\mathbf{F}_q$.

Συσχετίζονται με αλγόριθμους παραγοντοποίησης όπως το τετραγωνικό κόσκινο και το κόσκινο του αριθμητικού σώματος, και είναι οι αποδοτικότεροι γνωστοί αλγόριθμοι για την επίλυση του DLP.

Βασική ιδέα του αλγορίθμου

(Υπενθύμιση)
Ο α είναι **B-λείος** αν όλοι οι πρώτοι παράγοντές του είναι μικρότεροι από το B.

Έστω p :πρώτος, g πρωταρχική ρίζα της $\mathbf{Z}_p^*$ (γεννήτορας) και $b \in \mathbf{Z}_p^*$. Θέλουμε να επιλύσουμε το DLP $g^x = b \bmod p$.

Η μέθοδος χρησιμοποιεί μια παραγοντική βάση (factor base), η οποία είναι ένα σύνολο $F \subset \mathbf{Z}_p^*$ "μικρών" πρώτων , έτσι ώστε αρκετά στοιχεία της $\mathbf{Z}_p^*$ να εκφράζονται σαν γινόμενα των στοιχείων της F .
Συνήθως επιλέγουμε ένα φράγμα B και υπολογίζουμε το σύνολο

$$F = F(B) = \{q : \text{πρώτος}, \ q \le B\}$$

σαν τη βάση πρώτων παραγόντων μας. Έστω $F(B) = \{q_1, ..., q_t\}$.

- Το πρώτο βήμα (προϋπολογισμοί) είναι να υπολογίσουμε μια βάση δεδομένων η οποία θα περιέχει τους διακριτούς λογαρίθμους όλων των στοιχείων της $F(B)$.
Για να το πετύχουμε αυτό δημιουργούμε t+c γραμμικές σχέσεις που εμπεριέχουν τους διακριτούς λογάριθμους των t στοιχείων της $F(B)$.Το c είναι μικρός θετικός ακέραιος , π.χ. c=10, έτσι ώστε να υπάρχει μεγάλη πιθανότητα το σύστημα των t+c σχέσεων να έχει μοναδική λύση.

Συμβολίζουμε τους διακριτούς λογαρίθμους των $q_i \in F(B)$ με[5] $x(q_i)$, δηλαδή :

$$g^{x(q_i)} = q_i \bmod p \ , \ \forall q_i \in F(B) \qquad (*)$$

- Στη συνέχεια ο αλγόριθμος χρησιμοποιεί αυτή τη βάση δεδομένων για υπολογίσει το διακριτό λογάριθμό του b.

Παραθέτουμε τώρα τον αλγόριθμο :

Αλγόριθμος 3.3: Index-calculus

- **(Μέρος Ι) Εύρεση των διακριτών λογαρίθμων των $q_i \in F(B)$.**

1. Επιλέγω φράγμα B και θέτω $F(B) = \{q : \text{πρώτος}, \ q \le B\}$.

2. Επιλέγω έναν τυχαίο ακέραιο k, $1 \le k \le p-1$ και υπολογίζω $g^k \in \mathbf{Z}_p^*$.

3. Αν ο g^k είναι B-λείος έχουμε για $c_i \ge 0$:

$$g^k = \prod_{i=1}^{t} q_i^{c_i} \ (\bmod p) \overset{(*)}{\Rightarrow} g^k = \prod_{i=1}^{t} g^{x(q_i)\cdot c_i} = g^{\sum_{i=1}^{t} x(q_i)\cdot c_i} \bmod p \Rightarrow$$

$$\Rightarrow k = \sum_{i=1}^{t} x(q_i)\cdot c_i \bmod (p-1) \qquad (**)$$

4. Επανέλαβε τα βήματα **2 , 3** μέχρι να προκύψουν t+c σχέσεις της μορφής $(**)$. (π.χ. για c=10) .Τελικά θα πάρω ένα γραμμικό σύστημα ισοδυναμιών modulo p-1.

5. Υπολογίζω τους διακριτούς λογαρίθμους $x(q_i)$ για $1 \le i \le t$, λύνοντας το γραμμικό σύστημα των t+c σχέσεων (με t αγνώστους) που προκύπτουν από το βήμα **4.**

συνεχίζεται στην επόμενη σελίδα

Αλγόριθμος 3.3: Index-calculus

- **(Μέρος ΙΙ) Εύρεση του b.**

1. Επιλέγω έναν τυχαίο ακέραιο y, $1 \le y \le p-1$ και υπολογίζω $b \cdot g^y \in \mathbf{Z}_p^*$.

2. Αν ο $b \cdot g^y$ είναι Β-λείος έχουμε για $e_i \ge 0$:

$$b \cdot g^y = \prod_{i=1}^{t} q_i^{e_i} \pmod p \overset{(*)}{\Rightarrow} b \cdot g^y = \prod_{i=1}^{t} g^{x(q_i)\cdot e_i} = g^{\sum_{i=1}^{t} x(q_i)\cdot e_i} \bmod p \Rightarrow$$

$$\Rightarrow g^x = b = g^{\sum_{i=1}^{t} x(q_i)\cdot e_i - y} \bmod p \Rightarrow$$

$$\Rightarrow x = \left(\sum_{i=1}^{t} x(q_i) \cdot e_i - y \right) \bmod (p-1) \qquad (***)$$

Δηλαδή υπολογίζουμε το διακριτό λογάριθμο που θέλουμε από τη σχέση $(***)$.

3. Αλλιώς (αν ο $b \cdot g^y$ δεν είναι Β-λείος) επανέλαβε τα βήματα **1,2 .**

Παρατηρήσεις :

1. Το πρώτο μέρος (εύρεση των $x(q_i)$) απαιτεί τους περισσότερους υπολογισμούς, αλλά χρειάζεται να υπολογίσουμε τα $x(q_i)$ μόνο μία φορά.
Έπειτα χρησιμοποιούμε τη βάση δεδομένων που κατασκευάσαμε για να υπολογίσουμε όποιον λογάριθμο μας ζητηθεί στην ίδια ομάδα $\mathbf{Z}_p^*$.

2. Η επιλογή του μεγέθους της παραγοντικής βάσης Β είναι σημαντική. Εάν το Β είναι πολύ μικρό, τότε θα είναι πολύ δύσκολο να βρούμε δυνάμεις του g που παραγοντοποιούνται με πρώτους στη Β. Εάν η Β είναι πολύ μεγάλη, θα είναι εύκολο να βρούμε σχέσεις, αλλά η γραμμική άλγεβρα modulo p-1 που χρειάζεται να λύσουμε για τους λογάριθμους των στοιχείων του Β θα είναι δύσχρηστη. Ένα παράδειγμα που ολοκληρώθηκε το 2001 από τους A. Joux και R. Lercier χρησιμοποίησε τους πρώτους ένα εκατομμύριο πρώτους αριθμούς για να υπολογίσει διακριτούς λογάριθμους για p ένα 120-ψήφιο πρώτο.

3. Στο βήμα **5** (Μέρος Ι) για να επιλύσουμε το σύστημα πρέπει να χρησιμοποιήσουμε γραμμική άλγεβρα modulo p-1. Αντίθετα σε προβλήματα παραγοντοποίησης μια παρόμοια μέθοδος θα απαιτούσε επίλυση συστήματος modulo 2.
Αυτό καθιστά το πρόβλημα του διακριτού λογαρίθμου πιο δύσκολο από τα προβλήματα παραγοντοποίησης με τον ίδιο αριθμό ψηφίων.

4. Με μια ιδανική επιλογή των στοιχείων της $F(B)$,ο αλγόριθμος Index-Calculus όπως περιγράφηκε αναμένουμε να έχει

Πολυπλοκότητα χρόνου[6] : $O\left(L_p\left(1/2, c\right)\right) = O\left(e^{\left(c+O(1)\right)\sqrt{(\log p)\log\log p}}\right)$

για c:σταθερά.

Σήμερα η πιο αποδοτική παραλλαγή του index-calculus για τον υπολογισμό διακριτών λογαρίθμων στην $\mathbb{Z}_p^*$, χρησιμοποιεί το κόσκινο του αριθμητικού σώματος στα βήματα **(I.2,3)** και **(II.1,2)** και τελικά μας δίνει χρονική πολυπλοκότητα

$$O\left(L_p\left(1/3, c\right)\right) \text{ με } c \approx 1.923$$

Αντίστοιχα, για διακριτούς λογαρίθμους στην $\mathbb{F}_{2^m}^*$ η πιο αποδοτική παραλλαγή ονομάζεται αλγόριθμος του Coppersmith και απαιτεί χρόνο

$$O\left(L_p\left(1/3, c\right)\right) \text{ με } c \approx 1.587$$

Τέλος η πολυπλοκότητα χώρου είναι ο αριθμός των δεικτών $x(q_i)$ δηλαδή το πλήθος των στοιχείων της $F(B)$.Άρα έχουμε

Πολυπλοκότητα χώρου : $O(1)$

Γενικά οι αλγόριθμοι index-calculus είναι **υποεκθετικοί αλγόριθμοι** (απαιτούν λιγότερο χρόνο από τους εκθετικούς και περισσότερο από τους πολυωνυμικούς).
Αυτό σημαίνει ότι είναι πολύ πιο γρήγοροι από τους αλγόριθμους που μελετήσαμε μέχρι τώρα οι οποίοι είναι όλοι εκθετικοί.

---

[6] Είναι $L_x(t,c) = e^{\left(c+O(1)\right)(\log x)^t(\log\log x)^{1-t}}$ (για $x \to \infty$).

Παράδειγμα 3.3 :

Έστω p=2027, g=2 και F(B)={2,3,5,7,11} ήτοι B=11.

Παρατηρούμε :

$3\cdot 11 = 33 = 2^{1593} \bmod 2027$

$5\cdot 7\cdot 11 = 385 = 2^{983} \bmod 2027$

$2^7\cdot 11 = 1408 = 2^{1318} \bmod 2027$

$3^2\cdot 7 = 63 = 2^{293} \bmod 2027$

$2^6\cdot 5^2 = 1600 = 2^{1918} \bmod 2027$

Έχουμε τώρα $q=g^{x(q)} \bmod 2027$, q=2,3,5,7,11 οπότε

$$\left.\begin{array}{l} x(3)+x(11)=1593 \bmod 2026 \\ x(5)+x(7)+x(11)=983 \bmod 2026 \\ 7\cdot x(7)+x(11)=1318 \bmod 2026 \\ 2\cdot x(3)+x(7)=293 \bmod 2026 \\ 6\cdot x(2)+2\cdot x(5)=1918 \bmod 2026 \end{array}\right\} 2026 = 2\cdot 1013 \text{ , } 1013 \text{ } \pi\rho \text{ } \tau o\varsigma.$$

Λύνω το σύστημα και έχω :

$$\left.\begin{array}{l} x(3)+x(11)=1 \bmod 2 \\ x(5)+x(7)+x(11)=1 \bmod 2 \\ x(2)+x(11)=0 \bmod 2 \\ x(7)=1 \bmod 2 \end{array}\right\}$$

Αλλά x(2) = 1mod2 διότι g=2 πρωταρχική ρίζα άρα

$$\left.\begin{array}{l} x(2)=x(5)=x(7)=x(11)=1 \bmod 2 \\ x(3)=0 \bmod 2 \end{array}\right\}$$

Επίσης

$$\left.\begin{array}{l} x(3)+x(11)=580 \bmod 1013 \\ x(5)+x(7)+x(11)=983 \bmod 1013 \\ x(11)=298 \bmod 1013 \\ 2\cdot x(3)+x(7)=293 \bmod 1013 \\ 2\cdot x(5)=899 \bmod 1013 \end{array}\right\}$$

Είναι x(11) = 298 mod1013.

Επίσης $2\cdot 507 = 1 \bmod 1013$ άρα $2^{-1} = 507$ και

η $5^{η}$ εξίσωση δίνει $x(5) = 899\cdot 507 = 956 \bmod 1013$,

η $2^{η}$ εξίσωση δίνει $x(7) = 742 \bmod 1013$,

η $1^{η}$ εξίσωση δίνει $x(3) = 282 \bmod 1013$.

Από το ΚΘΥ παίρνω τελικά x(2)=1, x(3)=282, x(5)=1969, x(7)=1755,x(11)=1311. Εύκολα επαληθεύονται τα αποτελέσματα.

W

3.3 Κρυπτοσυστήματα Δημοσίου Κλειδιού βασισμένα στο DLP

Όπως αναφέρθηκε στην εισαγωγή, στα ασύμμετρα κρυπτοσυστήματα (δημοσίου κλειδιού) δεν είναι αναγκαία η ύπαρξη ενός ασφαλούς διαύλου επικοινωνίας. Αυτό είναι και το βασικό πλεονέκτημα έναντι των συμμετρικών κρυπτοσυστημάτων (ή μυστικού κλειδιού).
Όμως τα περισσότερα ασύμμετρα κρυπτοσυστήματα (π.χ. RSA) είναι πιο αργά από κάποια συμμετρικά (π.χ. AES)
Συνεπώς, συνηθίζεται να χρησιμοποιούμε ένα κρυπτοσύστημα δημοσίου κλειδιού για να εδραιωθεί ένα κλειδί το οποίο μετά χρησιμοποιείται στο συμμετρικό σύστημα. Η βελτίωση στην ταχύτητα είναι σημαντική όταν μεταφέρεται μαζικός όγκος δεδομένων.
Εξετάζουμε τώρα το παρακάτω πρωτόκολλο το οποίο ανήκει στην κατηγορία των **πρωτοκόλλων συμφωνίας κλειδιού (**key agreement protocol **).**

3.3.1 Πρωτόκολλο Συμφωνίας Κλειδιού Diffie-Hellman

Το πρωτόκολλο επιτρέπει στην **A** και στον **B** να ανταλλάξουν δημόσια[7] δύο στοιχεία και έπειτα με τη χρήση των ιδιωτικών τους κλειδιών να καταλήξουν και οι δύο στο κοινό (μυστικό) κλειδί K.
Στην συνέχεια χρησιμοποιώντας το K θα μπορούν να ανταλλάζουν κρυπτογραφημένα μηνύματα χρησιμοποιώντας ένα συμμετρικό κρυπτοσύστημα.

[7] : Ισοδύναμα μπορούμε να πούμε ότι ανταλλάζουν τα στοιχεία μέσω ενός μη ασφαλούς διαύλου επικοινωνίας.

Πρωτόκολλο συμφωνίας κλειδιού Diffie-Hellman

1. Αρχικά δημοσιεύεται ένας πρώτος αριθμός p, κατάλληλα επιλεγμένος (ώστε να καθίσταται «αδύνατη» η επίλυση του αντίστοιχου DLP) και ένας γεννήτορας g του Z_p^* ($2 \leq g \leq p-2$)(Στην πράξη αυτά μπορούν να περιέχονται στο πρώτο μήνυμα).

2. Η Alice επιλέγει ένα τυχαίο $x \in \mathbf{Z}$ και στη συνέχεια υπολογίζει :

$$b_A = g^x \bmod p$$

και στέλνει το b_A στον Bob**.**

3. Ο Bob επιλέγει ένα τυχαίο $y \in \mathbf{Z}$ και στη συνέχεια υπολογίζει :

$$b_B = g^y \bmod p$$

και στέλνει το b_A στην Alice**.**

4. Ο Bob λαμβάνει το b_A και υπολογίζει

$$K = (b_A)^y = g^{xy}$$

5. Η Alice λαμβάνει το b_B και υπολογίζει

$$K = (b_B)^x = g^{yx}$$

Παρατηρήσεις :

1. Ασφάλεια του πρωτοκόλλου Συμφωνίας Κλειδιού Diffie-Hellman

Οι πληροφορίες που μπορεί να υποκλέψει ο αντίπαλος είναι τα

$$g, p, b_A (= g^x), b_B (= g^y)$$

τότε για τον υπολογισμό του κλειδιού K πρέπει να υπολογίσει το

$$K = g^{xy}$$

το οποίο ισοδυναμεί με την επίλυση του προβλήματος DHP (Πρόβλημα 2).

Συνεπώς, η ασφάλεια του πρωτοκόλλου βασίζεται στη δυσκολία επίλυσης του DHP.

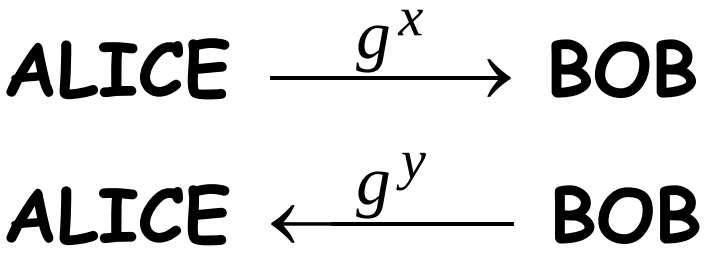
2. Μειονέκτημα πρωτοκόλλου Συμφωνίας Κλειδιού Diffie-Hellman

Υποθέτοντας ότι το DHP είναι δυσεπίλυτο , ένας παθητικός αντίπαλος δεν μπορεί να υπολογίσει πληροφορίες για το κλειδί K .

Υπάρχει όμως μια σημαντική αδυναμία του πρωτοκόλλου στην παρουσία ενός ενεργητικού αντίπαλου. Συγκεκριμένα η αδυναμία παρουσιάζεται εάν κάποιος ενεργητικός αντίπαλος κάνει μια επίθεση "**μεσολαβητή**" (**man in the middle attack)** όπου ουσιαστικά ο αντίπαλος (Eve) παίζει το ρόλο της Alice και του Bob.
Η επίθεση μεσολαβητή στο Πρωτόκολλο συμφωνίας κλειδιού Diffie-Hellman δουλεύει με τον ακόλουθο τρόπο:

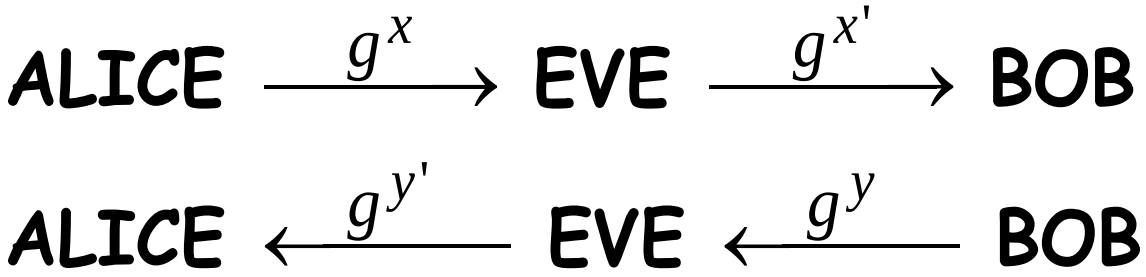
Η Eve υποκλέβει τα μηνύματα μεταξύ των Alice και Bob και τα αντικαθιστά με τα δικά της μηνύματα όπως φαίνεται στα επόμενα σχήματα.

Το Πρωτόκολλο συμφωνίας κλειδιού Diffie-Hellman κανονικά δουλεύει κάπως έτσι



Σχήμα 3.5
Πρωτόκολλο συμφωνίας κλειδιού Diffie-Hellman

Με την επίθεση μεσολαβητή της Eve μπορούμε να παρουσιάσουμε τη διαδικασία κάπως έτσι :



Σχήμα 3.6
Επίθεση μεσολαβητή (man in the middle attack)

Στο τέλος της διαδικασίας η Alice θα έχει εγκαθιδρύσει ένα μυστικό κλειδί $K_A = g^{x \cdot y'}$ με την Eve (ενώ νομίζει ότι το έχουν συμφωνήσει με τον Bob), και ο Bob θα έχει εγκαθιδρύσει ένα μυστικό κλειδί $K_B = g^{y \cdot x'}$ με την Eve.
Έτσι όταν η Α κρυπτογραφήσει ένα μήνυμα για να στείλει στον Β , η Ε θα μπορεί να το αποκρυπτογραφήσει ενώ ο Β όχι. (Ομοίως αν ο Β στείλει στην Α).

Προφανώς, είναι απαραίτητο για τους Α και Β να σιγουρευτούν ότι ανταλλάζουν μηνύματα και κλειδιά μεταξύ τους και όχι με κάποιον αντίπαλο.
Η λύση για τους Α,Β είναι να χρησιμοποιήσουν ένα πρωτόκολλο αμοιβαίας πιστοποίησης ταυτότητας και έπειτα να συμφωνήσουν σε ένα κλειδί ή ακόμη καλύτερα να χρησιμοποιήσουν ένα πρωτόκολλο συμφωνίας κλειδιού το οποίο πιστοποιεί τις ταυτότητες των Α,Β την ίδια στιγμή που εγκαθιδρύεται το κλειδί.
Περισσότερες λεπτομέρειες για αυτά τα πρωτόκολλα (ψηφιακές υπογραφές) θα δούμε παρακάτω .

