ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΙΣ ¨ΕΦΑΡΜΟΣΜΕΝΕΣ ΜΑΘΗΜΑΤΙΚΕΣ ΕΠΙΣΤΗΜΕΣ¨

ΝΙΚΟΛΑΪΔΟΥ ΧΑΡΟΥΛΑ

ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΩΝ

ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ

Θεωρήματα

Αλγόριθμοι

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων καθηγητής: Α.Παπαϊωάννου (Σ.Ε.Μ.Φ.Ε.)

Αθήνα, Ιούλιος 2011

Η μεταπτυχιακή αυτή εργασία πραγματοποιήθηκε στο Εθνικό Μετσόβειο Πολυτεχνείο, στα πλαίσια του Διατμηματικού Προγράμματος Μεταπτυχιακών σπουδών με τίτλο «Εφαρμοσμένες Μαθηματικές Επιστήμες», στην κατεύθυνση «Υπολογιστικά Μαθηματικά - Πληροφορική» και κατατέθηκε τον Ιούνιο του 2011.

Επιτροπή αξιολόγησης:

Α. Αρβανιτάκης

Α. Παπαϊωάννου (επιβλέπων καθηγητής)

Π. Ψαράκος

Περιεχόμενα ..... σελ.

Πρόλογος **7**

Συμβολισμοί **9**

Ορολογία-Προαπαιτούμενες γνώσεις **11**

Κεφάλαιο 1: Γνωρίζοντας την κρυπτογραφία **15**

Κεφάλαιο 2: Πιστοποίηση Πρώτου 33

Εισαγωγή, μέθοδος διαδοχικών διαιρέσεων 33

Ιστορική Αναδρομή (το κόσκινο του Ερατοσθένη) 35

Θεώρημα Lucas, αλγόριθμος 36

Κριτήριο Fermat, F-μάρτυρας, F-ψεύτης, αλγόριθμος Fermat-test ισαγωγή, μέθοδος διαδοχικών διαιρέσεων 37

Αλγόριθμος Iterated Fermat Test, αριθμοί Carmichael, Βασική ιδιότητα αριθμών Carmichael 39

Α-μάρτυρας, Α-ψεύτης 46

Κριτήριο Miller-Rabin, αλγόριθμος 47

Ισχυρός ψευδοπρώτος, τετραγωνικό υπόλοιπο mod n 48

Κριτήριο Euler 49

Σύμβολο Legendre και ιδιότητες 51

Σύμβολο Jacobi και ιδιότητες 52

Τετραγωνικός νόμος αντιστροφής 53

Βήματα υπολογισμού για το σύμβολο Jacobi, αλγόριθμος 59

Ε-μάρτυρας, Ε-ψεύτης 60

Κριτήριο Solovay-Strassen 61

Κεφάλαιο 3: Παραγοντοποίηση Ακεραίων **63**

Η μέθοδος των διαδοχικών διαιρέσεων 63

Η μέθοδος παραγοντοποίησης του Fermat, γενίκευση της μεθόδου του Fermat 64

Η μέθοδος παραγοντοποίησης του Euler 65

Αλγόριθμος του Dixon 66

Αλγόριθμος p-1 του Pollard, πολυπλοκότητα 70

Ορισμός σύγκρουσης, το παράδοξο των γενεθλίων 72

Παραγοντοποίηση μονού ακεραίου n 73

Αλγόριθμος Pollard Rho, πολυπλοκότητα 74

Βιβλιογραφία **79**

Πρόλογος

Επί χιλιάδες χρόνια, η Κρυπτογραφία, η «απόκρυφη τέχνη» των λίγων και μυημένων προσβάσιμων σ'αυτήν, πιστά ταγμένη να εξυπηρετεί βασιλείς, στρατηγούς και κυβερνήσεις, παρέχοντας τους την αποτελεσματική, ασφαλή επικοινωνία, μέχρι και σήμερα, με πεδία εφαρμογής σε κάθε τομέα της καθημερινής μας ζωής, από το ξεκλείδωμα ενός αυτοκινήτου έως την αγορά προϊόντων μέσω πιστωτικών και χρεωστικών καρτών και από την εγκατάσταση μιας ενημέρωσης λογισμικού έως και τη χρήση ενός δικτύου κινητής τηλεφωνίας ή του διαδικτύου, αποτελεί έναν ακατάπαυστο πόλεμο κρυπτογράφησης και αποκρυπτογράφησης, «κωδικοπλαστών» και «κωδικοθραυστών»...

Με τον όρο «κρυπτογραφία» εννοούμε την επιστήμη τη απόκρυψης του νοήματος ενός μηνύματος. Μέσα από τα μαθηματικά, τη γλωσσολογία, την πληροφορική, τη φυσική και πολλές άλλες επιστήμες αναζητούνται τρόποι διασφάλισης ή παραβίασης του απορρήτου.

Το μέλλον απρόβλεπτο, το διακύβευμα μείζον. Η τυχόν αποτυχία σε αυτό τον τομέα δεν μπορεί παρά να προκαλέσει αρνητικές αν όχι καταστροφικές συνέπειες, όπως γίνεται αντιληπτό από τις αλλεπάλληλες ειδήσεις για παραβιάσεις της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας πολιτών, παράνομες υποκλοπές, ηλεκτρονικές απάτες και εν γένει ηλεκτρονικά εγκλήματα.