Παράδειγμα 3.4:

Θεωρούμε ότι η Alice και ο Bob θέλουν να συμφωνήσουν σε ένα κοινό κλειδί.

1. Η Αλίκη επιλέγει p=2357, έναν γεννήτορα του $\mathbb{Z}_p^*$, τον g=2 και το τυχαίο χ $x = 135$ και στέλνει στον Μπομπ την τριάδα:

   $(2357, 2 , 2^{135} \bmod 2357) = (2357 , 2 , 641)$[8].

2. Ο Μπομπ επιλέγει ένα τυχαίο y =111 και στέλνει στην Αλίκη το μήνυμα:

   $(2^{111} \bmod 2357) = 1238.$

3. Ο Μπομπ λαμβάνει το μήνυμα της Αλίκης και υπολογίζει το κλειδί:

   $K= 641^{111} \bmod 2357 = 787.$

4. Η Αλίκη λαμβάνει το μήνυμα του Μπομπ και υπολογίζει το κλειδί:

   $K=1238^{135} \bmod 2357 = 787.$

3.3.2 Το Κρυπτοσύστημα ElGamal

Ο El Gamal πρότεινε το 1985 ένα κρυπτοσύστημα δημοσίου κλειδιού του οποίου η ασφάλεια στηρίζεται στη δυσκολία επίλυσης των DLP και DHP στην ομάδα $\mathbb{Z}_p^*$.

[8] : Αυτό μπορεί να θεωρηθεί το δημόσιο κλειδί της Αλίκης.

Το βλέπουμε παρακάτω

Κρυπτοσύστημα 3.1: ElGamal

- **Δημιουργία κλειδιού**

  Για να δημιουργήσει η **A** το δημόσιο και το αντίστοιχο ιδιωτικό κλειδί της ακολουθεί τα εξής βήματα :

  1. Επιλέγει κατάλληλα έναν μεγάλο πρώτο αριθμό p και ένα γεννήτορα g του $\mathbf{Z}_p^*$.
  2. Επιλέγει έναν τυχαίο ακέραιο a, ώστε $1 \le a \le p-2$,και υπολογίζει :
     $$b = g^a \bmod p \ .$$
  3. Το δημόσιο κλειδί της **A** είναι το (p,g,b) και το ιδιωτικό της κλειδί είναι το α .

  Ο Β θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στην **A**. Ακολουθεί την εξής διαδικασία :

- **Κρυπτογράφηση** : Ο **B** πρέπει να κάνει τα παρακάτω

  1. Βρίσκει το "αυθεντικό" δημόσιο κλειδί της **A ,**δηλαδή (p,g,b) .
  2. Κωδικοποιεί το μήνυμα έτσι ώστε να εκφράζεται ως $m \in \mathbf{Z}$ με $0 \le m \le p-1$.
  3. Επιλέγει έναν τυχαίο $k \in \mathbf{Z}$ με $1 \le k \le p-2$
  4. Υπολογίζει :
     $$\begin{cases} c_1 = g^k \pmod p \\ c_2 = m \cdot b^k \pmod p \end{cases}$$
  5. Στέλνει στην **A** το κρυπτογραφημένο κείμενο $c = (c_1, c_2)$

- **Αποκρυπτογράφηση**

  Η **A** για να ανακτήσει το απλό κείμενο m από το c κάνει τα εξής :

  1. Χρησιμοποιεί το ιδιωτικό της κλειδί α, για να υπολογίσει το
     $$c_1^{-\alpha} (= g^{-\alpha k}).$$
  2. Ανακτά το m υπολογίζοντας το :
     $$c_1^{-\alpha} \cdot c_2 \pmod p = g^{-\alpha k} m g^{\alpha k} \pmod p = m \pmod p.$$

Υποθέτουμε ότι η **A** θέλει να επικοινωνήσει λαμβάνοντας κείμενα κρυπτογραφημένα με το ElGamal. Το πρώτο πράγμα που πρέπει να κάνει είναι να δημιουργήσει ένα κατάλληλο δημόσιο (public) κλειδί και το αντίστοιχο ιδιωτικό (private). Στη συνέχεια η **A** μπορεί είτε να δημοσιεύσει το κλειδί της σε μια λίστα *με δημόσια κλειδιά* είτε να το στείλει απευθείας σε εκείνους με τους οποίους θέλει να επικοινωνήσει
(*κάτι τέτοιο απαιτεί βέβαια και τη χρήση μίας ασφαλούς ψηφιακής υπογραφής, για την πιστοποίηση ταυτότητας, ώστε ο παραλήπτης να είναι βέβαιος ότι το μήνυμα προήλθε από την **A** και περιέχει το δικό της δημόσιο κλειδί)*.

Παρατηρήσεις :

1. Αρχικά παρατηρούμε ότι το μήνυμα c που στέλνει ο **B** στην **A** δεν είναι παρά το απλό κείμενο m που φοράει μία "μάσκα" *(εννοούμε τον πολλαπλασιασμό του με το* $b^k \bmod p$*)* , ήτοι το c_2, και ένα στοιχείο για το τυχαίο k, ήτοι το c_1, που θα χρησιμοποιήσει η **A** για να βγάλει την "μάσκα" από το απλό κείμενο.

Εδώ παρατηρούμε και το πρώτο μειονέκτημα του El Gamal , το οποίο είναι η διόγκωση του μηνύματος m. Συγκεκριμένα το κρυπτογραφημένο μήνυμα $c = (c_1, c_2)$ θα περιέχει διπλάσιο όγκο πληροφορίας από ότι το καθαρό m.

2. Για τον υπολογισμό του $c_1^{\,-a}$ στο βήμα **(1)** της αποκρυπτογράφησης η **A** αρκεί να υπολογίσει το $c_1^{\,p-1-\alpha} = c_1^{\,-\alpha}$.

3. (Ασφάλεια του ElGamal)

- Το πρόβλημα του "σπασίματος" του κρυπτοσυστήματος El Gamal, δηλαδή το πρόβλημα ανάκτησης του καθαρού μηνύματος m δοθέντων των

$$\text{g, p, } b\left(=g^a\right),\ c_1\left(=g^k\right),\ c_2\left(=m\cdot g^{a\cdot k}\right)$$

αποδεικνύεται ότι είναι ισοδύναμο[9] με το DHP . Αυτό σημαίνει ότι εάν κάποιος αντίπαλος μπορεί να λύσει το DHP τότε μπορεί και να "σπάσει" και το El Gamal και αντίστροφα. *(βλέπε [Talbot],7.4)*
Συνεπώς η ασφάλεια του El gamal στηρίζεται στη δυσκολία επίλυσης του DHP.

- Παρατηρούμε όμως ότι το πρόβλημα της εξαγωγής του ιδιωτικού κλειδιού της **A** από το δημόσιο κλειδί της , δηλαδή ο υπολογισμός του α από την τριάδα (p,g,b) είναι ακριβώς το πρόβλημα DLP.

[9] : Εννοούμε ότι το ένα πρόβλημα είναι ισοδύναμο κατά Turing με το άλλο, δηλαδή ανάγονται το ένα στο άλλο σε πολυωνυμικό χρόνο .

Συνεπώς εάν κάποιος αντίπαλος μπορεί να λύσει το DLP τότε μπορεί να ανακαλύψει το ιδιωτικό κλειδί της **A** και επομένως μπορεί να αποκρυπτογραφήσει τα μηνύματα που έχει υποκλέψει ακριβώς όπως θα έκανε η **A.**
Άρα η ασφάλεια του El Gamal προφανώς στηρίζεται και στο πρόβλημα DLP το οποίο είναι μάλιστα το πολύ το ίδιο δύσκολο με το DHP (Αφού ισχύει $CDH \propto_p DLP$).

4. Τυχαιοποιημένη κρυπτογράφηση

- Η *Συνάρτηση Κρυπτογράφησης* του ElGamal είναι *τυχαιοποιημένη (randomized)*. Με τον όρο αυτό εννοούμε ότι η Συνάρτηση Κρυπτογράφησης εξαρτάται από τον τυχαία επιλεγμένο ακέραιο k. Έτσι από ένα Απλό Κείμενο μπορούν να προκύψουν πολλά διαφορετικά κρυπτογραφημένα κείμενα, γεγονός που αυξάνει την ασφάλεια του. Στην πράξη όμως η τυχαιοποιημένη αυτή συνάρτηση μπορεί να μετατραπεί σε ντετερμινιστική ακόμη και από ένα παθητικό αντίπαλο . Αυτό συμβαίνει γιατί συνήθως σαν g χρησιμοποιείται ο γεννήτορας μιας υποομάδας G της $\mathbf{Z}_p^*$ με

$$|G| = |\langle g \rangle| = r << p$$

για λόγους αποδοτικότητας.

Σε αυτή την περίπτωση αν το καθαρό μήνυμα $m \notin \langle g \rangle$ τότε ένας αντίπαλος ο οποίος έχει υποκλέψει το $c_2 \left(= m \cdot g^{a \cdot k}\right)$ μπορεί να υπολογίσει :

$$c_2^r = m^r \bmod p\,.$$

Δηλαδή να μετατρέψει το τυχαιοποιημένο κρυπτογραφικό σχήμα σε μια ντετερμινιστική εκδοχή.

Ειδικά στην περίπτωση όπου το μήνυμα m είναι μικρό και παραγοντοποιείται εύκολα

ο αντίπαλος μπορεί να υπολογίσει το μήνυμα σε μικρό χρόνο. *(βλέπε [Mao],8.13.1)*

Συμπερασματικά εάν το μήνυμα m δεν ανήκει στην ομάδα που παράγεται από το g τότε μπορεί να υπονομευτεί η ασφάλεια του κρυπτοσυστήματος ElGamal.

- Επίσης είναι πολύ σημαντικό να επιλέγονται διαφορετικοί τυχαίοι k για κάθε κρυπτογραφημένο κείμενο που στέλνεται. Αν υποθέσουμε ότι το ίδιο k χρησιμοποιείται για να κρυπτογραφηθούν δύο μηνύματα m και m΄ τότε τα αντίστοιχα κρυπτογραφημένα μηνύματα θα είναι (c_1, c_2) και (c'_1, c'_2). Τότε είναι

$$c_2 / c'_2 = m/m'$$

και το m’ εύκολα μπορεί να υπολογιστεί εάν το m είναι γνωστό.

5. Επίθεση από ενεργητικό αντίπαλο

Η ασφάλεια του ElGamal μπορεί να υπονομευθεί από έναν ενεργητικό αντίπαλο ,την Eve , εάν κάποιες προϋποθέσεις ισχύουν. Δίνουμε ένα παράδειγμα :

Προϋπόθεση :

Εάν η αποκρυπτογράφηση από την Alice ενός μηνύματος , έχει ως αποτέλεσμα ένα μήνυμα χωρίς νόημα (μοιάζει τυχαίο) τότε η Alice επιστρέφει το "τυχαίο" αυτό μήνυμα στον αποστολέα του.

Αν ισχύει η παραπάνω προϋπόθεση , τότε η Eve μπορεί να ανακτήσει οποιοδήποτε καθαρό μήνυμα m έχοντας υποκλέψει το κρυπτοκείμενο που αντιστοιχεί σε αυτό.

Διαδικασία :

-Έστω ότι η Eve έχει υποκλέψει το κρυπτοκείμενο $c = (c_1, c_2)$ το οποίο έχει στείλει ο Bob στην Alice.

-Εάν η Eve θέλει να ανακαλύψει το αντίστοιχο καθαρό μήνυμα m, διαλέγει έναν τυχαίο $r \in \mathbf{Z}_p^*$ και υπολογίζει

$$c'_2 = r \cdot c_2 \bmod p \ .$$

Έπειτα στέλνει το κρυπτοκείμενο $c' = (c_1, c'_2)$ στην Alice . Το αποτέλεσμα της αποκρυπτογράφησης από την Alice θα είναι :

$$c_1^{-\alpha} \cdot c'_2 \,(\bmod p) = g^{-\alpha k} r \cdot m g^{\alpha k} \,(\bmod p) = r \cdot m (\bmod p)$$

το οποίο θα μοιάζει χωρίς νόημα στην Alice , αφού ο πολλαπλασιασμός με το τυχαίο r μεταθέτει τυχαία τα πιθανά στοιχεία m πάνω στην $\mathbf{Z}_p^*$.

Έτσι , σύμφωνα με την προϋπόθεση η Alice θα επιστρέψει το :

$$m' = r \cdot m \ (\bmod p)$$

στην Eve . Η Eve ξέροντας το r εύκολα υπολογίζει :

$$m = r \cdot m \cdot r^{-1} (\bmod p) \ .$$

6. Τέλος η κατάλληλη επιλογή του p, που αναφέρουμε στην δημιουργία δημοσίου κλειδιού, συνίσταται σε επιλογή ενός πρώτου αριθμού με τουλάχιστον έναν «μεγάλο» πρώτο παράγοντα και μέγεθος μεγαλύτερο από 768 bits
(ένας ακέραιος k παριστάνεται στον υπολογιστή (στο δυαδικό σύστημα) με $\lfloor \log_2 n \rfloor + 1$ *bit).*

Στο παράδειγμα που ακολουθεί γίνεται μία επίδειξη της λειτουργίας του κρυπτοσυστήματος ElGamal για μικρές παραμέτρους.

Παράδειγμα 3.5:

Δημιουργία Κλειδιού **:**

Η Αλίκη επιλέγει τον p = 2579 και τον γεννήτορα a = 2 του Z_{2579}^{*}. Στη συνέχεια επιλέγει το ιδιωτικό της κλειδί α = 765 και υπολογίζει το

$$g^a \bmod p = 2^{765} \bmod 2579 = 949 \ .$$

Το δημόσιο κλειδί της Αλίκης είναι το : $(p, g, g^a) = (2579, 2, 949)$.

Κρυπτογράφηση **:**

Έστω τώρα ότι ο Μπομπ θέλει να στείλει στην Αλίκη το μήνυμα m = 1299. Για να το κρυπτογραφήσει επιλέγει έναν τυχαίο k, έστω k = 853, και υπολογίζει τα :

$c_1 = 2^{853} \bmod 2579 = 435$ και $c_2 = 1299 \cdot 949^{853} \bmod 2579 = 2396$.

Στέλνει λοιπόν στην Αλίκη το μήνυμα : $c = (c_1, c_2) = (435, 2396)$.

Αποκρυπτογράφηση **:**

Η Αλίκη λαμβάνει το c και υπολογίζει το :

$$g^{p-1-a} = 435^{1813} \bmod 2579 = 1980$$

και τέλος ανακτά το m υπολογίζοντας το :

$$m = (1980 \cdot 2396) \bmod 2579 = 1299 \ .$$

3.3.3 Το Κρυπτοσύστημα των Massey-Omura

Ένα ακόμα λιγότερο γνωστό κρυπτοσύστημα που στηρίζεται στο DLP εισήχθη από τους James L. Massey και Jim K. Omura *(στο κρυπτοσύστημα αυτό δεν υπάρχει δημόσιο κλειδί για τις δύο πλευρές που επικοινωνούν, δεν είναι όμως συμμετρικό και η επικοινωνία γίνεται δημόσια, γι' αυτό και το εξετάζουμε στην ενότητα αυτή)*.

Παρακάτω περιγράφεται η διαδικασία που θα πρέπει να ακολουθήσουν η **A** και ο **B** για να επικοινωνήσουν με ασφάλεια, χρησιμοποιώντας *το Κρυπτοσύστημα των Massey-Omura*.

Κρυπτοσύστημα 3.2: Massey-Omura

- **Δημιουργία κλειδιών**

1. Αρχικά επιλέγεται κατάλληλα ένα πεπερασμένο σώμα $\mathbf{Z}_q$.

2. Στη συνέχεια και οι δύο πλευρές επιλέγουν από έναν τυχαίο (κρυφό) ακέραιο e, με

$$e \in [\,0,\, q-1\,],$$

τέτοιο ώστε ΜΚΔ(e, q – 1) = 1 και υπολογίζουν τον αντίστροφο του

$$d = e^{-1} \bmod q-1$$

(π.χ. με χρήση του εκτεταμένου ευκλείδειου αλγόριθμου). Έστω ότι (e_A, d_A) οι επιλογές της **A** και (e_B, d_B) οι επιλογές του **B.**

Υποθέτουμε ότι η **A** θέλει να στείλει στον **B** το κείμενο m κρυπτογραφημένο με το Massey-Omura. Η διαδικασία που ακολουθεί είναι η παρακάτω:

- **Ανταλλαγή μηνύματος**

1. Η **A** υπολογίζει :

$$m_A = m^{e_A}$$ και το στέλνει στον **B**.

2. Ο **B** λαμβάνει το m_A ,υπολογίζει :

$$m_{AB} = (m_A)^{e_B} = m^{e_A e_B}$$ και το στέλνει στην **A**.

3. Η **A** λαμβάνει το m_{AB} και αφαιρεί από αυτό τον εκθέτη e_A υψώνοντάς το στη δύναμη d_A. Δηλαδή υπολογίζει :

$$m_B = (m_{AB})^{d_A}$$ και το στέλνει στον **B**.

4. Ο **B** ανακτά το m από το m_B υπολογίζοντας :

$$m = (m_B)^{d_B}.$$

Παρατηρήσεις :

1. Παρατηρούμε ότι σε κανένα βήμα της παραπάνω διαδικασίας δεν είναι δυνατό για τον **B** να υπολογίσει το κλειδί της **A** (ήτοι το e_A), αφού κάτι τέτοιο ισοδυναμεί με επίλυση του DLP στο Z_q^*.

2. Επίσης είναι πολύ σημαντικό για τη σωστή λειτουργία του κρυπτοσυστήματος να χρησιμοποιείται μαζί με ένα καλό *Σχήμα Υπογραφής*. Σε αντίθετη περίπτωση είναι δυνατόν κάποιος αντίπαλος που έχει υποκλέψει το m_A, να προσποιηθεί πως είναι ο **B** και να στείλει στην **A** το $m_{AC} = m^{e_A e_C}$. Η **A** μη γνωρίζοντας την υποκλοπή θα συνεχίσει τη διαδικασία που θα επιτρέψει στον αντίπαλο να διαβάσει το m.

Κεφάλαιο 4:

Βασική θεωρία ελλειπτικών καμπυλών

4.1 Εισαγωγή στις ελλειπτικές καμπύλες, εξισώσεις Weierstrass

Οι ελλειπτικές καμπύλες, ως αντικείμενο της θεωρίας αριθμών και της αλγεβρικής γεωμετρίας, έχουν μελετηθεί για περισσότερο από έναν αιώνα και η θεωρία που έχει αναπτυχθεί γύρω τους είναι ιδιαίτερα πλούσια σε αποτελέσματα. Ωστόσο, την τελευταία δεκαετία το ενδιαφέρον της ακαδημαϊκής κοινότητας για της ελλειπτικές καμπύλες έχει αυξηθεί σημαντικά, τόσο λόγω των εφαρμογών τους στην κρυπτογραφία, όσο και της άμεσης σχέσης της θεωρίας ελλειπτικών καμπυλών με την απόδειξη του θεωρήματος του Fermat. Η εφαρμογή τους στην κρυπτογραφία προτάθηκε ανεξάρτητα το 1985 από δύο ερευνητές τον Neal Koblitz του πανεπιστημίου της Ουάσιγκτον και τον Victor Miller από την IBM.

Στο κεφάλαιο αυτό, θα κάνουμε μία στοιχειώδη εισαγωγή στη θεωρία ελλειπτικών καμπυλών, ενώ σε επόμενο κεφάλαιο θα εξετάσουμε τις κυριότερες εφαρμογές της στην κρυπτογραφία .

- **Ορισμός 4.1 Ελλειπτική Καμπύλη E πάνω σε ένα σώμα F**

Μια ***ελλειπτική καμπύλη*** **E** πάνω σε ένα σώμα F, ορίζεται από την παρακάτω εξίσωση η οποία καλείται ***γενικευμένη εξίσωση Weirstrass*** :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (4.1)$$

όπου $a_1, a_2, a_3, a_4, a_6 \in \mathsf{F}$.

Συμβολίζουμε με $E(\mathsf{F})$ το σύνολο των σημείων $(x, y) \in \mathsf{F} \times \mathsf{F}$ τα οποία ικανοποιούν την εξίσωση (4.1) μαζί με ένα σημείο που ονομάζεται "***σημείο στο άπειρο***[10]**"** (point at infinity) και θα το συμβολίζουμε με ∞.

[10] : Ο όρος σημείο στο άπειρο προέρχεται από τις αναπαραστάσεις των καμπυλών στο επίπεδο.

Έχουμε δηλαδή

$$E(\mathsf{F}) = \left\{(x,y) \in \mathsf{F} \times \mathsf{F} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \bigcup \{\infty\}$$

Για να είναι η καμπύλη (4.1) μία ελλειπτική καμπύλη θα πρέπει να είναι **ομαλή** (ή μη ιδιάζουσα**) .**

Παρατηρήσεις**:**

1. Αν γράψουμε την σχέση (4.1) στη μορφή $F(x,y) = 0$, δηλαδή $F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ τότε ένα σημείο (x,y) της καμπύλης θα λέγεται **ομαλό** (ή μη ιδιάζον) αν τουλάχιστον μία από τις μερικές παραγώγους $\partial F / \partial x, \partial F / \partial y$ είναι μη μηδενική στο (x,y).
2. Για να είναι η καμπύλη $F(x,y) = 0$ **ομαλή** πρέπει όλα τα σημεία $(x,y) \in E\left(\overline{\mathsf{F}}\right)$ [11] να είναι ομαλά. Δηλαδή δεν υπάρχει σημείο $(x,y) \in E\left(\overline{\mathsf{F}}\right)$ τέτοιο ώστε

$$\partial F/\partial x = \partial F/\partial y = 0 \Leftrightarrow a_1y - 3x^2 - 2a_2x - a_4 = 2y + a_1x + a_3 = 0$$

- **Ορισμός 4.2 Διακρίνουσα ελλειπτικής καμπύλης**

Έστω Ε μία καμπύλη πάνω στο F που ορίζεται από τη σχέση (4.1). Η **διακρίνουσα** Δ της καμπύλης Ε ορίζεται ως εξής

$$\left.\begin{aligned} \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^3a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}\right\}$$

- **Θεώρημα**

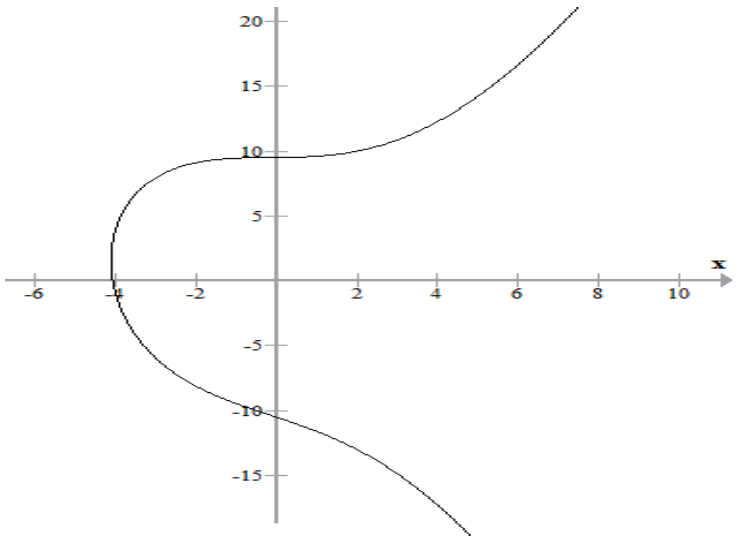
Έστω Ε μία καμπύλη πάνω στο F που ορίζεται από τη σχέση (4.1), Δ η διακρίνουσα της, τότε

$$\text{Ε είναι ομαλή καμπύλη} \Leftrightarrow \Delta \neq 0$$

Άρα, επειδή μια ελλειπτική καμπύλη με διακρίνουσα Δ είναι ομαλή θα πρέπει να ισχύει $\Delta \neq 0$.

[11] : Υπενθυμίζουμε ότι με $\overline{\mathsf{F}}$ συμβολίζουμε την αλγεβρική κλειστότητα του F.

Για να αποκτήσουμε μια γεωμετρική εικόνα δίνουμε παρακάτω τη γραφική παράσταση μιας ελλειπτικής καμπύλης πάνω στο .



Σχήμα 4.1

Η ελλειπτική καμπύλη E: $y^2 + xy + y = x^3 + \frac{1}{2}x^2 + 10x + 100$ πάνω στο .

Ειδικές περιπτώσεις ελλειπτικών καμπυλών

- **Σώμα F με χαρακτηριστική 2 ή 3** **(**$Char(\mathsf{F}) = 2$ **ή** $Char(\mathsf{F}) = 3$**)**

- Αν το F είναι ένα σώμα χαρακτηριστικής 2, τότε μία ελλειπτική καμπύλη πάνω από το F είναι το "σημείο στο άπειρο" μαζί με το σύνολο των σημείων $(x, y) \in \mathsf{F} \times \mathsf{F}$ τα οποία ικανοποιούν είτε μία εξίσωση της μορφής[12] :

$$y^2 + cy = x^3 + ax + b \quad \text{με} \quad a, b, c \in \mathsf{F} \tag{4.2}$$

την οποία καλούμε **υπεριδιάζουσα (supersingular)** μορφή.

είτε της μορφής

$$y^2 + xy = x^3 + ax^2 + b \quad \text{με} \quad a, b \in \mathsf{F} \tag{4.3}$$

την οποία καλούμε **κανονική (non-supersingular ή ordinary)** μορφή.
Η οποία είναι μη-ιδιάζουσα εάν $b \neq 0$.

[12] : Για τους μετασχηματισμούς των εξισώσεων βλέπε [*Cohen, 13.3*]

- Αν το F είναι σώμα χαρακτηριστικής 3, τότε μία ελλειπτική καμπύλη πάνω από το F είναι το σύνολο των σημείων $(x,y)\in \mathsf{F}\times\mathsf{F}$, τα οποία ικανοποιούν μία εξίσωση της μορφής

$$y^2 = x^3 + ax^2 + bx + c \quad \text{με} \quad a,b,c \in \mathsf{F} \tag{4.4}$$

μαζί με το "σημείο στο άπειρο". Επίσης τα a,b,c πρέπει να ικανοποιούν τη συνθήκη ομαλότητας της καμπύλης.

- **Σώμα F με** $Char(\mathsf{F}) \neq 2,3$

-Τότε στην περίπτωση μιας ελλειπτικής καμπύλης πάνω στο F η εξίσωση (4.1) μετατρέπεται στην πιο απλή

$$y^2 = x^3 + ax + b \tag{4.5}$$

με $a,b \in \mathsf{F}$, η οποία καλείται **εξίσωση *Weierstrass***

-Η συνθήκη ομαλότητας της καμπύλης είναι ισοδύναμη με τη συνθήκη μη ύπαρξης πολλαπλών ριζών στο πολυώνυμο $3^{ου}$ βαθμού $x^3 + ax + b$. Αυτό ισχύει αν και μόνον αν η διακρίνουσα Δ του $x^3 + ax + b$ είναι διάφορη του μηδενός.

Αν οι ρίζες της κυβικής εξίσωσης είναι r_1, r_2, r_3, τότε μπορεί να δειχθεί ότι η διακρίνουσα της είναι :

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4a^3 + 27b^2)$$

επομένως η σχέση

$$4a^3 + 27b^2 \neq 0 \tag{4.6}$$

είναι ισοδύναμη με την συνθήκη ομαλότητας της καμπύλης.

Άρα έχουμε ότι μια ελλειπτική καμπύλη πάνω στο F είναι το σύνολο των σημείων $(x,y)\in \mathsf{F}\times\mathsf{F}$, τα οποία ικανοποιούν μία εξίσωση της μορφής

- $y^2 = x^3 + ax + b$ με
- $4a^3 + 27b^2 \neq 0$ και $a,b \in \mathsf{F}$

μαζί με το σημείο στο άπειρο ∞.

Στη συνέχεια θα αναπτύξουμε τη θεωρία χρησιμοποιώντας κυρίως ελλειπτικές καμπύλες ορισμένες σε σώμα F με $Char(\mathsf{F}) \neq 2,3$.

Παρατηρήσεις

1. Η εξίσωση (4.4) προκύπτει από τα εξής :

- Αν η χαρακτηριστική του σώματος δεν είναι 2, τότε μπορούμε να διαιρέσουμε κατά μέλη την (4.1) με το 2 και να συμπληρώσουμε το τετράγωνο :

$$\left(y+\frac{a_1x}{2}+\frac{a_3}{2}\right)^2 = x^3+(a_2+\frac{a_1^{\,2}}{4})x^2+\left(a_4+\frac{a_1a_3}{2}\right)x+\left(\frac{a_3^2}{4}+a_6\right)$$

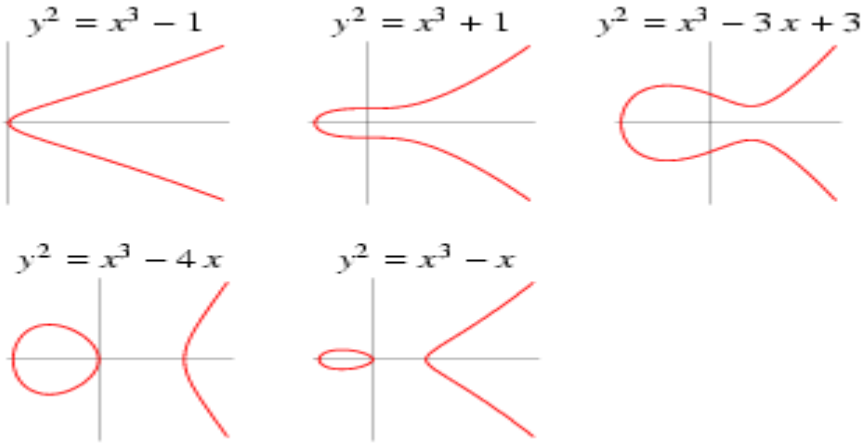
το οποίο μπορεί να γραφεί ως :

$$y_1^{\,2} = x^3+a_2'x^2+a_4'x+a_6'$$

με $y_1 = y+\frac{a_1x}{2}+\frac{a_3}{2}$ και με κάποιες σταθερές a_2', a_4', a_6'.

- Αν επίσης η χαρακτηριστική δεν είναι 3, τότε μπορούμε να θέσουμε $x_1 = x+\frac{a_2'}{3}$ και να έχουμε $y_1^{\,2} = x_1^{\,3}+ax_1+b$, για κάποιες σταθερές α, $b \in \mathsf{F}$ οπότε καταλήγουμε στην εξίσωση (4.4)

2. Μία ελλειπτική καμπύλη που αναπαρίσταται από μια εξίσωση της μορφής (4.5) είναι συμμετρική ως προς τον άξονα των x.



Σχήμα 4.2
Παραδείγματα ελλειπτικών καμπυλών για διάφορες τιμές των α και b.

Η βασική ιδιότητα των ελλειπτικών καμπυλών που τις κάνει πολύτιμα κρυπτογραφικά εργαλεία είναι πως μας δίνουν με φυσικό τρόπο αβελιανές ομάδες με δομή τέτοια ώστε το πρόβλημα DLP να είναι υπολογιστικά δύσκολο. Πιο συγκεκριμένα το σύνολο των σημείων μιας ελλειπτικής καμπύλης Ε εφοδιασμένο με μία πράξη πρόσθεσης (την οποία ορίζουμε παρακάτω) αποτελεί αβελιανή ομάδα, την οποία συμβολίζουμε με G(E) και της οποίας το ουδέτερο στοιχείο είναι το ∞"σημείο στο άπειρο" που προαναφέραμε.

4.2 Σημείο στο άπειρο

Για τεχνικούς λόγους, είναι χρήσιμο να συμπεριλάβουμε σε μία ελλειπτική καμπύλη ένα ***"σημείο στο άπειρο"***. Το θεωρούμε να είναι το σημείο (∞,∞), που συνήθως συμβολίζεται απλά με ∞, και το οποίο τοποθετείται στην κορυφή του άξονα των y. Μία ευθεία θα περνάει από το ∞, ακριβώς αν αυτή είναι κάθετη στον άξονα των x (δηλαδή, $x = $σταθερό).

Θα κάνουμε άλλη μία παραδοχή όσον αφορά το ∞ : Αυτό δεν βρίσκεται μόνο στην κορυφή αλλά και στο τέλος του άξονα των y. Πιο συγκεκριμένα, θεωρούμε τα άκρα του άξονα των y να αναδιπλώνονται και να συναντώνται (ας σκεφτούμε κάπου πίσω από τη σελίδα) στο σημείο στο άπειρο.

Επίσης, έχουμε δεχτεί ότι δύο κατακόρυφες ευθείες συναντώνται στο ∞. Λόγω συμμετρίας, εάν συναντώνται στην κορυφή του άξονα των y, θα πρέπει να συναντώνται και στο τέλος. Αλλά, δύο ευθείες, ως γνωστόν, τέμνονται σε ένα και μοναδικό σημείο, έτσι η "κορυφή ∞" και το "τέλος ∞" πρέπει αναγκαστικά να ταυτίζονται.

Συμπερασματικά, το σημείο στο άπειρο είναι εξ' ορισμού το ουδέτερο στοιχείο της ομάδας $G(\varepsilon)$, ενώ γραφικά είναι το τρίτο σημείο τομής μεταξύ της ελλειπτικής καμπύλης και κάθε κατακόρυφης ευθείας.

Ένας πιο αυστηρός τρόπος να εισάγουμε το σημείο στο άπειρο είναι ο ακόλουθος :

Στο σύνολο των τριάδων (X,Y,Z), τα οποία δεν είναι όλα ταυτόχρονα μηδέν, θεωρούμε τη σχέση ισοδυναμίας : $(X,Y,Z) \sim (\lambda X,\lambda Y,\lambda Z)$, δηλαδή δύο τριάδες είναι ισοδύναμες αν η μία είναι βαθμωτό πολλαπλάσιο της άλλης. Μία κλάση ισοδυναμίας $[(X,Y,Z)]$ λέγεται **προβολικό σημείο**. Ονομάζουμε **προβολικό επίπεδο** το σύνολο των προβολικών σημείων. Αν ένα σημείο (X,Y,Z) έχει $Z \neq 0$ τότε υπάρχει μοναδικό σημείο $(x,y,1)$, τέτοιο ώστε $(X,Y,Z) \in [(x,y,1)]$ (απλά θέτουμε $x = X/Z$, $y = Y/Z$). Επομένως, θα μπορούσαμε να πούμε πως το προβολικό επίπεδο περιέχει όλα τα σημεία (x,y) του συνήθους (αφφινικού)

επιπέδου, καθώς και τα σημεία για τα οποία $Z = 0$. Τα τελευταία βρίσκονται πάνω σε μία ευθεία, την αποκαλούμενη επ' άπειρον ευθεία.

Κάθε εξίσωση καμπύλης $F(x, y) = 0$ στο αφφινικό επίπεδο, αντιστοιχεί σε μία εξίσωση $F(X, Y, Z) = 0$, που ικανοποιείται από τα αντίστοιχα προβολικά σημεία : απλά αντικαθιστούμε το x με X / Z, το y με Y / Z και πολλαπλασιάζουμε με κατάλληλη δύναμη του Z. Για παράδειγμα, αν εφαρμόσουμε αυτήν τη διαδικασία στην εξίσωση $y^2 = x^3 + ax + b$ (1), θα πάρουμε την αντίστοιχη "προβολική εξίσωση" $Y^2 Z = X^3 + aXZ^2 + bZ^3$. Η τελευταία ικανοποιείται προφανώς για κάθε σημείο $(\mathrm{X}, \mathrm{Y}, Z)$ για το οποίο το $(\mathrm{X} / Z, \mathrm{Y} / Z)$ ικανοποιεί την (1).

Ας εξετάσουμε ωστόσο ποια σημεία της επ' άπειρον ευθείας ικανοποιούν την εξίσωση. Θέτοντας $Z = 0$, η εξίσωση γίνεται $0 = X^3$, δηλαδή $X = 0$. Όμως, η μόνη κλάση ισοδυναμίας με $X = Z = 0$ είναι το προβολικό σημείο $[0,1,0]$. Ακριβώς αυτό το σημείο αποκαλούμε "σημείο στο άπειρο". Το ∞ δηλαδή είναι το σημείο τομής του άξονα $y'y$ με την επ' άπειρον ευθεία.

4.3 Πρόσθεση Σημείων σε μία Ελλειπτική Καμπύλη

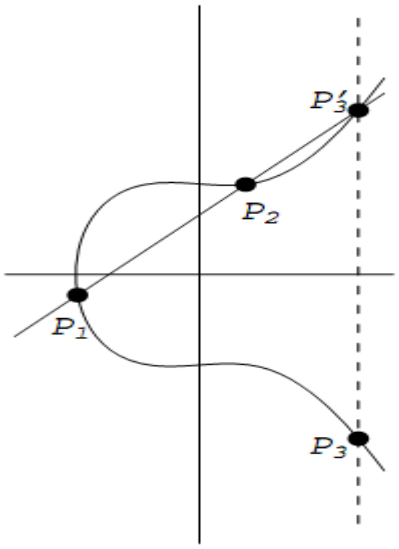
Σε αυτό το σημείο θα χρησιμοποιήσουμε ελλειπτικές καμπύλες πάνω στο προκειμένου να δοθεί ένας γεωμετρικός ορισμός της πρόσθεσης των σημείων και να γίνει διαισθητικά σαφές ότι αυτά αποτελούν αβελιανή ομάδα. Έτσι σε όσα ακολουθούν σε αυτήν την υποενότητα μία ελλειπτική καμπύλη θα είναι μια συνήθης καμπύλη στο επίπεδο μαζί με το "σημείο στο άπειρο".

Ας ξεκινήσουμε με δύο σημεία : $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$ σε μία ελλειπτική καμπύλη E που δίνεται από την εξίσωση (4.4), δηλαδή $y^2 = x^3 + ax + b$.

Ορίζουμε ένα καινούριο σημείο $P_3 \in E$ ως εξής :

Σχεδιάζουμε την ευθεία L που διέρχεται από τα P_1 και P_2. Θα δούμε παρακάτω ότι η L τέμνει την E σε ένα τρίτο σημείο P_3'. Βρίσκουμε το συμμετρικό του P_3' ως προς τον άξονα των x (δηλαδή, το σημείο με την ίδια τετμημένη και αντίθετη τεταγμένη από το P_3') και παίρνουμε το σημείο P_3. Το σημείο P_3 ανήκει στην Ε επειδή η Ε είναι συμμετρική ως προς τον άξονα των x.

Ορίζουμε : $P_1 + P_2 = P_3$.



Σχήμα 4.3
Πρόσθεση σημείων σε μία ελλειπτική καμπύλη

Να σημειώσουμε εδώ ότι η πρόσθεση σημείων σε μία ελλειπτική καμπύλη είναι μία τελείως διαφορετική διαδικασία από το να προσθέτουμε συντεταγμένες σημείων.

Παράδειγμα 4.1 :

Έστω Ε η καμπύλη που δίνεται από τη σχέση : $y^2 = x^3 + 73$ (1).

Έστω $P_1 = (2,9)$ και $P_2 = (3,10)$.

Η ευθεία μεταξύ των P_1 και P_2 βρίσκουμε ότι είναι η $y = x + 7$.

Αντικαθιστώντας στη σχέση (1) έχουμε :

$(x+7)^2 = x^3 + 73$, το οποίο δίνει

$x^3 - x^2 - 14x + 24 = 0$.

Αφού η L τέμνει την Ε στα P_1 και P_2, ήδη γνωρίζουμε δύο ρίζες, τις $x = 2$ και $x = 3$. Επιπλέον, το άθροισμα των τριών ριζών είναι ίσο με τον αντίθετο του συντελεστή του x^2, οπότε θα είναι ίσο με 1. Αν x είναι η τρίτη ρίζα, τότε

$2 + 3 + x = 1,$

έτσι το τρίτο σημείο τομής θα είναι το $x = -4$.

Αφού $y = x + 7$, έχουμε $y = 3$, και $Q = (-4,3)$.
Παίρνοντας το συμμετρικό ως προς τον $x'x$, έχουμε :

$$(2,9)+(3,10)=P_3=(-4,-3)\,.$$ W

Επανερχόμενοι τώρα στην πρόσθεση σημείων, διακρίνουμε τις εξής περιπτώσεις :

1. Υποθέτουμε πρώτα ότι $P_1 \neq P_2$ και κανένα από αυτά δεν είναι το ∞. Σχεδιάζουμε την ευθεία L μεταξύ των P_1 και P_2. Ο συντελεστής διεύθυνσης της L είναι :

$$m=\frac{y_2-y_1}{x_2-x_1}\,.$$

Αν $x_1=x_2$, τότε η L είναι κατακόρυφη.

Θα ασχοληθούμε με αυτήν την περίπτωση αργότερα, γι' αυτό υποθέτουμε ότι $x_1 \neq x_2$. Η εξίσωση της L είναι τότε :

$$y=m(x-x_1)+y_1\,.$$

Για να βρούμε την τομή με την E, αντικαθιστούμε ώστε να πάρουμε :

$$(m(x-x_1)+y_1)^2=x^3+ax+b\,.$$

Αυτό μπορεί να μετασχηματιστεί στη μορφή

$$0=x^3-m^2x^2+... \qquad (*)$$

Οι τρεις ρίζες αυτής της κυβικής εξίσωσης αντιστοιχούν στα τρία σημεία τομής της L με την E .