Στην εργασία αυτή θα εξετάσουμε το μαθηματικό υπόβαθρο της κρυπτογραφίας (δεύτερο και τρίτο κεφάλαιο), δηλαδή θα αναλύσουμε μερικές κλασσικές μεθόδους πιστοποίησης πρώτου αλλά και μεθόδους και αλγορίθμους παραγοντοποίσης ακεραίων. Παρατίθενται πολλά παραδείγματα για καλύτερη κατανόηση. Το πρώτο κεφάλαιο αποσκοπεί στο να αποκτήσουμε μια πρώτη επαφή με την κρυπτογραφία καθώς και να μελετήσουμε την ιστορική της πορεία.

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου, κ. Α. Παπαϊωάννου που χωρίς την πολύτιμη βοήθεια και καθοδήγησή του δεν θα είχε γίνει αυτή η εργασία, καθώς και την οικογένειά μου για την στήριξη όλα αυτά τα χρόνια που παρ' όλες τις δυσκολίες έκαναν τα πάντα για να μπορέσω εγώ με ευκολία να κάνω τα όνειρά μου πραγματικότητα.

Νικολαΐδου Χαρούλα

Συμβολισμοί:

$a = b \bmod n$	α ισοδύναμος b modulo n
$\bar{a}$	αντίστροφος του α
$b \mid a$	b διαιρεί α
$\left(\frac{b}{n}\right)$	σύμβολο Jacobi
$\left(\frac{b}{p}\right)$	σύμβολο Legendre
C	κρυπτογραφημένο κείμενο
C^L	κρυπτογραφημένο κείμενο μήκους L
F_n	αριθμοί Fermat
ΘΘΑ	Θεμελιώδες Θεώρημα της Αριθμητικής
M_p	πρώτοι του Mersenne
$ord_n(a)$	τάξη του $a \bmod n$
K	κλειδί
ΚΘΥ	Κινέζικο Θεώρημα Υπολοίπων
M	από κείμενο
ΜΚΔ(α,β)	μέγιστος κοινός διαιρέτης
PNT	θεώρημα πρώτων αριθμών
QR	τετραγωνικά υπόλοιπα
QNR	τετραγωνικά μη υπόλοιπα
QRL	νόμος τετραγωνικής αντιστρεπτότητας
RSA	μέθοδος Rivest Shamir Adleman
$\varphi(n)$	συνάρτηση Euler

Ορολογία – Προαπαιτούμενες γνώσεις:

<u>Ορισμός</u>: Πρώτο αριθμό p (prime number) ονομάζουμε κάθε θετικό ακέραιο αριθμό μεγαλύτερο της μονάδας του οποίου οι μόνοι φυσικοί διαιρέτες του είναι η μονάδα και ο εαυτός του. Παραδείγματος χάριν πρώτοι είναι οι αριθμοί 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Ο αριθμός 1 δεν θεωρείται πρώτος αριθμός.

Σύνθετο αριθμό (composite number) (δηλαδή όχι πρώτο) ονομάζουμε τον ακέραιο αριθμό που έχει περισσότερους από δύο διαιρέτες (εκτός δηλαδή από την μονάδα και τον εαυτό του). Για παράδειγμα οι αριθμοί 4, 6, 8, 9, 10, 12, 14, 15, ... είναι σύνθετοι αριθμοί.

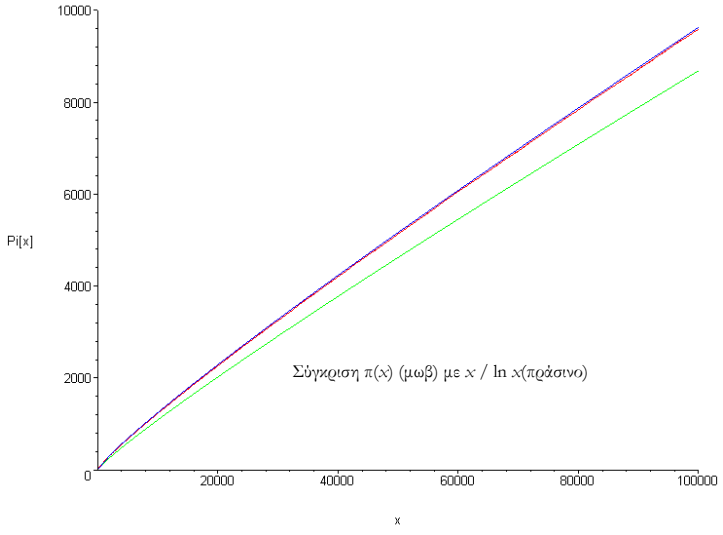
Ο αριθμός 2 είναι ο μόνος άρτιος πρώτος αριθμός. Όλοι οι υπόλοιποι άρτιοι αριθμοί είναι σύνθετοι αφού όλοι διαιρούνται εκτός από τον εαυτό τους και την μονάδα και από τον αριθμό 2. Οπότε, όλοι οι πρώτοι αριθμοί με εξαίρεση τον αριθμό 2 είναι περιττοί.