Γενικά, το να λύσουμε μία κυβική εξίσωση δεν είναι εύκολο, αλλά στην παρούσα περίπτωση, ήδη γνωρίζουμε δύο από τις ρίζες, συγκεκριμένα τις x_1 και x_2, αφού τα P_1 και P_2 είναι σημεία και στην L αλλά και στην E. Γι' αυτό το λόγο, μπορούμε να παραγοντοποιήσουμε την κυβική εξίσωση ώστε να αποκτήσουμε την τρίτη τιμή του x. Αλλά υπάρχει ένας πιο εύκολος τρόπος :

Υπενθυμίζουμε ότι το άθροισμα S των ριζών του πολυωνύμου

$$a_n x^n a_{n-1}x^{n-1}+...+a_1+a_0$$

ισούται με $-a_{n-1}/a_n$.

Οπότε σε ένα κυβικό πολυώνυμο της μορφής (*) με ρίζες r,s,t έχουμε

Οπότε, $S = r + s + t = m^2$.

Αν γνωρίζουμε δύο ρίζες r, s, τότε μπορούμε να εξάγουμε την τρίτη, ως $t = S - r - s$.

Στην δική μας περίπτωση, έχουμε :

$$x = m^2 - x_1 - x_2 \quad \text{και} \quad y = m(x - x_1) + y_1 .$$

Τώρα, παίρνουμε το συμμετρικό ως προς τον $x'x$ και έχουμε το σημείο $P_3 = (x_3, y_3)$:

$$\left.\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}\right\}$$

2. Στην περίπτωση όπου $x_1 = x_2$ αλλά $y_1 \neq y_2$, η ευθεία μεταξύ των P_1 και P_2 είναι μία κατακόρυφη ευθεία, η οποία, οπότε, τέμνει την Ε στο ∞ (διότι τοποθετούμε το ∞ και στην κορυφή και στο τέλος του άξονα $y'y$). Συνεπώς, σε αυτήν την περίπτωση : $P_1 + P_2 = \infty$.

3. Τώρα θεωρούμε την περίπτωση όπου $P = P_1 = P_2 = (x_1, y_1)$. Όταν δύο σημεία σε μία καμπύλη είναι πολύ κοντά το ένα με το άλλο, η ευθεία μεταξύ τους προσεγγίζει την εφαπτομένη.
Τότε ο συντελεστής διεύθυνσης της L είναι η παράγωγος $\frac{dy}{dx}$ στο Ρ. Επομένως παίρνουμε από το θεώρημα πεπλεγμένης συνάρτησης:

$$2y\frac{dy}{dx} = 3x^2 + a \ , \ \text{οπότε} \ \ m = \frac{dy}{dx} = \frac{3x_1^{\,2} + a}{2y_1} .$$

- Αν $y_1 = 0$, τότε η ευθεία είναι κατακόρυφη και θέτουμε $P_1 + P_2 = \infty$, όπως πριν.
- Αν $y_1 \neq 0$, η εξίσωση της L είναι $y = m(x - x_1) + y_1$, όπως πριν.

Προκύπτει η κυβική εξίσωση : $0 = x^3 - m^2 x^2 + \ldots$.
Αυτήν τη φορά, γνωρίζουμε μόνο μία ρίζα, την x_1, αλλά αυτή είναι διπλή ρίζα αφού η L είναι εφαπτόμενη στην Ε στο P_1.
Οπότε, ενεργώντας όπως πριν, έχουμε :

$$\left.\begin{aligned} x_3 &= m^2 - 2x_1 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}\right\}$$

Σε αυτή την περίπτωση εάν το Ρ είναι σημείο καμπής της καμπύλης Ε τότε το μοναδικό σημείο τομής της L με την Ε θα είναι το Ρ οπότε αν προσθέσουμε το Ρ στον εαυτό του παίρνουμε το συμμετρικό του ως προς τον άξονα των x.

4. Τέλος, υποθέτουμε $P_2 = \infty$. Η ευθεία μεταξύ P_1 και ∞ είναι μία κατακόρυφη ευθεία που τέμνει την Ε στο σημείο P_1', που είναι το συμμετρικό του P_1 ως προς τον $x'x$. Όταν παίρνουμε το συμμετρικό του P_1' ως προς τον άξονα των x για να προκύψει το $P_3 = P_1 + P_2$, καταλήγουμε πάλι στο P_1.
Οπότε, $P_1 + \infty = P_1$ για όλα τα σημεία P_1 στην Ε.

Φυσικά, αυτό επεκτείνεται ώστε να συμπεριλάβουμε επίσης ότι : $\infty + \infty = \infty$.

Μπορούμε να συνοψίσουμε τα παραπάνω ως εξής :

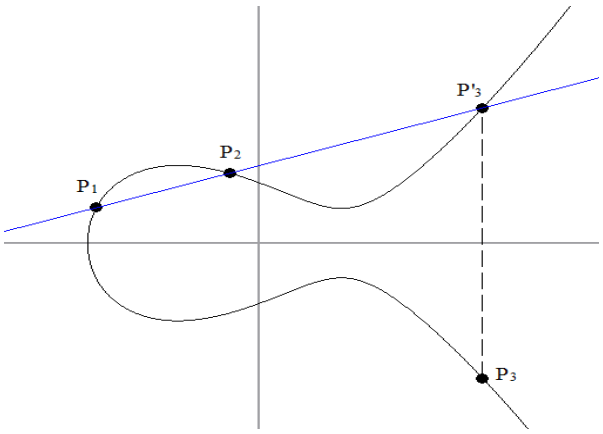
Προσθετικός Νόμος :

Έστω Ε μία ελλειπτική καμπύλη που ορίζεται από την $y^2 = x^3 + ax + b$.

Έστω $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$ σημεία στην Ε με $P_1,\ P_2 \neq \infty$.

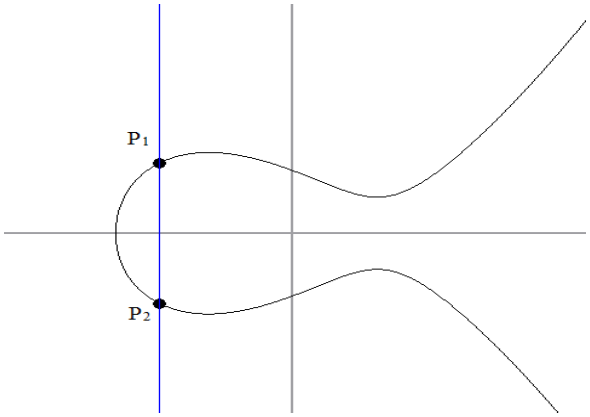
Ορίζουμε $P_1 + P_2 = P_3 = (x_3, y_3)$ ως εξής :

1. Αν $x_1 \neq x_2$, τότε
$x_3 = m^2 - x_1 - x_2$,
$y_3 = m(x_1 - x_3) - y_1$, όπου $m = \dfrac{y_2 - y_1}{x_2 - x_1}$.



Σχήμα 4.4

2. Αν $x_1 = x_2$ αλλά $y_1 \neq y_2$, τότε $P_1 + P_2 = \infty$.

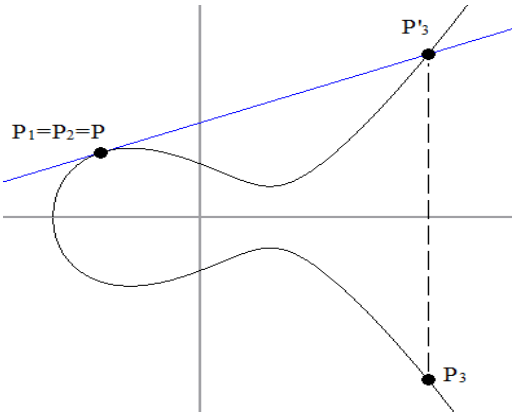


Σχήμα 4.5

3. Αν $P_1 = P_2 = P$ και $y_1 \neq 0$ τότε

$x_3 = m^2 - 2x_1 - x_2$

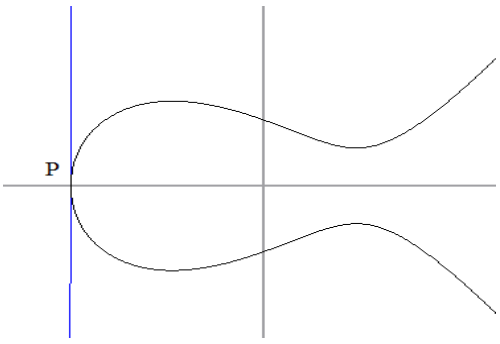
$y_3 = m(x_1 - x_3) - y_1$, όπου $m = \dfrac{3x_1^{\,2} + A}{2y_1}$.



Σχήμα 4.6

4. Αν $P_1 = P_2 = P$ και $y_1 = 0$ τότε $P_1 + P_2 = \infty$.

Επιπλέον, ορίζουμε $P + \infty = P$ για όλα τα σημεία P στην Ε.



Σχήμα 4.7

Παρατήρηση **:**

Όταν έχουμε $E(\mathsf{F})$ $Char(\mathsf{F}) = 2$ 3 τότε οι τύποι τις πρόσθεσης διαφέρουν λίγο αλλά προκύπτουν με παρόμοιο τρόπο.

- **Θεώρημα**

Η πρόσθεση σημείων σε μία ελλειπτική καμπύλη Ε ικανοποιεί τις παρακάτω ιδιότητες :

1. *(αντιμεταθετική)* $P_1 + P_2 = P_2 + P_1$ για όλα τα P_1, P_2 στην E.

2. *(ύπαρξη ουδέτερου στοιχείου)* $P + \infty = P$ για όλα τα σημεία P στην E.

3. *(ύπαρξη αντίστροφων)* Για δεδομένο σημείο P στην E, υπάρχει P' στην E με $P + P' = \infty$. Το σημείο P' συνήθως θα συμβολίζεται με $-P$.

4. *(προσεταιριστική)* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ για όλα τα P_1, P_2, P_3 στην E.

Με άλλα λόγια, τα σημεία στην E σχηματίζουν μία προσθετική αβελιανή ομάδα με το σημείο στο άπειρο να είναι το ουδέτερο στοιχείο.

4.4 Πολλαπλασιασμός ακεραίου επί σημείο

Έχοντας ορίσει την πράξη της πρόσθεσης στην ομάδα των σημείων μιας ελλειπτικής καμπύλης, μπορεί να οριστεί μία ακόμη πράξη, αυτή του πολλαπλασιασμού ενός σημείου με έναν ακέραιο αριθμό. Έστω k ένας και P ένα σημείο σε μια ελλειπτική καμπύλη. Τότε, ο πολλαπλασιασμός του ακεραίου k με το σημείο P ορίζεται ως εξής:

$$kP = \begin{cases} \sum_{j=1}^{k} P & \alpha\nu\ k > 0 \\ 0 & \alpha\nu\ k = 0 \\ \sum_{j=1}^{k} -P & \alpha\nu\ k < 0 \end{cases}$$

Το αποτέλεσμα δηλαδή αυτού του πολλαπλασιασμού είναι άλλο ένα σημείο στην ελλειπτική καμπύλη.

Για να υπολογίσουμε το kP για ένα μεγάλο ακέραιο k, δεν είναι αποδοτικό να προσθέσουμε το P στον εαυτό του επαναλαμβανόμενα. Ο πιο απλός αποδοτικός αλγόριθμος βασίζεται στη δυαδική αναπαράσταση του k . Αναφέρεται και σαν ***διαδοχικός διπλασιασμός***.

Για παράδειγμα, για να υπολογίσουμε το $19P$, υπολογίζουμε

$$2P,\ 4P = 2P + 2P,\ 8P = 4P + 4P,\ 16P = 8P + 8P,\ 19P = 16P + 2P + P.$$

Αυτή η μέθοδος , μας επιτρέπει να υπολογίσουμε το kP για πολύ μεγάλο k, για παράδειγμα, αρκετών εκατοντάδων ψηφίων, πολύ γρήγορα. Η μόνη δυσκολία είναι ότι το μέγεθος των συντεταγμένων των σημείων αυξάνεται ταχύτατα εάν εργαζόμαστε στους πραγματικούς αριθμούς.

Ωστόσο, όταν εργαζόμαστε σε ένα πεπερασμένο σώμα, για παράδειγμα στο F_p, αυτό δεν αποτελεί πρόβλημα, διότι μπορούμε να ανάγουμε συνεχώς $\bmod p$ και επομένως να διατηρήσουμε τους αριθμούς που εμπλέκονται, σχετικά μικρούς.

Ας σημειώσουμε ότι ο προσεταιριστικός νόμος μας επιτρέπει να κάνουμε αυτούς τους υπολογισμούς χωρίς να ανησυχούμε για την σειρά που θα χρησιμοποιήσουμε για να συνδυάσουμε τους προσθετέους.

Έστω k ένας θετικός ακέραιος και έστω P ένα σημείο σε μία ελλειπτική καμπύλη. Ο ακόλουθος αλγόριθμος υπολογίζει το Q= kP :

Σημειώνουμε ότι

Αλγόριθμος 4.1 : Διαδοχικός διπλασιασμός

1. $Q = 0$

2. Όσο ισχύει $(k > 0)$ κάνε

3. Αν $k = 1 \bmod 2$ (*k περιττός*)

4. $Q := Q + P$

5. $k := k - 1$

6. $P := P + P$

7. $k := k/2$

8. Επέστρεψε Q

Στον αλγόριθμο έχουμε διαδοχικές διαιρέσεις με το 2 του αριθμού k, προφανώς

Πολυπλοκότητα χρόνου: $O(\log k)$

Αντιθέτως, αν εργαζόμαστε σε ένα μεγάλο πεπερασμένο σώμα και δίνονται τα σημεία P και kP, είναι πολύ δύσκολο να προσδιορίσουμε την τιμή του k. Αυτό καλείται

Πρόβλημα του Διακριτού Λογαρίθμου για ελλειπτικές καμπύλες και αποτελεί την βάση για πολλές κρυπτογραφικές εφαρμογές που θα συζητηθούν παρακάτω.

Παραδείγματα 4.1 :

1. Στην ελλειπτική καμπύλη : $y^2 = \frac{x(x+1)(2x+1)}{6}$ υπολογίζουμε το άθροισμα

- $(0,0)+(1,1)$

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1-0}{1-0} = 1$$

$$x_3 = m^2 - x_1 - x_2 = 1^2 - 0 - 1 = 0$$

$$y_3 = m(x_1 - x_3) - y_1 = 1(0-0) = 0$$

άρα : $(0,0)+(1,1) = (0,\ 0)$

W

2. Στην ελλειπτική καμπύλη : $y^2 = x^3 - 25x$ να υπολογιστούν τα παρακάτω :

- $2(-4,6)$

Ελέγχω ότι το (-4,6) ανήκει στην καμπύλη.

$$m = \frac{3x_1^{\ 2} + a}{2y_1} = \frac{3(-4)^2 - 25}{2 \cdot 6} = \frac{23}{12}$$

$$x_3 = m^2 - 2x_1 = \left(\frac{23}{12}\right)^2 + 8 = \frac{1681}{144}$$

$$y_3 = m(x_1 - x_3) - y_1 = \frac{23}{12}\left(-4 - \frac{1681}{144}\right) - 6 = -\frac{62279}{1728}$$

W

- $(0,0)+(-5,0)$

$$m = \frac{y_2 - y_1}{x_2 - x_1} = 0$$

$$x_3 = m^2 - x_1 - x_2 = 5$$

$$y_3 = m(x_1 - x_3) - y_1 = 0$$

W

- $2(0,0) = \infty = 2(-5,0) = 2(5,0)$

Επειδή $P_1 = P_2$ και $y_1 = 0$.

W

3. Στην ελλειπτική καμπύλη : $y^2 = x^3 - 36x$ έστω τα σημεία :

- $P_1 = (-3,9)$ και $P_2 = (-2,8)$

Θα έχουμε $m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-9}{-2+3} = -1$

$x_3 = m^2 - x_1 - x_2 = 1+3+2 = 6$

$y_3 = m(x_1 - x_3) - y_1 = -1(-3-6)+9=0$

άρα $P_1 + P_2 = (6,0)$.

W

- $2(-3,9)$

$$m = \frac{3x_1^{\,2} + A}{2y_1} = \frac{3 \cdot 9 - 36}{2 \cdot 9} = \frac{-9}{2 \cdot 9} = -\frac{1}{2}$$

$$x_3 = m^2 - 2x_1 = \frac{1}{4} + 2 \cdot 3 = \frac{25}{4}$$

$$y_3 = m(x_1 - x_3) - y_1 = -\frac{1}{2}\left(-3 - \frac{25}{4}\right) - 9 = -\frac{35}{8}$$

άρα : $x_3 = m^2 - 2x_1 = \left(\frac{23}{12}\right) + 8 = \frac{1681}{144}$. W

Κεφάλαιο 5:

Ελλειπτικές Καμπύλες πάνω σε Πεπερασμένα Σώματα

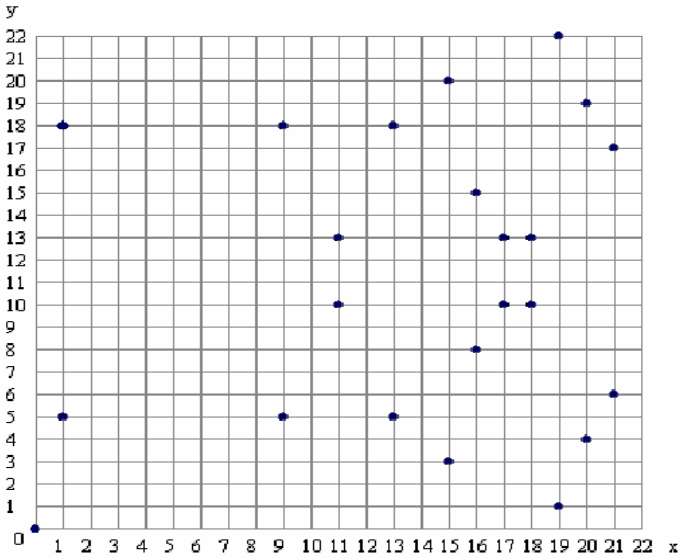
5.1 Ελλειπτικές Καμπύλες πάνω σε Πεπερασμένα Σώματα

Υπενθύμιση

- **Τάξη** ενός σώματος F ονομάζεται το πλήθος των στοιχείων του F.
- **Πεπερασμένο σώμα** καλείται ένα σώμα πεπερασμένης τάξης**.**
- Ένα σώμα τάξης q υπάρχει αν και μόνον αν το q είναι δύναμη πρώτου, δηλαδή $q=p^n$, $n \in \mathbb{N}$ και p: πρώτος. (Το θεώρημα αυτό οφείλεται στον E.Galois)
- Δύο σώματα της ίδιας τάξης είναι ισομορφικά, δηλαδή για κάθε δύναμη πρώτου υπάρχει ακριβώς ένα πεπερασμένο σώμα το οποίο συμβολίζουμε με F_{p^n} *ή* $GF\left(p^n\right)$.
- **Χαρακτηριστική** του σώματος F_{p^n} καλείται το p.

Στο εξής θα θεωρούμε κάθε ελλειπτική καμπύλη E ορισμένη πάνω στο πεπερασμένο σώμα F_q, όπου $q=p^n$ και p: πρώτος. Την συμβολίζουμε με $E\left(\mathsf{F}_q\right)$. Ανάλογα με τη χαρακτηριστική του σώματος F_q η E δίνεται από τις εξισώσεις (4.2),(4.3), (4.4), (4.5) του προηγούμενου κεφαλαίου.

Η εικόνα της $E\left(\mathsf{F}_q\right)$ είναι κάπως έτσι:



Σχήμα 5.1: Η ελλειπτική καμπύλη E: $y^2 = x^3 + x$ πάνω στο F_{23}.

Εύκολα παρατηρούμε πως μια ελλειπτική καμπύλη $E\left(\mathsf{F}_q\right)$ έχει το πολύ 2q+1 σημεία, το σημείο ∞ μαζί με 2q ζεύγη (x, y), $x, y \in \mathsf{F}_q$, που ικανοποιούν την εξίσωση της E. Αυτό συμβαίνει επειδή για κάθε ένα από τα q πιθανά x υπάρχουν το πολύ δύο ώστε να ικανοποιείται η εξίσωση της E. Καθώς μόνο τα μισά από τα στοιχεία του F_q έχουν τετραγωνική ρίζα, είναι φυσικό να περιμένουμε ότι υπάρχουν περίπου τα μισά από αυτά τα 2q+1 σημεία στην καμπύλη.

Πιο συγκεκριμένα, το θεώρημα Hasse-Weil συνδέει το πλήθος των σημείων $\#E\left(\mathsf{F}_q\right)$ με το q.