Η ακολουθία των 25 πρώτων αριθμών είναι η εξής: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

Διάσημες και άλυτες εικασίες, όπως η Εικασία του Riemann και η Εικασία του Goldbach εμπλέκουν ή αφορούν πρώτους αριθμούς.

Το θεώρημα πρώτων αριθμών περιγράφει την ασυμπτωτική κατανομή των πρώτων αριθμών. Αν διαλέξουμε τυχαία έναν αριθμό μικρότερο ή ίσο του x η πιθανότητα αυτός να είναι πρώτος είναι περίπου $\frac{1}{\ln x}$.

Έστω η ***συνάρτηση πρώτων αριθμών*** $\pi(x)$ που δηλώνει το πλήθος των πρώτων αριθμών μικρότερων ή ίσων του x, $x \in R_+$. $\pi(x) = \sum_{p \le x} 1$. Ισχύει $\pi(x) \sim \frac{x}{\ln x}$, δηλαδή η συνάρτηση $\pi(x)$ και η $\frac{x}{\ln x}$ έχουν ασυμπτωτικά την ίδια συμπεριφορά.



Ο πίνακας δίνει το πλήθος των πρώτων αριθμών μέχρι το x σε σύγκριση με τις προαναφερθείσες προσεγγίσεις.

x	π(x)	π(x) / x	x / ln(x)	π(x)·ln(x) / x
10	4	0,400000	4	0,921034
10^2	25	0,250000	22	1,151292
10^3	168	0,168000	145	1,160503
10^4	1.229	0,122900	1.086	1,131951
10^5	9.592	0,095920	8.686	1,104320
10^6	78.498	0,078498	72.382	1,084490
10^7	664.579	0,066458	620.421	1,071175
10^8	5.761.455	0,057615	5.428.681	1,061299
10^9	50.847.534	0,050848	48.254.942	1,053727
10^{10}	455.052.511	0,045505	434.294.482	1,047797
10^{11}	4.118.054.813	0,041181	3.948.131.654	1,043039
10^{12}	37.607.912.018	0,037608	36.191.206.825	1,039145
10^{13}	346.065.536.839	0,034607	334.072.678.387	1,035899
10^{14}	3.204.941.750.802	0,032049	3.102.103.442.166	1,033151
10^{15}	29.844.570.422.669	0,029845	28.952.965.460.217	1,030795
10^{16}	279.238.341.033.925	0,027924	271.434.051.189.532	1,028752
10^{17}	2.623.557.157.654.233	0,026236	2.554.673.422.960.305	1,026964
10^{18}	24.739.954.287.740.860	0,024740	24.127.471.216.847.324	1,025385
10^{19}	234.057.667.276.344.607	0,023406	228.576.043.106.974.646	1,023982
10^{20}	2.220.819.602.560.918.840	0,022208	2.171.472.409.516.259.138	1,022725
10^{21}	21.127.269.486.018.731.928	0,021127	20.680.689.614.440.563.222	1,021594
10^{22}	201.467.286.689.315.906.290	0,020147	197.406.582.683.296.285.296	1,020570
10^{23}	1.925.320.391.606.803.968.923	0,019253	1.888.236.877.840.225.337.614	1,019639

Ορισμός: Δύο αριθμοί α και b ονομάζονται **πρώτοι μεταξύ τους** (ή αλλιώς **πρώτοι προς αλλήλους**) αν δεν υπάρχει κανένας φυσικός διαιρέτης c των α και b ταυτόχρονα που να είναι μεγαλύτερος της μονάδας.

Συμβολισμός: (α, b)=1 .

Με τους πρώτους αριθμούς μπορούμε να κατασκευάσουμε όλους τους ακέραιους αριθμούς. Από το **Θεμελιώδες Θεώρημα της Αριθμητικής** κάθε θετικός ακέραιος μπορεί να γραφεί σαν γινόμενο δυνάμεων πρώτων παραγόντων.

Με βάση αυτό το θεώρημα ο Ευκλείδης κατέληξε στο συμπέρασμα ότι το πλήθος των πρώτων αριθμών είναι άπειρο.

Θεώρημα: Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.

Απόδειξη: Γράφουμε τους πρώτους αριθμούς με βάση την φυσική τους διάταξη κατά αύξουσα σειρά. Έστω δηλαδή p_n ο τελευταίος πρώτος με $1 < p_1 < p_2 < ... < p_n$. Θεωρώ τον φυσικό αριθμό $P = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$ όπου βλέπουμε εύκολα $P > 1$ και P όχι πρώτος αφού $P > p_n$. Θα υπάρχει λοιπόν πρώτος p_k με $p_k \mid P$ όπου $1 \le k \le n$. Αλλά τότε θα ίσχυαν οι σχέσεις:

$p_k \mid p_1 \cdot ... \cdot p_n$ αφού ο p_k είναι ένας παράγοντας του γινομένου

$p_k \mid P$ αφού έτσι δεχτήκαμε άρα $p_k \mid P - p_1 \cdot ... \cdot p_n \Rightarrow p_k \mid 1$ άτοπο αφού $p_k > 1$.