- **Θεώρημα (**Hasse-Weil): Αν $E\left(\mathsf{F}_q\right)$ μια ελλειπτική καμπύλη πάνω στο F_q τότε

$$\#E\left(\mathsf{F}_q\right) = q + 1 - t \quad \kappa\alpha\iota \quad |t| \le 2\sqrt{q}.$$

Παρατηρήσεις :

1. Ο ακέραιος t ονομάζεται **ίχνος του Frobenius**

2. Έστω p πρώτος. Αν το ίχνος του Frobenius είναι ίσο με 1 για μια E, τότε αυτή καλείται **μη ομαλή** (anomalous). **Υπεριδιάζουσα** (supersingular) είναι μια ελλειπτική καμπύλη $E\left(\mathsf{F}_p\right)$ για την οποία ο πρώτος αριθμός p διαιρεί το ίχνος του Frobenius. Οι ελλειπτικές καμπύλες που εμπίπτουν σε αυτές τις δύο κατηγορίες αποφεύγονται σε κρυπτογραφικές εφαρμογές γιατί είναι πολύ ευάλωτες σε επιθέσεις.

3. Έστω p:πρώτος. Για κάθε ακέραιο $t \in \left[-2\sqrt{p}, 2\sqrt{p}\right]$ υπάρχει τουλάχιστον μία ελλειπτική καμπύλη Ε πάνω στο F_p για την οποία $\#E\left(\mathsf{F}_p\right) = p+1-t$, όπου.

- **Θεώρημα**

Έστω q=p^n. Τότε υπάρχει μια ελλειπτική καμπύλη $E\left(\mathsf{F}_q\right)$ με $\#E\left(\mathsf{F}_q\right) = q+1-t$ αν και μόνον αν μία από τις ακόλουθες συνθήκες ισχύει :

1. $t \neq 0 \bmod p \;\; και \;\; t^2 \leq 4q.$

2. Το n είναι περιττός και είτε (i) t=0 είτε (ii) p=2 και $t^2 = 2q$ είτε (iii) p=2 και $t^2 = 3q$

3. Το n είναι άρτιος και είτε (i) $t^2 = 4q$ είτε (ii) $p \neq 1 \bmod 3$ και $t^2 = q$ είτε (iii) $p \neq 1 \bmod 4$ και $t = 0$

5.2 Ελλειπτικές Καμπύλες πάνω στο F_p , όπου p πρώτος (Ελλειπτικές καμπύλες modp)

Αν p πρώτος, μπορούμε να εργαστούμε με ελλειπτικές καμπύλες mod p χρησιμοποιώντας τα ως τώρα γνωστά στοιχεία θεωρίας. Για παράδειγμα, θεωρούμε

$$\text{E}: \; y^2 = x^3 + 4x + 4 \pmod 5.$$

Τα σημεία στην Ε είναι τα ζεύγη $(x, y) \bmod 5$ που ικανοποιούν την εξίσωση, μαζί με το "σημείο στο άπειρο". Οι πιθανές τιμές για το $x \bmod 5$ είναι 0,1,2,3,4. Αντικαθιστούμε καθένα από αυτά στην εξίσωση και βρίσκουμε τις τιμές του y που επιλύουν την εξίσωση :

$$x = 0 \Rightarrow y^2 = 4 \left(\bmod 5\right) \Rightarrow y = 2, 3 \pmod 5$$

$$x = 1 \Rightarrow y^2 = 9 = 4 \left(\bmod 5\right) \Rightarrow y = 2, 3 \pmod 5$$

$$x = 2 \Rightarrow y^2 = 20 = 0 \left(\bmod 5\right) \Rightarrow y = 0 \pmod 5$$

$$x = 3 \Rightarrow y^2 = 43 = 3 \left(\bmod 5\right) \Rightarrow \text{δεν } \exists \text{ λύση}$$

$x = 4 \Rightarrow y^2 = 84 = 4 \pmod 5 \Rightarrow y = 2,3 \pmod 5$

$x = \infty \Rightarrow y = \infty$.

Τα σημεία στην E είναι

(0,2), (0,3), (1,2), (1,3), (2,0), (4,2), (4,3), (∞, ∞). W

Η πρόσθεση σημείων σε μία ελλειπτική καμπύλη mod p γίνεται με τις ίδιες μεθόδους, όπως προηγουμένως, όπου ο ρητός $\frac{a}{b}$ ερμηνεύεται σαν $a \cdot b^{-1}$, όπου $b^{-1}b = 1 \pmod p$. Αυτό απαιτεί $(b, p) = 1$.

Η ελλειπτική καμπύλη mod p είναι λοιπόν, ένα σύνολο σημείων και όχι μία συνεχής καμπύλη όπως είχαμε πάνω στο □ .

Παράδειγμα 5.2 :

Στην ελλειπτική καμπύλη E : $y^2 \equiv x^3 + 4x + 4$ επί του $\square_5$ ας υπολογίσουμε το $(1,2) + (4,3)$:

Ο συντελεστής διεύθυνσης είναι:

$m = \frac{3-2}{4-1} = \frac{1}{3} = 3^{-1} = 2 \pmod 5$ (διότι $2 \cdot 3 = 6 = 1 \bmod 5$) οπότε,

$x_3 = m^2 - x_1 - x_2 = 2^2 - 1 - 4 = -1 = 4 \pmod 5$

$y_3 = m(x_1 - x_3) - y_1 = 2(1-4) - 2 = -8 = -3 \pmod 5 = 2 \pmod 5$

άρα : $(1,2) + (4,3) = (4,2)$. W

Γενικότερα, είναι δυνατόν να αναπτύξουμε μία θεωρία ελλειπτικών καμπυλών $\bmod n$, για κάθε ακέραιο n. Σε αυτήν την περίπτωση, όταν συναντήσουμε ένα κλάσμα $\frac{a}{b}$, χρειάζεται να ισχύει $\gcd(b, n) = 1$.

5.3 Ελλειπτικές Καμπύλες mod n, όπου n σύνθετος

Σε κάποιες περιπτώσεις, χρειάζεται να εργαστούμε με ελλειπτικές καμπύλες mod n, όπου n είναι σύνθετος. Επίσης, να πάρουμε ελλειπτικές καμπύλες πάνω στο και να τις ανάγουμε mod n, όπου n είναι ένας ακέραιος.

Παράδειγμα 5.3 :

Έστω E η ελλειπτική καμπύλη που δίνεται από την σχέση

$y^2 = x^3 - x + 1 \pmod{5^2}$.

Ας υποθέσουμε ότι θέλουμε να υπολογίσουμε το $(1,1) + (21,4)$. Ο συντελεστής διεύθυνσης της ευθείας μεταξύ των δύο σημείων είναι :

$$m = \frac{4-1}{21-1} = \frac{3}{20}.$$

Ο παρονομαστής δεν είναι μηδέν $(\mathrm{mod}\, 25)$, αλλά επίσης δεν είναι υπάρχει ο $20^{-1} \bmod 25$. Οπότε, ο συντελεστής διεύθυνσης δεν είναι ούτε άπειρος ούτε πεπερασμένος $(\mathrm{mod}\, 25)$.
Αν υπολογίσουμε το άθροισμα χρησιμοποιώντας τις μεθόδους για τον προσθετικό νόμο, η x-συντεταγμένη του αθροίσματος είναι :

$$x_3 = m^2 - x_1 - x_2 = \left(\frac{3}{20}\right)^2 - 1 - 21 = \frac{9}{400} - 22 = \frac{8771}{400} \equiv \infty \pmod{25}$$

(Διότι ο παρονομαστής τώρα είναι μηδέν $\bmod 25$)

Αλλά :

$(1,1) + (1,24) = \infty$ οπότε δεν μπορούμε επίσης να έχουμε $(1,1) + (24,1) = \infty$.

Παράδειγμα 5.4 :

Έστω E η ελλειπτική καμπύλη που δίνεται από την σχέση

$$y^2 = x^3 - x + 1 \pmod{35}.$$

Ας υποθέσουμε ότι θέλουμε να υπολογίσουμε το $(1,1) + (26,24)$. Ο συντελεστής διεύθυνσης είναι :

$$m = \frac{24-1}{26-1} = \frac{23}{25},$$

το οποίο είναι $\infty \mod 5$ και πεπερασμένος $\mod 7$.

Κατά μία έννοια, το σημείο είναι "μερικώς" στο ∞. Δεν μπορούμε να το εκφράσουμε σε αφφινικές συντεταγμένες $\mod 35$. Μία λύση είναι να χρησιμοποιήσουμε το Κινέζικο Θεώρημα Υπολοίπων και να γράψουμε :

$$E(\mathbf{Z}_{35}) = E(\mathbf{Z}_5) \oplus E(\mathbf{Z}_7),$$

και μετά να εργαστούμε $\mod 5$ και $\mod 7$ ξεχωριστά. Αυτή η στρατηγική αποδίδει στην παρούσα περίπτωση αλλά όχι και στο προηγούμενο παράδειγμα.

5.4 Τάξη της ομάδας

Το θεώρημα του Hasse θέτει όρια για το πλήθος των σημείων σε μία ελλειπτική καμπύλη πάνω σε ένα πεπερασμένο σώμα. Θα αναπτύξουμε μερικές μεθόδους που θα καθορίζουν την τάξη της ομάδας αυτής.

5.4.1 Σύμβολα Legendre

Για να κατασκευάσουμε μία λίστα σημείων στην $y^2 = x^3 + Ax + B$ πάνω σε ένα πεπερασμένο σώμα, δοκιμάσαμε κάθε πιθανή τιμή του x και μετά βρήκαμε τις τετραγωνικές ρίζες y του $x^3 + Ax + B$, αν υπήρχαν. Αυτή η διαδικασία είναι η βάση για έναν απλό αλγόριθμο καταμέτρησης σημείων.

Το ***σύμβολο Legendre*** $\left(\frac{x}{p}\right)$ για έναν πρώτο p, ορίζεται ως εξής :

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \alpha\nu \;\; t^2 \equiv x \pmod p \;\; \acute{\varepsilon}\chi\varepsilon\iota \;\; \mu\acute{\iota}\alpha \;\; \lambda\acute{\upsilon}\sigma\eta \; t \neq 0 \pmod p \\ -1 & \alpha\nu \;\; t^2 \equiv x \pmod p \;\; \delta\varepsilon\nu \;\; \acute{\varepsilon}\chi\varepsilon\iota \;\; \lambda\acute{\upsilon}\sigma\eta \; t \\ 0 & \alpha\nu \;\; x \equiv 0 \pmod p \end{cases}.$$

Αυτό μπορεί να γενικευθεί σε οποιοδήποτε πεπερασμένο σώμα $\mathbf{F}_q$ με q περιττό εξ' ορισμού, για $x \in \mathbf{F}_q$,

$$\left(\frac{\mathrm{x}}{\mathbf{F}_q}\right) = \begin{cases} +1 & \alpha\nu \;\; t^2 = x \;\; \acute{\varepsilon}\chi\varepsilon\iota \;\; \mu\acute{\iota}\alpha \;\; \lambda\acute{\upsilon}\sigma\eta \;\; t \in \mathbf{F}_q \\ -1 & \alpha\nu \;\; t^2 = x \;\; \delta\varepsilon\nu \;\; \acute{\varepsilon}\chi\varepsilon\iota \;\; \lambda\acute{\upsilon}\sigma\eta \;\; t \in \mathbf{F}_q \\ 0 & \alpha\nu \;\; x = 0 \end{cases}$$

Θεώρημα :

Έστω Ε μία ελλειπτική καμπύλη ορισμένη από τη σχέση $y^2 = x^3 + ax + b$ πάνω στο F_q. Τότε

$$\#E(\mathsf{F}_q) = q + 1 + \sum_{x \in \mathsf{F}_q} \left(\frac{x^3 + Ax + B}{\mathsf{F}_q} \right).$$

Απόδειξη :

Για ένα δοσμένο x_0, υπάρχουν δύο σημεία (x, y) με x-συντεταγμένη x_0 αν $x_0^3 + Ax_0 + B$ είναι ένα μη-μηδενικό τετράγωνο στο F_q, ένα τέτοιο σημείο αν είναι μηδενικό, και καθόλου σημεία αν δεν είναι ένα τετράγωνο. Οπότε, ο αριθμός των σημείων με x-συντεταγμένη x_0 ισούται με

$1 + \left(\frac{x_0^3 + Ax_0 + B}{\mathsf{F}_q} \right)$.Αθροίζοντας για όλα τα $x_0 \in \mathsf{F}_q$ και περιλαμβάνοντας μία μονάδα για το σημείο ∞, προκύπτει :

$$\#E(\mathsf{F}_q) = 1 + \sum_{x \in \mathsf{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathsf{x}\ \mathsf{F}_q} \right) \right).$$

Και παίρνοντας τον όρο 1 από κάθε έναν από τους q προσθετέους, προκύπτει ο ζητούμενος τύπος. W

Παρατήρηση :

Το θεώρημα αυτό, που μερικές φορές είναι γνωστό ως *μέθοδος Lang-Trotter*, δουλεύει γρήγορα για μικρές τιμές του q, q <100 ίσως, αλλά είναι αργό για μεγαλύτερο q, και είναι αδύνατο να χρησιμοποιηθεί όταν το q είναι γύρω στο 10^{100} ή μεγαλύτερο.

Πόρισμα :

Έστω $x^3 + Ax + B$ ένα πολυώνυμο με $A, B \in \mathsf{F}_q$, όπου q είναι περιττός. Τότε :

$$\left| \sum_{x \in \mathsf{F}_q} \left(\frac{x^3 + Ax + B}{\mathsf{x}\ \mathsf{F}_q} \right) \right| \leq 2\sqrt{q} \ .$$

Απόδειξη :

Όταν το $x^3 + Ax + B$ δεν έχει πολλαπλές ρίζες, το $y^2 = x^3 + Ax + B$ δίνει μία ελλειπτική καμπύλη, οπότε από το προηγούμενο θεώρημα :

$$q + 1 - \#E(\mathsf{F}_q) = -\sum_{x \in \mathsf{F}_q} \left(\frac{x^3 + Ax + B}{\mathsf{x}\ \mathsf{F}_q} \right)$$

Το αποτέλεσμα τώρα έπεται από το θεώρημα του Hasse. W

Παράδειγμα 5.5 :

Έστω Ε η ελλειπτική καμπύλη $y^2 = x^3 + x + 1$ πάνω στο F_5.

Τα μη μηδενικά τετράγωνα mod 5 είναι 1 και 4. Οπότε :

$$\#E(\mathsf{F}_5) = 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{5} \right) = 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right)$$

και σύμφωνα με τον ορισμό του συμβόλου Legendre :

$$\#E(\mathsf{F}_5) = 6 + 1 - 1 + 1 + 1 + 1 = 9 \ .$$

5.4.2 Τάξη Σημείου

Έστω $P \in E(\mathsf{F}_q)$. Η ***τάξη*** του P είναι ο μικρότερος θετικός ακέραιος k τέτοιος ώστε $kP = \infty$.

- Ένα θεμελιώδες αποτέλεσμα της θεωρίας Ομάδων (πόρισμα του θεωρήματος Lagrange) είναι ότι η τάξη ενός σημείου διαιρεί την τάξη της ομάδας $E(\mathsf{F}_q)$.

- Επίσης, για έναν ακέραιο n, έχουμε $nP = \infty$ αν και μόνον αν η τάξη του P διαιρεί τον n. Από το θεώρημα του Hasse, το $\#E(\mathsf{F}_q)$ κείται σε ένα διάστημα μήκους $4\sqrt{q}$. Οπότε, εάν μπορούμε να βρούμε ένα σημείο τάξης μεγαλύτερης από $4\sqrt{q}$, μόνο ένα πολλαπλάσιο αυτής της τάξης μπορεί να υπάρχει στο σωστό διάστημα, και πρέπει να είναι το $\#E(\mathsf{F}_q)$. Ακόμη και αν η τάξη του σημείου είναι μικρότερη από $4\sqrt{q}$, αποκτούμε μία μικρή λίστα πιθανοτήτων για το $\#E(\mathsf{F}_q)$. Χρησιμοποιώντας λίγα περισσότερα σημεία, συχνά μειώνεται αρκετά η λίστα, ώστε να υπάρχει μία μοναδική πιθανότητα για το $\#E(\mathsf{F}_q)$.

Πώς βρίσκουμε την τάξη ενός σημείου ;

Εάν γνωρίζουμε την τάξη όλης της ομάδας των σημείων, τότε μπορούμε να εξετάσουμε τους παράγοντες αυτής της τάξης. Αλλά, εδώ, η τάξη της ομάδας είναι αυτή που προσπαθούμε να βρούμε. Παρακάτω, θα αναπτύξουμε μία μέθοδο (Baby Step, Giant Step) για να βρίσκουμε την τάξη ενός σημείου.

Παράδειγμα 5.6:

Έστω E η ελλειπτική καμπύλη $y^2 = x^3 + 7x + 1$ πάνω στο F_{101}. Είναι δυνατόν να δείξουμε ότι το σημείο (0, 1) έχει τάξη 116, έτσι $\mathrm{N}_{101} = \#\mathrm{E}(\mathsf{F}_{101})$ είναι ένα πολλαπλάσιο του 116. Σύμφωνα με το θεώρημα του Hasse :

$$101+1-2\sqrt{101} \le \mathrm{N}_{101} \le 101+1+2\sqrt{101},$$

το οποίο σημαίνει ότι

$$82 \le \mathrm{N}_{101} \le 122 \ .$$

Το μόνο πολλαπλάσιο του 116 σε αυτό το εύρος είναι το 116, έτσι $\mathrm{N}_{101} = 116$.

Άρα, το (0, 1) εφόσον έχει τάξη 116 είναι ο γεννήτορας της κυκλικής ομάδας τάξης 116. W

Παράδειγμα 5.7 :

Έστω E η ελλειπτική καμπύλη $y^2 = x^3 - 10x + 21$ πάνω στο F_{557}. Μπορεί να δειχθεί ότι το σημείο (2, 3) έχει τάξη 189. Από το θεώρημα του Hasse έπεται ότι :

$$511 \le \mathrm{N}_{557} \le 605.$$

Το μόνο πολλαπλάσιο του 189 σε αυτό το εύρος είναι $3 \cdot 189 = 567$.

Άρα $\mathrm{N}_{557} = 567$.

Παράδειγμα 5.8 :

Έστω E η ελλειπτική καμπύλη $y^2 = x^3 + 7x + 12$ πάνω στο F_{103}. Το σημείο (-1, 2) έχει τάξη 13 και το σημείο (19, 0) έχει τάξη 2. Οπότε, η τάξη N_{103} του $\mathrm{E}(\mathsf{F}_{103})$ είναι ένα πολλαπλάσιο του 26. Το θεώρημα του Hasse συνεπάγεται ότι

$$84 \le \mathrm{N}_{103} \le 124 .$$

Το μόνο πολλαπλάσιο του 26 σε αυτό το εύρος είναι το 104, έτσι $\mathrm{N}_{103} = 104$. W

5.4.3 Μέθοδος Baby Step, Giant Step

Έστω $P \in E(\mathsf{F}_q)$. Θέλουμε να βρούμε την τάξη του P. Πρώτα, θέλουμε να βρούμε έναν ακέραιο k τέτοιο ώστε $kP = \infty$. Έστω $\#\mathrm{E}(\mathsf{F}_q) = N$. Από το θεώρημα του Lagrange, $NP = \infty$. Φυσικά, μπορεί ακόμη να μη γνωρίζουμε το N, αλλά γνωρίζουμε ότι :

$$q + 1 - 2\sqrt{q} \le N \le q + 1 + 2\sqrt{q} .$$

Θα μπορούσαμε να δοκιμάσουμε όλες τις πιθανές τιμές του N σε αυτό το διάστημα και να δούμε ποια ικανοποιεί τη συνθήκη $NP = \infty$. Για αυτό θα χρειαστούν γύρω στα $4\sqrt{q}$ βήματα. Ωστόσο, είναι δυνατόν να τα μειώσουμε γύρω στα $4q^{1/4}$ βήματα με τον ακόλουθο αλγόριθμο :

1. Υπολόγισε το $Q = (q+1)P$.

2. Διάλεξε έναν ακέραιο m με $m > q^{1/4}$. Υπολόγισε και αποθήκευσε τα σημεία jP για $j = 0, 1, 2, ..., m$.

3. Υπολόγισε τα σημεία

$$Q + k(2mP) \quad \text{για} \quad k = -m, -(m-1), ..., m$$

ωσότου υπάρχει μία αντιστοίχηση $Q + k(2mP) = \pm j\,\mathrm{P}$ με ένα σημείο (ή με τον αρνητικό του) στην αποθηκευμένη λίστα.

4. Συμπέρανε ότι $(q + 1 + 2mk \pm j)P = \infty$. Έστω $M = q + 1 + 2mk \mp j$.

5. Παραγοντοποίησε το M. Έστω $p_1, p_2, ..., p_r$ να είναι οι διακριτοί πρώτοι

παράγοντες του Μ.