Το άτοπο προέκυψε διότι δεχτήκαμε την ύπαρξη του τελευταίου πρώτου p_n . ■

Ορισμός: Έστω (α, n)=1 (δηλαδή α και n πρώτοι μεταξύ τους), και έστω k ο ελάχιστος φυσικός τ.ω να ισχύει $a^k = 1 \bmod n$, τότε ο k ονομάζεται **τάξη** (order) του n και συμβολίζεται με $ord_n(a)$.

Ορισμός: Με **φ** συμβολίζουμε τη συνάρτηση του Euler.

Η συνάρτηση φ(n) του Euler δίνει το πλήθος των θετικών ακέραιων μικρότερων (ή μικρότερων και ίσων) του n που είναι πρώτοι ως προς τον n.

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Ορισμός: Ονομάζουμε ένα φυσικό αριθμό q **πρωταρχική** (ή αρχική) ρίζα αν $ord_n(q) = \phi(n)$.

Ορισμός: Έστω $1 \le a < n$. Ο α ονομάζεται **τετραγωνική ρίζα** της μονάδας mod n αν $a^2 \bmod n = 1$.

Ορισμός: **Βάση παραγοντοποίησης** καλούμε ένα σύνολο $B = \{-1, p_1, ..., p_h\}$ όπου $p_1, ..., p_h$ είναι διακεκριμένοι πρώτοι. Ένας ακέραιος καλείται **Β-λείος** αν γράφεται ως γινόμενο των στοιχείων του Β. Ένας ακέραιος b καλείται **Β-προσαρμοσμένος** ως προς τον θετικό ακέραιο n, αν ο ακέραιος c, με $-\frac{n}{2} \le c \le \frac{n}{2}$ και $b^2 \equiv c \pmod{n}$, είναι Β-λείος.

Κινέζικο Θεώρημα Υπολοίπων (ΚΘΥ): Έστω οι s φυσικοί $m_1, m_2, ..., m_s$ όπου όλοι είναι πρώτοι προς αλλήλους, και $M = m_1 \cdot m_2 \cdot ... \cdot m_s$. Έστω επιπλέον οι s το πλήθος ακέραιοι a_i $1 \le i \le s$ με $\text{ΜΚΔ}(a_i, m_i) = 1$ για κάθε i .

Τότε οι ταυτοδυναμίες:

$a_1 x = b_1 \bmod m_1$
$a_2 x = b_2 \bmod m_2$
..... και
$a_s x = b_s \bmod m_s$

έχουν μία λύση μοναδική $\bmod M$.

Κεφάλαιο 1:

Γνωρίζοντας την κρυπτογραφία...

Εισαγωγή:

Η λέξη **κρυπτογραφία** προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η κρυπτογραφία αποτελεί τον επιστημονικό κλάδο της κρυπτολογίας που ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Κύριος στόχος της είναι η παροχή μηχανισμών για 2 ή περισσότερα μέλη ώστε να μπορέσουν να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Ετυμολογικά η λέξη κρυπτολογία αποτελείται από τις ελληνικές λέξεις "κρυπτός" και "λόγος" και χωρίζεται σε δύο κλάδους: την **Κρυπτογραφία** και την **Κρυπτανάλυση** με συγγενικό κλάδο την **Στεγανογραφία** και αντίστοιχα την **Στεγανοανάλυση**.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή τη μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς την γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν με κριτήριο την γλωσσική δομή της.

Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση πλέον έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως τα διακριτά μαθηματικά, τη θεωρία αριθμών, τη θεωρία πληροφορίας, την υπολογιστική πολυπλοκότητα αλλά και τη στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία εξυπηρετεί σε 4 βασικές λειτουργίες ως προς την αντικειμενική της σκοπιμότητα:

- *Εμπιστευτικότητα*: Πρόσβαση στην πληροφορία που θέλουμε να μεταδώσουμε έχουν μόνο τα εξουσιοδοτημένα μέλη. Σε περίπτωση υποκλοπής της πληροφορίας από κάποιον τρίτο η πληροφορία είναι ακατανόητη.
- *Ακεραιότητα*: Αλλοίωση της πληροφορίας μπορούν να επιτύχουν μόνο τα εξουσιοδοτημένα μέλη. Σε διαφορετική περίπτωση η πληροφορία δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- *Μη απάρνηση*: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- *Πιστοποίηση*: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητες τους καθώς και την πηγή/προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητες τους δεν είναι πλαστές.

Ορισμοί:

Κρυπτογράφηση (*encryption*) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν άλλο εκτός του νόμιμου παραλήπτη.

Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση (*decryption*)**.

Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

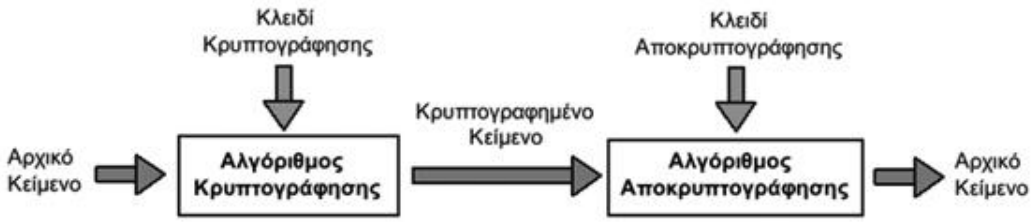
Αρχικό κείμενο (*plaintext*) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (*key*) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (*ciphertext*) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (*cryptanalysis*) είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα.



Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Οπότε το κλειδί είναι καθοριστικής σημασίας. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Βασικές Έννοιες:

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει την δυνατότητα σε 2 πρόσωπα, έστω τον Κώστα και την Βασιλική, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

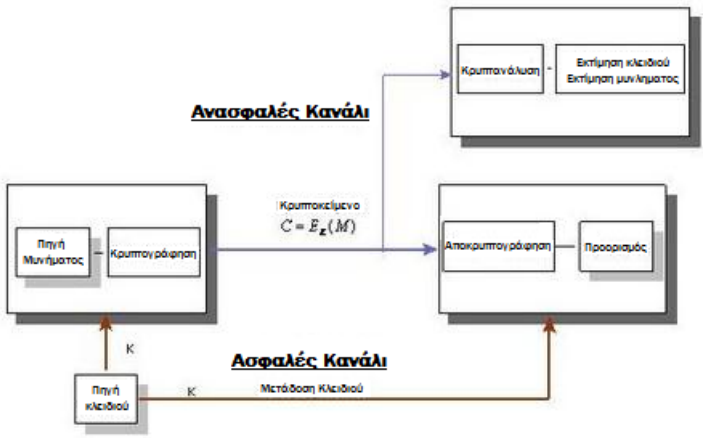
- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.

Το Σύστημα του Σχήματος λειτουργεί με τον ακόλουθο τρόπο :

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους *n* από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις 2 τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.



Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.):

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

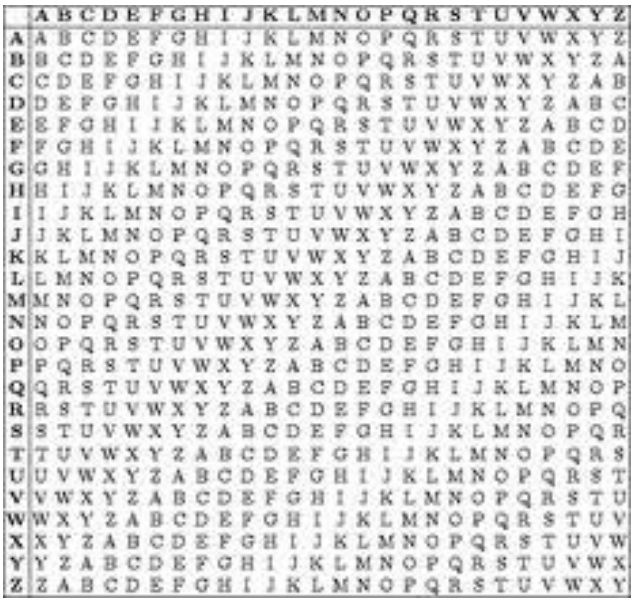
Όπως προκύπτει από μια μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μια σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

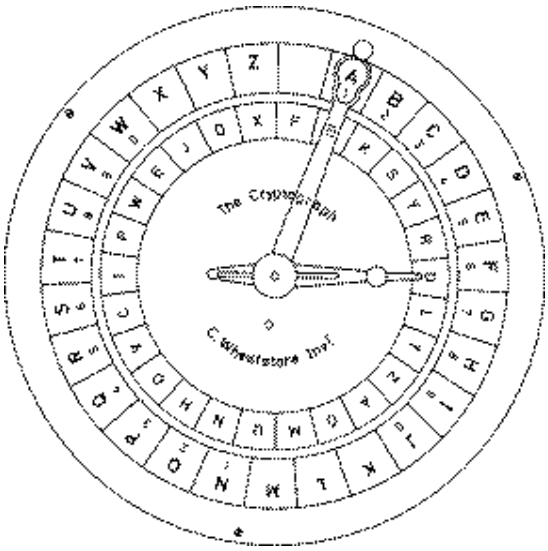
Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» Σχήμα (1.1), ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στην στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Στην διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός *Giovanni Batista Porta*, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «*De furtivis literarum notis*», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος *Vigenere*, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.

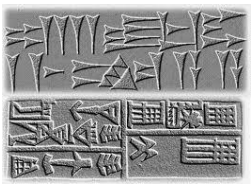




Ο *C.Wheatstone*, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «*Oedipus Aegyptiacus*». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια στην ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής

- 3000-1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850-1450 π.Χ.: Γραμμική γραφή Α
- 1450-1200 π.Χ.: Γραμμική Γραφή Β



Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με την γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού (Σχήμα 1.2), που ανακαλύφθηκε το 1908 στην νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Σχήμα 1.2 Ο Δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που έκανε συστηματικές ανασκαφές στην Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους.

Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

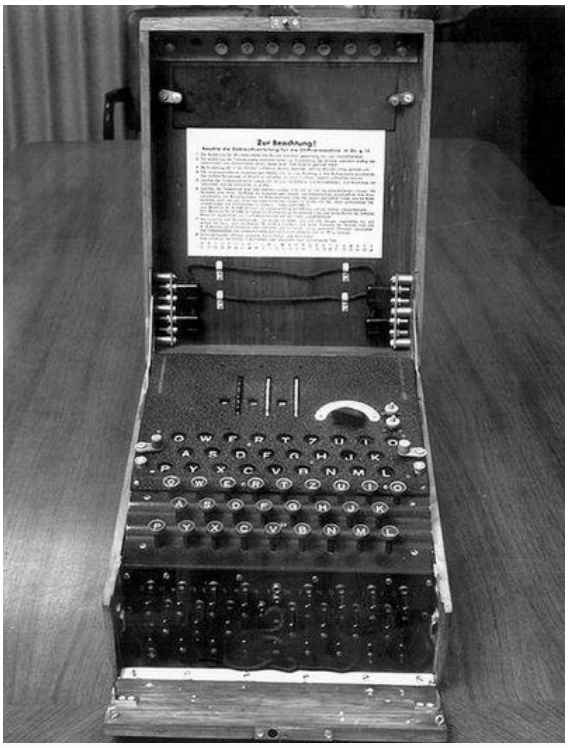
Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στην Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με την γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και τηνΤίρυνθα. Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στην συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση

της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες.

Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

<u>Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.):</u>

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma (Εικόνα 1.3).



Εικόνα 1.3 : Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως από την Γερμανία

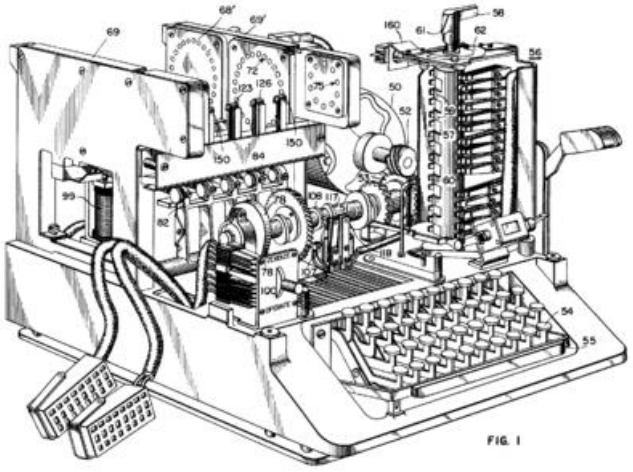
Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με την βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στην Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα τουαμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκλήθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β' Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA (Σχήμα 2.4). Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα

απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανάγγελε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν. τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.



Σχήμα 2.4 : Κρυπτό-μηχανή SIGABA

Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. – σήμερα):

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, που θεωρείται αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (*Communication Theory of Secrecy Systems*) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (*Mathematical Theory of Communication*), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την

κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

Συμμετρικά Κρυπτοσυστήματα:

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά την διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί (Σχ 1.3). Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Τα στάδια της επικοινωνίας του σχήματος 1.4 είναι τα ακόλουθα:

1. Ο Κώστας ή η Βασιλική αποφασίζει για ένα κλειδί το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο.
2. Η Βασιλική αποστέλλει το κλειδί στον Κώστα μέσα από ένα ασφαλές κανάλι.
3. Ο Κώστας δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από την Βασιλική και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.
5. Η Βασιλική λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Σχήμα 1.4 Μοντέλο Συμμετρικού Κρυπτοσυστήματος

Λίστα Συμμετρικών Κρυπταλγορίθμων:

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- *Δέσμης (Block Ciphers)*, οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
- *Ροής (Stream Ciphers)*, οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να την διαχωρίζουν σε τμήματα.

Συμμετρικοί Κρυπταλγόριθμοι Τμήματος (Block Ciphers) :

Data Encryption Standard,3-Way ,Blowfish, CAST ,CMEA ,Triple-DES,DEAL FEAL , GOST ,IDEA ,LOKI ,Lucifer,MacGuffin,Twofish

MARS , MISTY ,MMB ,NewDES ,RC2, RC5 , RC6 REDOC ,Rijndael ,Safer ,Serpent,S QUARE, Skipjack ,Tiny Encryption Algorithm

Συμμετρικοί Κρυπταλγόριθμοι ροής (Stream Ciphers) :

ORYX ,RC4 , SEAL

Συμμετρικοί Κρυπταλγόριθμοι Κατακερματισμού :

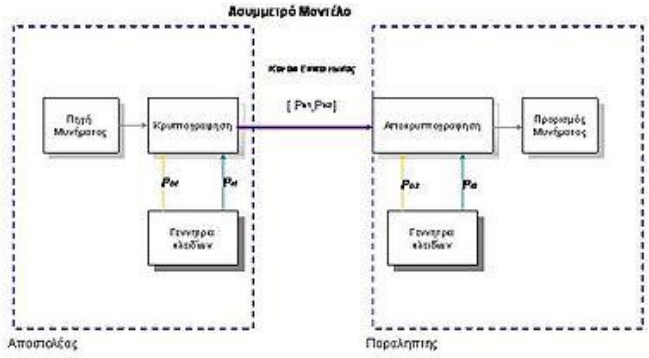
MD2 ,MD4 ,MD5 ,RIPEMD ,SHA1 ,Snefru ,Tiger

Ασύμμετρα κρυπτοσυστήματα:

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι : ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο .Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στην δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.

Τα στάδια της επικοινωνίας του σχήματος 1.5 είναι τα ακόλουθα:

1. Η γεννήτρια κλειδιών του Μένιου παράγει 2 ζεύγη κλειδιών,
2. Η γεννήτρια κλειδιών της Ελένης παράγει 2 ζεύγη κλειδιών
3. Η Ελένη και ο Μένιος ανταλλάσσουν τα δημόσια ζεύγη
4. Ο Μένιος δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
5. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Ελένης και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται
6. Η Ελένη λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ιδιωτικό της κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.



Σχήμα 1.5 Μοντέλο Ασύμμετρου Κρυπτοσυστήματος

Λίστα Ασύμμετρων Κρυπταλγορίθμων:

- RSA
- Ανταλλαγή κλειδιού Diffie–Hellman
- DSA
- Paillier
- El Gamal
- Κρυπτογραφία ελλειπτικών καμπυλών (ECC)

Εφαρμογές Κρυπτογραφίας:

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

1. Ασφάλεια συναλλαγών σε τράπεζες - δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

Κεφάλαιο 2:

Πιστοποίηση Πρώτου

Εισαγωγή:

Οι πρώτοι αριθμοί αποτελούν ένα αναπόσπαστο και ουσιασιώδες κομμάτι του τομέα των Μαθηματικών. Η Θεωρία Αριθμών έχει τους πρώτους αριθμούς σαν άξονα μελέτης της αλλά και πολλές σύγχρονες εφαρμογές της όπως η Θεωρία Κωδικοποίησης και η Κρυπτογραφία στηρίζουν εν μέρη τις βάσεις τους σ'αυτούς. Ένα από τα πιο καίρια προβλήματα είναι αυτό της πιστοποίησης πρώτου αριθμού, το αν δηλαδή μπορούμε να αποφανθούμε αν ένας αριθμός είναι πρώτος ή όχι. Το ερώτημα αυτό απασχολεί τους μαθηματικούς εδώ και πολλά χρόνια τόσο από θεωρητική όσο και από πρακτική σκοπιά. Μεγάλος αριθμός συστημάτων κρυπτογράφησης χρειάζεται μεγάλους πρώτους αριθμούς αφού πάνω σ'αυτούς στηρίζονται πολλά συστήματα ασφάλειας.

Θα αρχίσουμε με το ακόλουθο βασικό θεώρημα της Θεωρίας Αριθμών το οποίο αποτελεί και την πιο παλιά αλλά και απλή μέθοδο ελέγχου πιστοποίησης πρώτου:

Θεώρημα 2.1: Αν ο φυσικός αριθμός $n>1$ δεν έχει πρώτο διαιρέτη μικρότερο ή ίσο της $\sqrt{n}$ τότε ο n είναι πρώτος.

Απόδειξη: Έστω $n>1$ σύνθετος, δηλαδή $n=d_1\cdot d_2$ με $d_1,d_2>1$. Έστω $d_1>\sqrt{n}$ και $d_2>\sqrt{n}$ τότε $n=d_1d_2>\sqrt{n}\cdot\sqrt{n}=n$ άτοπο. Άρα έστω $d_1\le\sqrt{n}$. Αλλά τότε ή ο d_1 πρώτος ή ο d_1 έχει πρώτο διαιρέτη μικρότερο ή ίσο της $\sqrt{n}$. Φθάσαμε σε άτοπο άρα ο n είναι πρώτος. ■

Έτσι για να διαπιστώσουμε αν ένας αριθμός n είναι πρώτος πρέπει να ελέγξουμε αν διαιρείται με όλους τους πρώτους $\leq \sqrt{n}$. Η μέθοδος αυτή ονομάζεται ***μέθοδος των διαδοχικών διαιρέσεων***.

Ο χρόνος που απαιτείται για την μέθοδο των διαδοχικών προσεγγίσεων είναι εκθετικός (όχι όμως πολυωνυμικός):

- $O\left(\sqrt{n}\log n\right)$, στην περίπτωση που όλοι οι πρώτοι $\leq \sqrt{n}$ είναι γνωστοί.
- $O\left(\sqrt{n}(\log n)^2\right)$, διαφορετικά.

Οπότε η μέθοδος αυτή για μεγάλο n δεν είναι αποτελεσματική.

Ιστορική Αναδρομή:

Ο ***Ερατοσθένης*** (Κυρήνη 276 π.Χ. – Αλεξάνδρεια 194 π.Χ.), ήταν αρχαίος Έλληνας μαθηματικός, γεωγράφος και αστρονόμος εφηύρε έναν τρόπο υπολογισμού των πρώτων αριθμών γνωστό ως το ***κόσκινο του Ερατοσθένη***.