6. Υπολόγισε το $\left(\frac{M}{p_i}\right)P$ για $i=1,2,...,r$.

- Αν $\left(\frac{M}{p_i}\right)P=\infty$ για κάποιο i, αντικατέστησε το Μ με $\frac{M}{p_i}$ και πήγαινε πίσω στο βήμα (5).

- Αν $\left(\frac{M}{p_i}\right)P\neq\infty$ για όλα τα i, τότε Μ είναι η τάξη του σημείου P.

7. Αν ψάχνουμε το $\#E(\mathsf{F}_{qq})$, τότε επανέλαβε τα βήματα (1) - (6) με τυχαία επιλεγμένα σημεία στο $E(\mathsf{F}_q)$ ωσότου το μέγιστο κοινό πολλαπλάσιο των τάξεων να διαιρεί μόνο έναν ακέραιο N με $q+1-2\sqrt{q}\le N\le q+1+2\sqrt{q}$. Τότε $N=E(\mathsf{F}_q)$. W

Υπάρχουν δύο σημεία τα οποία πρέπει να διευκρινιστούν :

I. *Υποθέτοντας ότι υπάρχει μία αντιστοίχηση, αυτή η μέθοδος πράγματι παράγει έναν ακέραιο που είναι η τάξη του P. Αλλά γιατί υπάρχει αντιστοίχηση ;*

Λήμμα :

Έστω a ένας ακέραιος με $|a|\le 2m^2$. Υπάρχουν ακέραιοι a_0 και a_1 με $-m<a_0\le m$ και $-m<a_1\le m$ τέτοιοι ώστε $a=a_0+2ma_1$.

Απόδειξη :

Έστω $a_0\equiv a\pmod{2m}$, με $-m<a_0\le m$ και $a_1=\frac{a-a_0}{2m}$.

Τότε, $|a_1|\le\frac{2m^2+m}{2m}<m+1$.

• Έστω $a=a_0+2ma_1$ να είναι όπως στο παραπάνω λήμμα και έστω $k=-a_1$. Τότε

$$Q+k(2mP)=(q+1-2ma_1)P$$

$$=(q+1-a+a_0)P$$

$$= NP + a_0 P$$

$$= a_0 P = \pm jP$$

όπου $j = |a_0|$. Οπότε, υπάρχει μία αντιστοίχηση. W

II. *Γιατί το βήμα (6) παράγει την τάξη του P ;*

Λήμμα :

Έστω G Μία προσθετική ομάδα (με ουδέτερο στοιχείο το 0) και έστω $g \in G$. Υποθέτουμε ότι $Mg = 0$ για κάποιο θετικό ακέραιο M. Έστω $p_1, p_2, ..., p_r$ να είναι οι διακριτοί πρώτοι που διαιρούν τον M. Αν $\left(\frac{M}{p_i}\right) g \neq 0$ για όλα τα i, τότε M είναι η τάξη του g.

Απόδειξη :

Έστω k η τάξη g. Τότε το k διαιρεί το M : k / M. Υποθέτουμε ότι $k \neq M$. Έστω p_i ένας πρώτος που διαιρεί το $\frac{M}{k}$.

Τότε, $p_i \cdot k / M$, έτσι $k /(M / p_i)$. Οπότε, $(M / p_i)g = 0$, άτοπο. Άρα, $k = M$.

Οπότε το βήμα (6) βρίσκει την τάξη του P. W

Παρατηρήσεις :

1. Για εξοικονόμηση μνήμης, θα είναι πιο αποδοτικό να αποθηκεύουμε μόνο τις $x-$συντεταγμένες των σημείων jP (μαζί με τον αντίστοιχο ακέραιο j), αφού αναζητούμε μία αντιστοίχηση με $\pm jP$, απαιτείται μόνο η $x-$συντεταγμένη (υποθέτοντας ότι εργαζόμαστε με μία εξίσωση Weierstrass). Όταν έχει βρεθεί μία αντιστοίχηση, οι δύο πιθανές $y-$συντεταγμένες μπορούν να υπολογισθούν ξανά.

2. Ο υπολογισμός του $Q + k(2mP)$ μπορεί να γίνει υπολογίζοντας το Q και $2mP$ μόνο μία φορά. Για να πάμε από το $Q + k(2mP)$ στο $Q + (k+1)(2mP)$, απλά προσθέτουμε $2mP$, αντί να ξανα-υπολογίζουμε το καθετί. Παρόμοια, από τη

στιγμή που έχει υπολογισθεί το jP μία φορά, προσθέτουμε το P για να πάρουμε το $(j+1)P$.

3. Υποθέτουμε ότι μπορούμε να παραγοντοποιήσουμε το M. Αν όχι, μπορούμε τουλάχιστον να βρούμε όλους τους μικρούς πρώτους παράγοντες p_i και να ελέγξουμε αν $\left(\frac{M}{p_i}\right)P \neq \infty$ για αυτούς. Τότε το M θα είναι ένας καλός υποψήφιος για την τάξη του P.

4. Γιατί αυτή η μέθοδος καλείται "Baby Step, Giant Step" ;

Τα baby steps είναι τα βήματα από το σημείο jP στο $(j+1)P$. Τα giant steps τα βήματα από το σημείο $k(2mP)$ στο $(k+1)(2mP)$, αφού κάνουμε το "μεγαλύτερο" βήμα 2mP

.

Παράδειγμα 5.9 :

Έστω Ε η ελλειπτική καμπύλη $y^2 = x^3 - 10x + 21$ πάνω στο F_{557} όπως και στο παράδειγμα 3.5. Έστω $P = (2,3)$. Θα ακολουθήσουμε την παραπάνω διαδικασία :

1. $Q = 558P = (418,33)$

2. Έστω $m = 5$ το οποίο είναι μεγαλύτερο από $557^{1/4}$. Η λίστα των jP είναι :

$$\infty, (2,3), (58,164), (44,294), (56,339), (132,364).$$

3. Για $k = 1$ έχουμε $Q + k(2mP) = (2,3)$, το οποίο αντιστοιχεί με το σημείο της λίστας μας για $j = 1$.

4. Έχουμε $(q + 1 + 2mk - j)P = 567P = \infty$.

5. Παραγοντοποιούμε $567 = 3^4 \cdot 7$.

6. Υπολογίζουμε $\left(\frac{567}{3}\right)P = 189P = \infty$.

Τώρα έχουμε το 189 ως υποψήφιο για την τάξη του P. Αφού $189P = \infty$, αντικαθιστούμε το $M = 567$ με $\frac{M}{p_i} = 189$ και πηγαίνουμε πίσω στο βήμα (5), οπότε :

7. Παραγοντοποιούμε 189= $3^3 \cdot 7$. Υπολογίζουμε το $\left(\frac{189}{3}\right)P = (38,535) \neq \infty$

και $\left(\frac{189}{7}\right)P = (136,360) \neq \infty$. Οπότε, 189 είναι η τάξη του P.

Όπως διευκρινίστηκε και στο παράδειγμα 3.5, αυτό επαρκεί για να καθορίσει ότι

$$\#\mathsf{F}_{557} = 567.$$ W

5.4.4 Ο Αλγόριθμος του Schoof

Το 1985, ο Schoof δημοσίευσε έναν αλγόριθμο για τον υπολογισμό των σημείων στις Ελλειπτικές Καμπύλες πάνω σε πεπερασμένα σώματα F_q, ο οποίος «τρέχει» πολύ πιο γρήγορα από τους υπάρχοντες αλγόριθμους, τουλάχιστον για πολύ μεγάλο q. Συγκεκριμένα, απαιτεί το πολύ $k \log^8 q$ bit λειτουργίες (k: σταθερά), σε αντίθεση με τις $q^{1/4}$ που χρησιμοποιούταν στο Baby Step, Giant Step, για παράδειγμα. Στη συνέχεια, οι Atkin και Elkies βελτίωσαν την μέθοδο του Schoof. Έχει χρησιμοποιηθεί τώρα επιτυχώς, όταν το q έχει μερικές εκατοντάδες ψηφία.

Κεφάλαιο 6:

Το Πρόβλημα Διακριτού Λογαρίθμου στις Ελλειπτικές Καμπύλες (ECDLP).

6.1 Ορισμός των προβλημάτων

Έχουμε ήδη δει το DLP στο κεφάλαιο 3, καθώς και κρυπτοσυστήματα βασισμένα στο DLP στην πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος. Ας παρατηρήσουμε όμως ότι αφού η ομάδα $E(\mathsf{F}_q)$, μιας ελλειπτικής καμπύλης Ε πάνω σε ένα πεπερασμένο σώμα F_q , είναι προσθετική, η αντίστοιχη πράξη της ύψωσης σε δύναμη θα αντικατασταθεί από το βαθμωτό γινόμενο. Οπότε το *πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες* (ECDLP) θα είναι το εξής :

Πρόβλημα 6.1 : Πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες (ECDLP)

Δίνεται : Μία ελλειπτική καμπύλη Ε, ορισμένη πάνω στο F_q, ένα σημείο $P \in E\left(\mathsf{F}_q\right)$ (η βάση του διακριτού λογαρίθμου) και ένα άλλο σημείο $Q \in E\left(\mathsf{F}_q\right)$.

Ζητείται : Να βρεθεί, αν υπάρχει, ακέραιος k τέτοιος ώστε : **kP=Q.**

Παρατήρηση :

Το ECDLP φαίνεται να είναι δυσκολότερο από το DLP. Μάλιστα, για το δεύτερο υπάρχει, όπως είδαμε, αλγόριθμος υποεκθετικού χρόνου, ενώ για το πρώτο όχι. Έτσι, αν και δεν υπάρχει απόδειξη, που να μας εξασφαλίζει ότι το ECDLP είναι πράγματι δυσκολότερο από το DLP, με τα σημερινά δεδομένα έχουμε εξίσου καλή ασφάλεια με αρκετά μικρότερο μήκος κλειδιού όταν χρησιμοποιούμε κρυπτοσυστήματα ελλειπτικών καμπυλών.

Αναλόγως μπορούμε να ορίσουμε τα προβλήματα DHP και DDHτου κεφαλαίου 3 πάνω στην προσθετική ομάδα $E(\mathsf{F}_q)$.

Πρόβλημα 6.2 : Υπολογιστικό Diffie-Hellman στις ελλειπτικές καμπύλες (ECDHP)

Δίνεται : Μία ελλειπτική καμπύλη Ε, ορισμένη πάνω στο F_q, ένα σημείο Ρ $\in E\left(\mathsf{F}_q\right)$ (η βάση του διακριτού λογαρίθμου) και δύο άλλα σημεία G,Q $\in E\left(\mathsf{F}_q\right)$ πολλαπλάσια του Ρ. Δηλαδή είναι $G = aP$ και $Q = bP$ για κάποιους $a, b \in \square$.

Ζητείται : Να βρεθεί το σημείο $R = abP$

Πρόβλημα 6.3 : Diffie-Hellman απόφασης στις ελλειπτικές καμπύλες (ECDDH)

Δίνεται : Μία ελλειπτική καμπύλη Ε, ορισμένη πάνω στο F_q, ένα σημείο Ρ $\in E\left(\mathsf{F}_q\right)$ (η βάση του διακριτού λογαρίθμου) και τρία σημεία $Q, R, G \in E\left(\mathsf{F}_q\right)$.

Ζητείται : Αποφάσισε αν υπάρχουν $a, b \in \mathsf{Z}$ τέτοιοι ώστε $aP = Q$, $bP = R$ και $G = abP$.

Παρατηρήσεις :

1. Αποδεικνύεται ότι τα ECDDH,ECDHP,ECDLP ανάγονται πολυωνυμικά το ένα στο άλλο με τη σειρά

$$ECDDH \propto_p ECDHP \propto_p ECDLP$$

Η απόδειξη είναι παρόμοια με αυτή του κεφαλαίου 3 για τα αντίστοιχα προβλήματα στην ομάδα $\square_p^*$.

Για παράδειγμα εάν κάποιος μπορεί να επιλύσει το ECDLP τότε μπορεί να χρησιμοποιήσει το P και το aP για να βρει το a. Έπειτα μπορεί να υπολογίσει το $a(bP)$ και να πάρει το abP και έτσι να έχει λύσει το ECDHP.

Σημειώνεται επίσης ότι δεν είναι γνωστό εάν υπάρχει κάποιος τρόπος να υπολογίσουμε το abP χωρίς να λύσουμε πρώτα το πρόβλημα του διακριτού λογαρίθμου.

2. Παρατηρούμε ότι το σημείο P στον ορισμό των προηγούμενων προβλημάτων παίζει το ρόλο του γεννήτορα g στα αντίστοιχα προβλήματα DLP,DHP,DDH.
Εδώ όμως δεν μας ενδιαφέρει αν το P είναι γεννήτορας της $E\left(\mathsf{F}_q\right)$ η οποία, όπως είπαμε ήδη, πιθανόν να μην είναι κυκλική. Μάλιστα εδώ δεν χρειαζόμαστε ούτε την ακριβή τιμή του $\#E\left(\mathsf{F}_q\right)$. Το μόνο που θέλουμε είναι η κυκλική υποομάδα που παράγεται από το P να είναι μεγάλη, κατά προτίμηση της ίδιας τάξης μεγέθους με την $E\left(\mathsf{F}_q\right)$.

6.2 Αλγόριθμοι επίλυσης του ECDLP

Οι **γενετικοί αλγόριθμοι** που παρουσιάσαμε στο κεφάλαιο 3.2 δουλεύουν σε αυθαίρετες ομάδες. Σε αυτό το κεφάλαιο παρουσιάζουμε τις απαραίτητες τροποποιήσεις οι οποίες πρέπει να γίνουν ώστε οι αλγόριθμοι αυτοί να εφαρμοστούν σε μια ομάδα $E(\mathsf{F}_q)$, μιας ελλειπτικής καμπύλης Ε πάνω σε ένα πεπερασμένο σώμα F_q για να επιλυθεί το ECDLP.

Συγκεκριμένα θεωρούμε την προσθετική ομάδα G= $E(\mathsf{F}_q)$ και $P,Q\in G$ και αναζητούμε έναν ακέραιο k τέτοιο ώστε $kP=Q$. Υποθέτουμε ότι υπάρχει ένα τέτοιο k.
Επίσης υποθέτουμε ότι η τάξη της G, $N=\#G$ είναι γνωστή.

Ο στοιχειώδης αλγόριθμος εδώ είναι η **εξαντλητική μέθοδος αναζήτησης** στην G και απαιτεί O(N) χρόνο και O(1) χώρο.
Υπολογίζω δηλαδή τα $P,2P,3P,,...$ (υπολογίζοντας κάθε φορά $iP=\left(i-1\right)P+P$) μέχρι να βρεθεί $kP=Q$.

Ας δούμε όμως κάποιες πιο αποδοτικές μεθόδους.

6.2.1 Αλγόριθμος του Shanks (ή Baby step/Giant step)

Έστω η προσθετική ομάδα G και έστω $P, Q \in G$. Θέλουμε να λύσουμε την $kP = Q$.

Αλγόριθμος 6.1 : Shanks (Baby step/Giant step)

1. Όρισε έναν ακέραιο $m \geq \sqrt{N}$ και υπολόγισε το mP.

2. Κατασκεύασε και αποθήκευσε μία λίστα από iP για $0 \leq i \leq m$.

3. Υπολόγισε τα σημεία $Q - jmP$ για $j = 0,1,....,m-1$ μέχρι ένα από αυτά να ταιριάζει με ένα στοιχείο από την αποθηκευμένη λίστα.

4. Αν $iP = Q - jmP$, έχουμε $Q = kP$ με $k = i + jm \pmod{N}$.

Παρατηρήσεις :

1. Ο αλγόριθμος μας δίνει το σωστό αποτέλεσμα .
Αφού $m^2 \geq N$, μπορούμε να υποθέσουμε ότι η απάντηση k ικανοποιεί την

$$0 \leq k < m^2.$$

Γράφουμε $k = k_0 + mk_1$ με $k_0 = k \pmod{m}$ και $0 \leq k_0 \leq m$ κι έστω

$$k_1 = (k - k_0)/m \quad .$$

Τότε $0 \leq k_1 \leq m$. Όταν $i = k_0$ και $j = k_1$, έχουμε

$$Q - k_1 mP = kP - k_1 mP = k_0 P ,$$

έτσι υπάρχει ένα ταίριασμα.

2. Το σημείο iP υπολογίζεται προσθέτοντας το P (ένα **"baby step"**) στο (i-1)P. Το σημείο $Q - jmP$ υπολογίζεται προσθέτοντας $-mP$ (ένα **"giant step"**) στο $Q - (j-1)mP$. Η μέθοδος αναπτύχθηκε από τον Shanks για υπολογισμούς στην αλγεβρική θεωρία αριθμών.

3. Ας σημειώσουμε ότι δεν χρειαζόταν να γνωρίζουμε την ακριβή τάξη N του G. Το

μόνο που απαιτήσαμε ήταν ένα άνω φράγμα για το N. Συνεπώς, για ελλειπτικές καμπύλες πάνω στο F_q, θα μπορούσαμε να χρησιμοποιήσουμε αυτήν τη μέθοδο με $m^2 \geq q+1+2\sqrt{q}$, από το θεώρημα του Hasse.

4. Μία μικρή βελτίωση της μεθόδου μπορεί να γίνει για ελλειπτικές καμπύλες υπολογίζοντας και αποθηκεύοντας μόνο τα σημεία iP για $0 \leq i \leq \frac{m}{2}$ και ελέγχοντας αν $Q - jmP = \pm iP$.

5. Τελικά από την ανάλυση του αλγορίθμου έχουμε:

Πολυπλοκότητα χώρου $O\left(\sqrt{N}\right)$

Πολυπλοκότητα χρόνου $O\left(\sqrt{N}\right)$

Παράδειγμα 6.1 :

Έστω $G = E(\mathsf{F}_{41})$, όπου E δίνεται από την $y^2 = x^3 + 2x + 1$.

Έστω P = (0,1) και Q = (30,40).

Από το θεώρημα του Hasse, γνωρίζουμε ότι η τάξη της G είναι το πολύ 54 :

$$N \leq q+1+2\sqrt{q} \;=\; 41+1+2\cdot\sqrt{41} \approx 54.8$$

έτσι, έστω $m = 8$ (αφού $m = \sqrt{N}$).

Τα σημεία iP για $0 \leq i \leq 7$ είναι :

• i = 0 → ∞

• i = 1 → (0,1)

• i = 2 → 2P = P+P

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{2}{2} = 1 \;\Rightarrow\; x = 1^2 - 2\cdot 0 = 1 \quad \text{και} \quad y = -1+1\cdot(0-1) = -1+40 = 39$$

Άρα 2P = (1,39) .

• i = 3 → 3P = 2P+P = (1,39)+(0,1)

$$m = \frac{39-1}{1-0} = 38 \;\Rightarrow\; x = 38^2 - 1 - 0 = 1444 - 1 = 1443 \equiv 8 \bmod 41 \text{ και}$$

$y = 38(0-8)-1 = 33\cdot 38-1 = 1254-1 = 1253 = 23 \bmod 41$.

Άρα 3P = (8,23) .

• i = 4 → 4P = 2P+2P

$$m = \frac{3\cdot 1^2+2}{2\cdot 39} = \frac{5}{78} = \frac{5}{37} = 5\cdot 37^{-1} = 5\cdot 10 = 50 \equiv 9 \bmod 41$$

$\Rightarrow \quad x = 9^2 - 2\cdot 1 = 79 = 38 \bmod 41$ και $y = 9(1-38)-39 = 9\cdot 4-39 = -3 \equiv 38 \bmod 41$

Άρα 4P = (38,38) .

• i = 5 → 5P = P+4P = (0,1)+(38,38)

$$m = \frac{38-1}{38-0} = \frac{37}{38} = 37\cdot 38^{-1} = 37\cdot 27 \equiv 15 \bmod 41$$

$\Rightarrow \quad x = 15^2 - 0 - 38 = 225-38 = 187 = 23 \bmod 41$ και

$y = 15(0-23)-1 = 15\cdot 18-1 = 270-1 = 269 = 23 \bmod 41$.

Άρα 5P = (23,23) .

• i = 6 → 6P = 3P+3P

$$m = \frac{3\cdot 8^2+2}{46} = \frac{194}{5} = 194\cdot 5^{-1} = 194\cdot 33 = 6402 = 6 \bmod 41$$

$\Rightarrow \quad x = 6^2 - 2\cdot 8 = 36-16 = 20$ και $y = 6(8-20)-23 = 6\cdot 29-23 = 151 = 28 \bmod 41$

Άρα 6P = (20,28) .

• i = 7 → 7P = P+6P

$$m = \frac{28-1}{20-0} = \frac{27}{20} = 27\cdot 20^{-1} = 27\cdot 39 \equiv 28 \bmod 41$$

$\Rightarrow$ x=$28^2 - 0 - 20 = 784-20 = 764 \equiv 26 \bmod 41$ και

$y = 28(0-26)-1 = 28\cdot 25-1 = 420-1 = 419 = 9 \bmod 41$.

Άρα 7P = (26,9) .

Οπότε έχουμε :

$$\infty,(0,1),\ (1,39),\ (8,23),\ (38,38),\ (23,23),\ (20,28),\ (26,9).$$

Υπολογίζουμε το $Q - jmP$ για $j = 0,1,2$ και παίρνουμε

$$(30,\ 40)\ ,\ (9,\ 25),\ (26,\ 9)$$

στο οποίο σημείο σταματάμε αφού το τρίτο σημείο ταιριάζει με το $7P$.

Αφού για j = 2, παρήχθη το ταίριασμα, έχουμε :

$$Q = (i + jm)P$$

$$(30,\ 40) = (7 + 2 \cdot 8)\ \mathrm{P} = 23\ \mathrm{P}$$

Συνεπώς, k = 23.

6.2.2 Αλγόριθμος των Pohlig-Hellman

Όπως πριν, P, Q είναι στοιχεία μιας ομάδας G και θέλουμε να βρούμε έναν ακέραιο k με $Q = kP$. Γνωρίζουμε επίσης την τάξη N του P και την παραγοντοποίηση του N σε πρώτους :

$$N = \prod_i q_i^{e_i} \quad .$$

Η ιδέα της μεθόδου Pohlig – Hellman είναι να βρούμε το $k \pmod{q_i^{e_i}}$ για κάθε i, και μετά να χρησιμοποιήσουμε το Κινέζικο Θεώρημα Υπολοίπων και να συνδυάσουμε αυτά για να υπολογίσουμε το $k \pmod{N}$.

Έστω q ένας πρώτος, και έστω q^e να είναι η μεγαλύτερη δύναμη του q που διαιρεί το N. Γράφουμε το k χρησιμοποιώντας ως βάση το q :

$$k = k_0 + k_1 q + k_2 q^2 + \ldots \qquad \text{με} \quad 0 \le k_i \le q\,.$$

Θα υπολογίσουμε το $k \pmod{q^e}$ προσδιορίζοντας διαδοχικά τα $k_0, k_1, \ldots, k_{e-1}$. Η διαδικασία είναι η εξής :

Αλγόριθμος 6.2: Pohlig-Hellman

1. Υπολόγισε το $T = \left\{ j(\frac{N}{q}P) / 0 \le j \le q-1 \right\}$.

2. Υπολόγισε το $\frac{N}{q}Q$. Αυτό θα είναι ένα στοιχείο $k_0(\frac{N}{q}P)$ του T.

3. Αν $e=1$, σταμάτα. Αλλιώς , συνέχισε.

4. Έστω $Q_1 = Q - k_0 P$.

5. Υπολόγισε το $\frac{N}{q^2}Q_1$. Αυτό θα είναι ένα στοιχείο $k_1(\frac{N}{q}P)$ του T.

6. Αν $e=2$, σταμάτα. Αλλιώς, συνέχισε.

7. Υποθέτουμε ότι έχουμε υπολογίσει τα $k_0, k_1, ..., k_{r-1}$, και $Q_1, Q_2, ..., Q_{r-1}$.

8. Έστω $Q_r = Q_{r-1} - k_{r-1}q^{r-1}P$.

9. Καθορίζουμε το k_r, έτσι ώστε $\frac{N}{q^{r+1}}Q_r = k_r\left(\frac{N}{q}P\right)$.

10. Αν $r=e-1$, σταμάτα. Διαφορετικά, επέστρεψε στο βήμα (7).

Τότε $k \equiv k_0 + k_1 q + ... + k_{e-1}q^{e-1} \pmod{q^e}$

Παρατηρούμε ότι αλγόριθμος μας δίνει το σωστό αποτέλεσμα :

Έχουμε :

$$\frac{N}{q}Q = \frac{N}{q}(k_0 + k_1 q + ...)P =$$

$$= k_0 \frac{N}{q}P + (k_1 + k_2 q + ...)NP = k_0 \frac{N}{q}P,$$

αφού $NP = \infty$. Συνεπώς, το βήμα (2) βρίσκει το k_0. Τότε

$$Q_1 = Q - k_0 P = (k_1 q + k_2 q^2 + ...)P,$$

έτσι

$$\frac{N}{q^2}Q_1 = (k_1 + k_2 q + ...)\frac{N}{q}P =$$

$$= k_1 \frac{N}{q}P + (k_2 + k_3 q + ...)NP = k_1 \frac{N}{q}P.$$

Συνεπώς, βρίσκουμε το k_1. Παρόμοια, η μέθοδος παράγει τα k_2, k_3, …. Θα πρέπει να σταματήσουμε αφότου $r = e-1$ διότι το N/q^{e+1} δεν είναι πλέον ακέραιος, και δεν μπορούμε να πολλαπλασιάσουμε το Q_e με τον μη-ακέραιο N/q^{e+1}. Επιπλέον, δεν χρειάζεται να συνεχίσουμε διότι γνωρίζουμε το k $\bmod q^e$.

Παράδειγμα 6.4 :

Έστω $G = E(F_{599})$, όπου Ε είναι η ελλειπτική καμπύλη που δίνεται από την σχέση $y^2 = x^3 + 1$. Έστω P = (60, 19) και Q = (277, 239). Οι μέθοδοι της παραγράφου 4.3.2 μπορούν να χρησιμοποιηθούν για να δείξουν ότι η τάξη του P είναι N = 600. Θέλουμε να λύσουμε την εξίσωση $kP = Q$ για το k.

Η παραγοντοποίηση του N σε πρώτους παράγοντες είναι

$$600 = 2^3 \cdot 3 \cdot 5^2 .$$

Θα υπολογίσουμε το k mod 8, mod 3, και mod 25, έπειτα θα τα συνδυάσουμε για να αποκτήσουμε το k mod 600 (το Κινέζικο Θεώρημα Υπολοίπων μας επιτρέπει να το κάνουμε αυτό).

- **k mod 8 :**

1ο βήμα :

$$T = \left(j\left(\frac{N}{q}P\right) / 0 \le j \le q-1 \right)$$

q = 2, άρα για j = 0 και j = 1 έχουμε :

για j = 0: $0 \cdot \left(\frac{N}{2}P\right) = \infty$ και

για j =1: $\frac{N}{2}P = 300 \cdot (60,19) = (598,0)$

άρα $T = \{\infty, (598,0)\}$.

2ο βήμα :

$\frac{N}{q}Q = \left(\frac{N}{2}\right)Q = \infty = 0 \cdot \left(\frac{N}{2}P\right)$ άρα $k_0 = 0$.

3ο βήμα :

$e = 3$ δηλαδή $e \neq 1$ οπότε συνεχίζουμε.

4ο βήμα :

$Q_1 = Q - k_0 P = Q - 0P = Q$.

5ο βήμα :

$\frac{N}{q^2} Q_1 = \frac{N}{4} Q_1 = 150 Q_1 = (598, 0) = 1 \cdot \frac{N}{2} P \Rightarrow k_1 = 1$

6ο βήμα :

$e = 3$ δηλαδή $e \neq 2$ οπότε συνεχίζουμε.

7ο βήμα :

$Q_2 = Q_1 - k_1 q_1 P = Q_1 - 1 \cdot 2 \cdot P = (35, 243)$

8ο βήμα :

$\left(\frac{N}{q^3}\right) Q_2 = \left(\frac{N}{8}\right) Q_2 = 75 Q_2 = \infty = 0 \cdot \frac{N}{2} P \Rightarrow k_2 = 0$

Κι επειδή e = 3, σταματάμε.

9ο βήμα :

Συνεπώς, $k = k_0 + k_1 q + k_2 q^2 + \ldots \pmod{q^e}$

άρα : $k = 0 + 1 \cdot 2 + 0 \cdot 4 = 2 \pmod 8$.

- **k mod 3 :**

1ο βήμα :

$T = \{\infty, (0,1), (0,598)\}$

2ο βήμα :

$\left(\frac{N}{3}\right) Q = (0, 598) = 2 \cdot \frac{N}{3} P$ άρα $k_0 = 2$ **.**

Επειδή e = 1, σταματάμε.

3ο βήμα :

Συνεπώς, $k = 2 \pmod 3$.

- **k mod 25 :**

1ο βήμα :

$T = \{\infty, (84,179), (491,134), (491, 465)(84, 420)\}$

2ο βήμα :

$\left(\frac{N}{5}\right) Q = (84,179)$ **άρα** $k_0 = 1$ **.**

3ο βήμα :

$Q_1 = Q - 1 \cdot P = (130,129)$

4^o βήμα :

$\left(\frac{N}{5^2}\right)Q = (491,465)$ άρα k = 3.

5^o βήμα :

$k = 1 + 3 \cdot 5 = 16 \pmod{25}$

Οπότε, έχουν προκύψει τώρα οι εξής ισότητες :

$$x = 2 \quad (\bmod 8)$$
$$x = 2 \quad (\bmod 3)$$
$$x = 16 \quad (\bmod 25)$$

Θα χρησιμοποιήσουμε το Κινέζικο Θεώρημα Υπολοίπων, οπότε έχουμε τον εξής συμβολισμό :

$a_1 = a_2 = a_3 = 1$, $b_1 = 2$, $b_2 = 2$, $b_3 = 16$, $m_1 = 8$, $m_2 = 3$, $m_3 = 25$, $M = 600$,

$n_1 = 75$, $n_2 = 200$, $n_3 = 24$, όπου $n_i = \frac{M}{m_i}$. Τώρα :

$$n_1 \cdot \overline{n}_1 = 1 \bmod 8 \Rightarrow 75\overline{n}_1 = 1 \bmod 8 \Rightarrow \overline{n}_1 = 3$$

$$n_2 \cdot \overline{n}_2 = 1 \bmod 3 \Rightarrow 200\overline{n}_2 = 1 \bmod 3 \Rightarrow \overline{n}_2 = 2$$

$$n_3 \cdot \overline{n}_3 = 1 \bmod 25 \Rightarrow 24\overline{n}_3 = 1 \bmod 25 \Rightarrow \overline{n}_3 = 2$$

Άρα, μία λύση του συστήματος είναι η εξής:

$$x_0 = b_1 \cdot n_1 \cdot \overline{n}_1 + b_2 \cdot n_2 \cdot \overline{n}_2 + b_3 \cdot n_3 \cdot \overline{n}_3$$

$$= 2 \cdot 75 \cdot 3 + 2 \cdot 200 \cdot 2 + 16 \cdot 24 \cdot 24 = 10.466 \equiv 266 \pmod{600}$$

Άρα k = 266. W

Αναφέρουμε επίσης δύο ακόμη αλγορίθμους επίλυσης του προβλήματος οι οποίοι λειτουργούν υπό προϋποθέσεις .

- **Η επίθεση MOV (MOV attack)**.

Αυτή βασίζεται σε μια αναγωγή του προβλήματος ECDLP σε μια ελλειπτική καμπύλη $E\left(\mathsf{F}_p\right)$, στο πρόβλημα DLP στο σώμα F_{p^l} όπου l είναι ο μικρότερος ακέραιος για τον οποίο ισχύει η εξίσωση $p^l = 1 \bmod m$ με $m = \#E\left(\mathsf{F}_p\right)$. Για να είναι αποδοτική η επίθεση θα πρέπει ο l να είναι ένας μικρός αριθμός.

- **Η επίθεση σε μη ομαλές καμπύλες**.

Οι μη ομαλές καμπύλες είχαν προταθεί από την Miyaji γιατί είναι πολύ ανθεκτικές στην επίθεση MOV. Ωστόσο, οι συγκεκριμένες δεν πρέπει να χρησιμοποιούνται σε κρυπτογραφικά συστήματα ελλειπτικών καμπυλών αφού έχουν βρεθεί μέθοδοι που επιλύουν το ECDLP σε γραμμικό χρόνο.

Τονίζεται ότι καμία από τις παραπάνω μεθόδους δεν μπορεί να είναι αποδοτική αν γίνει μια κατάλληλη επιλογή της ελλειπτικής καμπύλης E. Ο καλύτερος χρόνος επίλυσης του ECDLP είναι εκθετικός για τις μεθόδους Baby step-Giant step και Pollard ενώ οι υπόλοιπες επιθέσεις μπορούν να αποφευχθούν με την κατάλληλη επιλογή της τάξης της E. Για να εξασφαλιστεί επομένως η ασφάλεια των κρυπτοσυστημάτων ελλειπτικών καμπυλών, θα πρέπει η τάξη m μιας $E\left(\mathsf{F}_q\right)$ που χρησιμοποιείται να ικανοποιεί τις παρακάτω συνθήκες.

1. Η m έχει ως παράγοντα έναν αρκετά μεγάλο πρώτο αριθμό (συνήθως μεγαλύτερο από 2^{160}).

2. Η m δεν είναι ίση με τον πρώτο αριθμό p.

3. Για κάθε $1 \le k \le 20$, ισχύει $p^k \ne 1 \bmod m$.

Με την πρώτη συνθήκη αποφεύγεται η αποδοτική χρήση του αλγορίθμου Pohlig-Hellman , η δεύτερη συνθήκη κάνει αδύνατη την εφαρμογή των επιθέσεων σε μη ομαλές καμπύλες , ενώ η τρίτη χρειάζεται για την αποφυγή της επίθεσης MOV. Σύμφωνα με τις ήδη υπάρχουσες επιθέσεις και την ισχύ των σύγχρονων υπολογιστικών συστημάτων ένα κλειδί πρέπει να έχει μέγεθος τουλάχιστον 160 bits για να θεωρείται ασφαλές. Το μέγεθος αυτό είναι πολύ μικρότερο από ότι το αντίστοιχο των κλειδιών κρυπτοσυστημάτων τα οποία βασίζονται στο κλασσικό DLP. Αυτό συμβαίνει γιατί δεν υπάρχει αλγόριθμος υποεκθετικού χρόνου για την επίλυση του ECDLP ενώ αντίθετα υπαρχουν οι αλγόριθμοι Index-Calculus για την επίλυση του DLP.

6.4 Εφαρμογές στην Κρυπτογραφία Δημοσίου Κλειδιού

Μπορεί να αναρωτηθεί κανείς γιατί χρησιμοποιούνται οι ελλειπτικές καμπύλες σε κρυπτογραφικές εφαρμογές. Ο λόγος είναι ότι οι ελλειπτικές καμπύλες παρέχουν ισοδύναμη ασφάλεια με τα κλασσικά συστήματα, χρησιμοποιώντας όμως λιγότερα bits. Για παράδειγμα, υπολογίζεται ότι ένα κλειδί μεγέθους 4096 στο RSA δίνει το ίδιο επίπεδο ασφάλειας με ένα κλειδί μεγέθους 313 σε ένα σύστημα ελλειπτικών καμπυλών.
Αυτό σημαίνει ότι εφαρμογές συστημάτων ελλειπτικών καμπυλών απαιτούν μικρότερο μέγεθος chip, λιγότερη κατανάλωση ισχύος, κλπ. Οι Daswani και Boneh εκτέλεσαν πειράματα χρησιμοποιώντας το 3Com's Palm Pilot, μια συσκευή χειρός, που είναι μεγαλύτερη από μία εξυπνη κάρτα αλλά μικρότερη από ένα laptop. Βρήκαν ότι για να παραχθεί ένα 512-bit κλειδί για το RSA χρειάστηκαν 3,4 λεπτά, ενώ για να παραχθεί ένα 163-bit κλειδί για το ECC-DSA χρειάστηκαν 0,597 δευτερόλεπτα. Αν και κάποιες διαδικασίες, όπως οι ψηφιακές υπογραφές, ήταν ελαφρώς γρηγορότερες για το RSA, οι μέθοδοι ελλειπτικών καμπυλών όπως η ECC-DSA προσφέρουν ολοκάθαρα μεγάλη αύξηση της ταχύτητας σε πολλές περιπτώσεις.

Στην ενότητα αυτή θα παραθέσουμε τα ανάλογα των τριών κρυπτοσυστημάτων του κεφαλαίου 3.3 για την περίπτωση των ελλειπτικών καμπυλών. Καθώς πρόκειται για τα ίδια κρυπτοσυστήματα τα οποία "δουλεύουν " σε διαφορετική ομάδα μπορούμε να επισημάνουμε τις παρακάτω αντιστοιχίες

- Η προσθετική ομάδα $E(\mathsf{F}_q)$ αντιστοιχεί στην πολλαπλασιαστική $\square^*_p$.
- Το βαθμωτό γινόμενο αντιστοιχεί στην πράξη της ύψωσης σε δύναμη.
- Το σημείο P της $E(\mathsf{F}_q)$ που χρησιμοποιούμε αντιστοιχεί στο γεννήτορα της $\square^*_p$.

6.3.1 Το ανάλογο του πρωτοκόλλου συμφωνίας κλειδιού Diffie – Hellman

Η Alice και ο Bob θέλουν να συμφωνήσουν σε ένα κοινό κλειδί το οποίο θα μπορούν να χρησιμοποιούν για να ανταλλάσουν δεδομένα μέσω ενός συμμετρικού σχήματος κρυπτογράφησης όπως το DES ή το AES. Δεν είναι πρακτικό, αλλά είναι και χρονοβόρο να χρησιμοποιήσουν έναν ταχυδρόμο για να παραδώσει το κλειδί.

Επιπλέον, υποθέτουμε ότι η Alice και ο Bob δεν έχουν προηγούμενη επικοινωνία και συνεπώς οι μόνοι δίαυλοι επικοινωνίας μεταξύ τους είναι δημόσιοι.

Ανάλογο του πρωτοκόλλου συμφωνίας κλειδιού Diffie-Hellman

1. Οι Alice και Bob συμφωνούν σε μία ελλειπτική καμπύλη E πάνω σε ένα πεπερασμένο σώμα F_q έτσι ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολα επιλύσιμο στο $E(\mathsf{F}_q)$. Συμφωνούν επίσης σε ένα σημείο $P \in E(\mathsf{F}_q)$ έτσι ώστε η υποομάδα που παράγεται από το P, να έχει μεγάλη τάξη (συνήθως, η καμπύλη και το σημείο επιλέγονται ώστε η τάξη να είναι ένας μεγάλος πρώτος).

2. Η Alice διαλέγει έναν ακέραιο a, τον οποίο γνωρίζει μόνο αυτή, υπολογίζει:

$$P_a = aP,$$

και στέλνει το P_a στον Bob.

3. Ο Bob διαλέγει έναν ακέραιο b, τον οποίο γνωρίζει μόνο αυτός, υπολογίζει:

$$P_b = bP$$

και στέλνει το P_b στην Alice.

4. Η Alice υπολογίζει το $Q = aP_b = abP$.

5. Ο Bob υπολογίζει το $Q = bP_a = baP$.

6. Οι Alice και Bob χρησιμοποιούν μία μέθοδο που έχουν συμφωνήσει δημόσια για να εξάγουν το κλειδί από το $Q = abP$. Για παράδειγμα θα μπορούσαν να χρησιμοποιήσουν τα τελευταία 256 bits της $x-$συντεταγμένης του abP ως το κλειδί. Διαφορετικά θα μπορούσαν να χρησιμοποιήσουν ως συνάρτηση κατακερματισμού την $x-$συντεταγμένη. Και στις δύο περιπτώσεις το κλειδί που εξάγεται θα ανήκει στο F_q.

Η μόνη πληροφορία που η Eve δύναται να γνωρίζει είναι η ελλειπτική καμπύλη E, το πεπερασμένο σώμα F_q, και τα σημεία P, aP και bP. Συνεπώς, για να αποσπάσει το μυστικό κλειδί $Q = abP$ θα πρέπει να λύσει το πρόβλημα ECDHP.

Οι αδυναμίες και η ασφάλεια του πρωτοκόλλου έχουν αναλυθεί ήδη στο κεφάλαιο 3.3.1 .

6.3.2 Το ανάλογο του κρυπτοσυστήματος Massey – Omura

Δίνουμε έναν επεξηγηματικό παραλληλισμό για την κατανόηση της λειτουργίας του κρυπτοσυστήματος Massey – Omura .

Η Alice θέλει να στείλει ένα μήνυμα στον Bob μέσω δημόσιων διαύλων. Δεν έχουν δημιουργήσει ακόμη ένα ιδιωτικό κλειδί. Ένας τρόπος για να το κάνουν είναι ο εξής. Η Alice τοποθετεί το μήνυμά της σε ένα κουτί και τοποθετεί σε αυτό την κλειδαριά της, και στέλνει το κουτί στον Bob. Ο Bob τοποθετεί στο κουτί την δική του κλειδαριά και το στέλνει πίσω στην Alice. Η Alice βγάζει από το κουτί την δική της κλειδαριά και το στέλνει και πάλι στον Bob. Ο Bob βγάζει την κλειδαριά του, ανοίγει το κουτί και διαβάζει το μήνυμα.

Τυπικά, δουλεύοντας σε μια ομάδα $E\left(\mathsf{F}_q\right)$,η διαδικασία αυτή, μπορεί να εκτελεστεί ως εξής:

Κρυπτοσύστημα 6.1 : **Massey-Omura**

- **Δημιουργία κλειδιών**

Η Alice και ο Bob συμφωνούν σε μία ελλειπτική καμπύλη E σε ένα πεπερασμένο σώμα F_q έτσι ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολο στο $E(\mathsf{F}_q)$. Έστω $N = \#E(\mathsf{F}_q)$.

2. Στη συνέχεια και οι δύο πλευρές επιλέγουν από έναν τυχαίο (κρυφό) ακέραιο m, με

$$m \in [0, N]$$

τέτοιο ώστε ΜΚΔ(m, $\#E(\mathsf{F}_q)$) = 1 και υπολογίζουν τον αντίστροφο του

$$d = m^{-1} \bmod N \quad \in \square_N$$

(π.χ. με χρήση του εκτεταμένου ευκλείδειου αλγόριθμου). Έστω ότι (m_A, d_A) οι επιλογές της Alice και (m_B, d_B) οι επιλογές του Bob**.**

Κρυπτοσύστημα 6.1 : Massey-Omura

- **Ανταλλαγή μηνύματος**

Υποθέτουμε ότι η Alice θέλει να στείλει στον Bob ένα μήνυμα κρυπτογραφημένο με το κρυπτοσύστημα Massey-Omura. Η διαδικασία που ακολουθεί είναι η παρακάτω:

1. Η Alice αναπαριστά το μήνυμά της με ένα σημείο $M \in E(\mathsf{F}_q)$.
(Θα συζητήσουμε παρακάτω πώς θα γίνει αυτό.)

2. Η Alice υπολογίζει το $M_1 = m_A M$, και στέλνει το M_1 στον Bob.

3. Ο Bob υπολογίζει το $M_2 = m_B M_1$, και στέλνει το M_2 στην Alice.

4. Η Alice υπολογίζει το $M_3 = m_A^{-1} M_2$ και στέλνει το M_3 στον Bob.

5. Ο Bob υπολογίζει το $M_4 = m_B^{-1} M_3$. Τότε, το $M_4 = M$ είναι το μήνυμα.

Ας δείξουμε ότι το M_4 είναι το πραγματικό μήνυμα M :

Σύμφωνα με τα παραπάνω, έχουμε

$$M_4 = m_B^{-1} m_A^{-1} m_B m_A M = M ,$$

αλλά χρειάζεται να αιτιολογήσουμε γιατί το m_A^{-1}, που είναι ένας ακέραιος που αναπαριστά τον αντίστροφο του $m_A \mod N$, και το m_A αλληλοεξουδετερώνονται:

Έχουμε $m_A^{-1} \cdot m_A = 1 \pmod N$, έτσι $m_A^{-1} \cdot m_A = 1 + kN$ για κάποιο k. Η ομάδα $E(\mathsf{F}_q)$ έχει τάξη N, οπότε από το θεώρημα του Lagrange συνεπάγεται ότι $NR = \infty$ για κάθε $R \in E(\mathsf{F}_q)$. Συνεπώς,

$$m_A^{-1} \cdot m_A R = (1 + kN) R = R + k\infty = R .$$

Εφαρμόζοντας αυτό στην σχέση $R = m_B M$, βρίσκουμε ότι

$$M_3 = m_A^{-1} m_B m_A M = m_B M .$$

Παρόμοια, τα m_B και m_B^{-1} αλληλοεξουδετερώνονται , οπότε

$$M_4 = m_B^{-1} M_3 = m_B^{-1} m_B M = M \ .$$ W

Παρατηρήσεις:

1. Η Eve γνωρίζει το $E(\mathsf{F}_q)$ και τα σημεία $m_A M$, $m_B m_A M$ και $m_B M$. Έστω $a = m_A^{-1}$, $b = m_B^{-1}$, $P = m_A m_B M$. Άρα, η Eve γνωρίζει τα P, bP, aP και θέλει να βρει το abP. Αυτό είναι το πρόβλημα ECDHP.

2. Η παραπάνω διαδικασία δουλεύει σε οποιοδήποτε πεπερασμένο σώμα. Όμως η μέθοδος αυτή σπάνια χρησιμοποιείται στην πράξη.

3. Μένει να δείξουμε *πώς αναπαρίσταται ένα μήνυμα με ένα σημείο πάνω σε μία ελλειπτική καμπύλη:*

Χρησιμοποιούμε μία μέθοδο που προτάθηκε από τον N. Koblitz:

Έστω E μία ελλειπτική καμπύλη που δίνεται από την σχέση $y^2 = x^3 + ax + b$ πάνω στο F_p. (Η περίπτωση ενός αυθαίρετου πεπερασμένου σώματος F_q είναι παρόμοια.) Έστω m να είναι το μήνυμα, που εκφράζεται σαν ένας αριθμός $0 \le m < p/100$. Έστω $x_j = 100m + j$ για $0 \le j < 100$. Για $j = 1, 2, ..., 99$, υπολόγισε $s_j = x_j^3 + ax_j + b$. Εάν $s_j^{(p-1)/2} = 1 \pmod p$, τότε το s_j είναι τετραγωνικό υπόλοιπο $\bmod p$, οπότε, σε αυτήν την περίπτωση, δεν χρειάζεται να δοκιμάσουμε άλλες τιμές του j. Όταν $p = 3 \bmod 4$, τότε μία τετραγωνική ρίζα του s_j θα δίνεται από την σχέση $y_j \equiv s_j^{(p+1)/4} \pmod p$. Όταν το $p \equiv 1 \pmod 4$, μία τετραγωνική ρίζα του s_j μπορεί επίσης να υπολογιστεί, αλλά η διαδικασία είναι πιο πολύπλοκη. Αποκτούμε ένα σημείο (x_j, y_j) στην E. Για να ανακτήσουμε το m από το (x_j, y_j), απλά υπολογίζουμε $[x_j/100]$ (δηλαδή τον μεγαλύτερο ακέραιο που είναι μικρότερος ή ίσος από τον $x_j/100$). Αφού το s_j είναι απαραίτητα ένα τυχαίο στοιχείο του F_p^x, το οποίο είναι κυκλικό περιττής τάξης, η πιθανότητα το s_j να είναι τετράγωνο είναι περίπου ½. Οπότε η πιθανότητα να μην μπορούμε να βρούμε ένα σημείο για το m έχοντας δοκιμάσει 100 τιμές είναι περίπου 2^{-100}.

6.3.2 Το ανάλογο του κρυπτοσυστήματος ElGamal

Η Alice θέλει να στείλει ένα μήνυμα στον Bob μέσω του κρυπτοσυστήματος ElGamal ελλειπτικών καμπυλών. Η διαδικασία υλοποιείται ως εξής:

Κρυπτοσύστημα 6.2 : ElGamal

- **Δημιουργία κλειδιού**

Για να δημιουργήσει ο Bob το δημόσιο και το αντίστοιχο ιδιωτικό κλειδί του ακολουθεί τα εξής βήματα :

4. Επιλέγει μία ελλειπτική καμπύλη E πάνω από ένα πεπερασμένο σώμα F_q τέτοιο ώστε το πρόβλημα του διακριτού λογαρίθμου να επιλύεται δύσκολα στο $E(\mathsf{F}_q)$. Επιλέγει επίσης ένα σημείο P στην E (συνήθως, τέτοιο ώστε η τάξη του P να είναι ένας μεγάλος πρώτος).

2. Διαλέγει ένα μυστικό ακέραιο s και υπολογίζει το $B = sP$.

3. Η ελλειπτική καμπύλη E, το πεπερασμένο πεδίο F_q, και τα σημεία P και B είναι το *δημόσιο κλειδί* του Bob. Δημοσιοποιούνται. Το *ιδιωτικό κλειδί* του Bob είναι ο ακέραιος s.

- **Κρυπτογράφηση** : Η Alice, για να στείλει μήνυμα στον Bob πρέπει να κάνει τα παρακάτω

1. Βρίσκει το δημόσιο κλειδί του Bob.
2. Εκφράζει το μήνυμά της ως ένα σημείο $M \in \mathrm{E}(\mathsf{F}_q)$.
3. Διαλέγει έναν τυχαίο, μυστικό, ακέραιο k και υπολογίζει το $M_1 = kP$.
4. Υπολογίζει το $M_2 = M + kB$.
5. Στέλνει το ζεύγος σημείων (M_1, M_2) στον Bob.

Κρυπτοσύστημα 6.2 : **ElGamal**

- **Αποκρυπτογράφηση**

  Ο Bob αποκρυπτογραφεί το μήνυμα κάνοντας τα εξής

2. Πολλαπλασιάζει το σημείο M_1 με το ιδιωτικό του κλειδί s, υπολογίζει

$$sM_1$$

2. Ανακτά το M αφαιρώντας το sM_1 από το M_2, δηλαδή υπολογίζει:

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M$$

Παρατηρήσεις:

1. Η Eve γνωρίζει τη δημόσια πληροφορία του Bob και τα σημεία M_1 και M_2. Εάν αυτή μπορεί να υπολογίσει διακριτούς λογαρίθμους , τότε μπορεί να χρησιμοποιήσει τα P και B για να βρει το s, το οποίο μπορεί στη συνέχεια να χρησιμοποιήσει για να αποκρυπτογραφήσει το μήνυμα ως $M_2 - sM_1$. Επίσης, θα μπορούσε να χρησιμοποιήσει τα P και M_1 για να βρει το k. Τότε μπορεί να υπολογίσει το $M = M_2 - kB$. Αν δεν μπορεί να υπολογίσει διακριτούς λογαρίθμους, τότε δεν φαίνεται να υπάρχει τρόπος για να βρεθεί το M.

2. Είναι σημαντικό για την Alice να χρησιμοποιεί έναν διαφορετικό τυχαίο ακέραιο k κάθε φορά που στέλνει ένα μήνυμα στον Bob. Αν υποθέσουμε ότι η Alice χρησιμοποιεί το ίδιο k για τα M και M'. Η Eve το αναγνωρίζει αυτό διότι τότε $M_1 = M_1'$. Υπολογίζει τότε το $M_2' - M_2 = M' - M$. Έστω ότι το M είναι οι ανακοινώσεις των πωλήσεων που κοινοποιούνται μία μέρα αργότερα. Τότε η Eve βρίσκει το M, οπότε υπολογίζει το $M' = M - M_2 + M_2'$.
Συνεπώς, η γνώση ενός απλού κειμένου M, επιτρέπει στην Eve να εξάγει και ένα άλλο απλό κείμενο M' σε αυτήν την περίπτωση. (Όπου το k δεν άλλαξε.)

Οι αδυναμίες και η ασφάλεια του πρωτοκόλλου έχουν αναλυθεί περισσότερο στο κεφάλαιο 3.3.2 .

6.5 Σύγκριση ασφάλειας ECDLP-DLP

Η ασφάλεια των κρυπτοσυστημάτων που είδαμε στο παρόν κεφάλαιο και στο κεφάλαιο 3, βασίζεται στη δυσκολία επίλυσης των προβλημάτων ECDLP και DLP αντίστοιχα. Συγκρίνοντας τα δύο προβλήματα παρατηρείται ότι η πολυπλοκότητα επίλυσης του πρώτου είναι πολύ μεγαλύτερη από αυτή του δεύτερου. Αυτό συνεπάγεται ότι η ισχύς ανά bit είναι πολύ μεγαλύτερη σε συστήματα ελλειπτικών καμπυλών παρά σε συμβατικά συστήματα διακριτού λογαρίθμου.
Συγκεκριμένα, ο καλύτερος αλγόριθμος για την επίλυση του ECDLP είναι εκθετικός στον αριθμό $N = \lceil \log_2 p \rceil$ των bits που απαιτούνται για την αναπαράσταση αριθμών στο σώμα F_p πάνω στο οποίο ορίζεται η ελλειπτική καμπύλη, ενώ ο πιο αποδοτικός αλγόριθμος για την επίλυση του DLP έχει υποεκθετική πολυπλοκότητα που δίνεται από τη συνάρτηση

$$L_p(u,c) = e^{c(\ln p)^u (\ln\ln p)^{1-u}} \quad .$$

Για u=1 η συνάρτηση είναι εκθετική στο logp ενώ όταν u=0 είναι πολυωνυμική. Όταν 0<u<1 η συμπεριφορά της συνάρτησης είναι μεταξύ πολυωνυμικής και εκθετικής και καλείται υποεκθετική.
Το DLP στο σώμα F_p επιλύεται σε χρόνο ανάλογο του $L_p(1/3, c_0)$ και $c_0 \approx 1.923$. Αν $M = \lceil \log_2 p \rceil$ είναι ο αριθμός των bits που απαιτούνται για την αναπαράσταση αριθμών στο σώμα F_p στο οποίο ορίζεται ο διακριτός λογάριθμος, τότε η πολυπλοκότητα επίλυσης του προβλήματος είναι

$$C_{DLP} = e^{c_0 M^{\frac{1}{3}} \left(\ln\left(M \ln 2\right)\right)^{\frac{2}{3}}}.$$

Αντίστοιχα για το ECDLP η πολυπλοκότητα είναι

$$C_{ECDLP}(N) = 2^{\frac{N}{2}}$$

όπου N είναι ο αριθμός των bits που απαιτούνται για την αναπαράσταση αριθμών στο σώμα F_p πάνω στο οποίο ορίζεται η ελλειπτική καμπύλη.

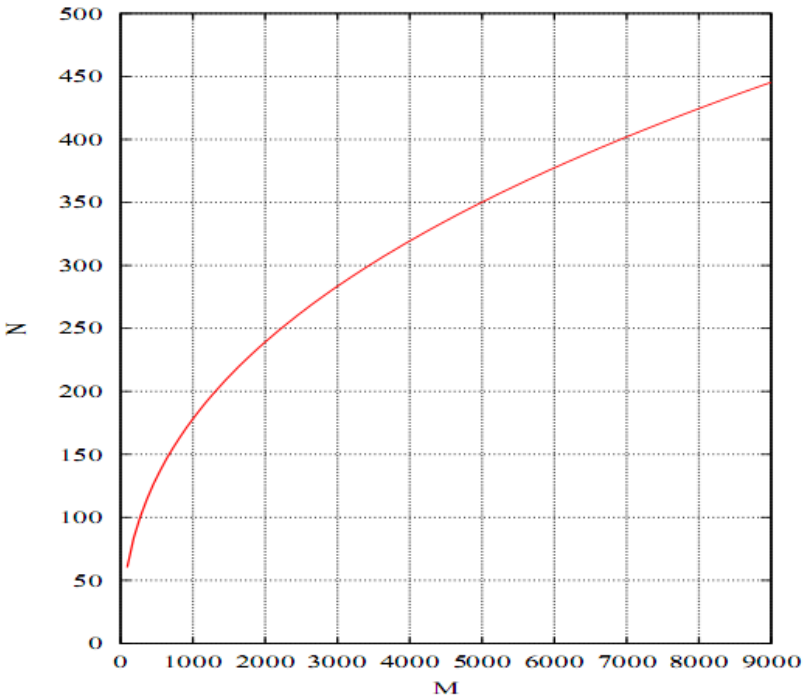
Εξισώνοντας το $C_{ECDLP}(N)$ και το C_{DLP} έτσι ώστε να έχουμε το ίδιο επίπεδο ασφάλειας προκύπτει:

$$N = c_1 M^{\frac{1}{3}} \left(\ln\left(M \ln 2\right)\right)^{\frac{2}{3}}$$

όπου $c_1 = \dfrac{2c_0}{(\ln 2)^{\frac{2}{3}}} \approx 4.91$.

Οι αριθμοί N και M είναι τα μεγέθη των κλειδιών που θα πρέπει να χρησιμοποιηθούν από ένα κρυπτοσύστημα ελλειπτικών καμπυλών και ένα σύστημα που βασίζεται στον

διακριτό λογάριθμο αντίστοιχα, για να επιτευχθεί το ίδιο επίπεδο ασφάλειας και στα δύο. Αυτό που παρατηρείται είναι ότι το μέγεθος κλειδιού σε ένα κρυπτοσύστημα ελλειπτικών καμπυλών αυξάνεται με ρυθμό ελαφρώς γρηγορότερο από την κυβική ρίζα του αντίστοιχου μεγέθους κλειδιού για τα κρυπτοσυστήματα διακριτού, για την επίτευξη περίπου των ίδιων επιπέδων ασφάλειας.
Η σχέση μεταξύ του N και του M φαίνεται στο παρακάτω σχήμα όπου για παράδειγμα κλειδιά μεγέθους 1024 και 4096 bits σε συστήματα διακριτού λογαρίθμου αντιστοιχούν σε κλειδιά μεγέθους 173 και 313 bits (αντίστοιχα) σε συστήματα ελλειπτικών καμπυλών.



Σχήμα 6.1
Σύγκριση μεγέθους κλειδιών κρυπτοσυστημάτων ελλειπτικών καμπυλών και κρυπτοσυστημάτων διακριτού λογαρίθμου, που προσφέρουν την ίδια ασφάλεια.

Τα πλεονεκτήματα που απορρέουν από τη χρήση μικρότερων παραμέτρων είναι μεγαλύτερη ταχύτητα κρυπτογράφησης/αποκρυπτογράφησης, μικρότερη κατανάλωση ισχύος, μικρότερος απαιτούμενος χώρος αποθήκευσης και μικρότερη υπολογιστική ισχύς. Σε περιβάλλοντα περιορισμένων πόρων όπως οι έξυπνες κάρτες (smart cards) και κινητά τηλέφωνα, όπου υπάρχουν διάφοροι περιορισμοί που αφορούν στο χώρο αποθήκευσης(μνήμη, καταχωρητές), την ταχύτητα επεξεργασίας, το εύρος ζώνης μετάδοσης(στην περίπτωση ασύρματων συσκευών) κ.τ.λ, τα πλεονεκτήματα αυτά είναι πολύ σημαντικά.
Σήμερα οι ελλειπτικές καμπύλες παίζουν πολύ σημαντικό ρόλο στις κρυπτογραφικές εφαρμογές και υπάρχουν ήδη αρκετές πρακτικές και αποδοτικές υλοποιήσεις. Παρόλα αυτά, επειδή απαιτούν ένα πολύ καλό συνδυασμό μαθηματικού υπόβαθρου

και γνώσεων κρυπτογραφίας και υπολογιστών, υπάρχουν ελάχιστες βιβλιοθήκες λογισμικού για την ανάπτυξη κρυπτογραφικών συστημάτων ελλειπτικών καμπυλών.

Βιβλιογραφία

[*Wash*] **L. Washington, "*Elliptic Curves: Number Theory and Cryptography*", Chapman & Hall / CRC, 2003**

[*Trap*] **W. Trappe - L. Washington, "Introduction *to Cryptography with Coding Theory*", Prentice-Hall, Inc, 2005**

[*Stins*] **D. Stinson, "*Cryptography: Theory and Practice (3rd edition)*", Chapman & Hall / CRC, 2006**

[*Smart*] **N. Smart, "*Cryptography: An Introduction*", McGraw-Hill, 2003**

[*Papa*] **Χ. Κουκουβίνος – Αλ. Παπαϊωάννου, "*Εισαγωγή στην Κρυπτογραφία*", Αθήνα 2007**

[*Zaxos*] **Ε. Ζάχος, "*Σημειώσεις στην Θεωρία Αριθμών και την Κρυπτογραφία*", Αθήνα 2013**

[*Handb*] **A. Menezes, P. van Oorschot and S. Vanstone, "*Handbook of Applied cryptography*", *CRC Press, 1996***

[*Mao*] **Wenbo Mao, "*Modern Cryptography: Theory and Practice*", Prentice Hall PTR, 2003**

[*Fraleigh*] **John B. Fraleigh, "*Εισαγωγή στην Άλγεβρα*", Πανεπιστημιακές εκδόσεις Κρήτης, 2002**

[*Shoup*] **Victor Shoup, " *Μια υπολογιστική εισαγωγή στη θεωρία αριθμών και την Αλγεβρα*", Κλειδάριθμος, 2005**

[*Talbot*] **John Talbot, Dominic Welsh, "*Complexity and Cryptography An Introduction*", Cambridge University Press ,2006**

[*Guid*] **D. Hankerson, A. Menezes and S. Vanstone, "*Guide to Elliptic Curve Cryptography*", Springer, 2004.**

[*Enc*] **Henk C.A. van Tilborg ,"*Encyclopedia of Cryptography and Security*", Springer, 2005.**

[*Kobl*] **Neal Koblitz, "*Algebraic aspects of cryptography*", Springer, 1999**

[*Cohen*] **Henri Cohen, Gerhard Frey, "*handbook of elliptic and Hyperelliptic Curve Cryptography*", Chapman & Hall/CRC, 2006.**