Η εύρεση όλων των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από έναν ακέραιο *n*, σύμφωνα με τη μέθοδο του Ερατοσθένη, γίνεται ως εξής:

1. Δημιουργούμε μια λίστα από διαδοχικούς ακέραιους από το 2 μέχρι το *n*: (2, 3, 4, ..., n).
2. Αρχικά, έστω ότι το *p* είναι ίσο με 2, τον 1ο πρώτο αριθμό.
3. Διαγράφουμε από τη λίστα όλα τα πολλαπλάσια του *p* που είναι μικρότερα ή ίσα με *n*. (*2p, 3p, 4p, κ.τ.λ.*)
4. Βρίσκουμε τον 1ο αριθμό που απομένει στη λίστα μετά τον *p* (αυτός ο αριθμός είναι ο επόμενος πρώτος αριθμός) και αντικαθιστούμε το *p* με αυτόν τον αριθμό.
5. Επαναλαμβάνουμε τα βήματα 3 και 4 μέχρι το p^2 να είναι μεγαλύτερο από *n*.
6. Όλοι οι αριθμοί που απομένουν στη λίστα είναι πρώτοι αριθμοί.

Ενδεικτικά το παρακάτω σχήμα δείχνει τους πρώτους ≤ 120 με την μέθοδο του Ερατοσθένη:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Πρώτοι:

2	3	5	7
11	13	17	19
23	29	31	37
41	43	47	53
59	61	67	71
73	79	83	89
97	101	103	107
109	113		

Σε αρκετά κρυπτοσυστήματα χρησιμοποιούνται τυχαίοι μεγάλοι πρώτοι αριθμοί. Θα μελετήσουμε ένα τρόπος κατασκευής πρώτων αριθμών μέσα από το ***θεώρημα του Lucas***.

Θεώρημα 2.2: Έστω n περιττός, θετικός αριθμός. Τότε n πρώτος εάν και μόνον εάν υπάρχει ακέραιος α με (α, n)=1 τέτοιος ώστε:

$$\alpha^{n-1} \equiv 1 \pmod{n} \quad \text{και} \quad a^{(n-1)/p} \not\equiv 1 \pmod{n}$$

για κάθε πρώτο διαιρέτη p του n-1 .

Απόδειξη: Έστω n πρώτος. Τότε οι παραπάνω σχέσεις πληρούνται από μια πρωταρχική (ή αρχική) ρίζα (mod n). Αντίστροφα αν υποθέσουμε ότι υπάρχει κάποιος ακέραιος α που να πληρεί αυτές τις σχέσεις. Τότε $ord_n(a) = n-1$. Οπότε $n-1 | \phi(n)$ και καθώς $\phi(n) \le n-1$ έπεται $\phi(n) = n-1$, απ' όπου έχουμε ότι ο n είναι πρώτος. ■

Για να κατασκευάσουμε μεγάλους πρώτους αριθμούς εργαζόμαστε ως εξής:

Έστω $p_1,...,p_k$ μερικοί γνωστοί πρώτοι και $e_0,e_1,...,e_k$ θετικοί ακέραιοι.

Θέτουμε $n = 1 + 2^{e_0} \cdot p_1^{e_1} \cdot ... \cdot p_k^{e_k}$ και με τυχαία επιλογή ακεραίου α ελέγχουμε αν οι υποθέσεις του πιο πάνω θεωρήματος πληρούνται.

<u>Παράδειγμα 2.1:</u> Θεωρούμε τον αριθμό $n = 1 + 2 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 101 = 11135251$.

Κάνουμε τους εξής υπολογισμούς:

$$2^{n-1} \equiv 1 \pmod{n}, \quad a^{(n-1)/2} \equiv -1 \pmod{n}$$

$$a^{(n-1)/3} \equiv 7009340 \pmod{n}, \quad a^{(n-1)/5} \equiv 390964 \pmod{n},$$
$$a^{(n-1)/7} \equiv 6654420 \pmod{n}, \quad a^{(n-1)/101} \equiv 6577006 \pmod{n}$$

Οπότε βλέπουμε ότι για α=2: $2^{n-1} \equiv 1 \pmod{n}$ και $a^{(n-1)/p} \not\equiv 1 \pmod{n}$ για κάθε πρώτο p_i $(1 \le i \le k)$ του $n = 1 + 2^{e_0} \cdot p_1^{e_1} \cdot ... \cdot p_k^{e_k}$.

Άρα οι σχέσεις του Θεωρήματος 2.2 πληρούνται άρα ο 11135251 είναι πρώτος. ■

Ο χρόνος που απαιτείται για τον υπολογισμό της δύναμης $\alpha^{n-1} \pmod n$ είναι $O\left((\log n)^3\right)$. Επίσης για τον υπολογισμό κάθε δύναμης $a^{(n-1)/p} \pmod n$ απαιτείται χρόνος $O\left((\log n)^2 \cdot (\log n/p)\right)$. Καθώς το πλήθος των πρώτων διαιρετών του n είναι της τάξης $\log n$ έπεται ότι για κάθε α ο χρόνος που απαιτείται για να εφαρμόσουμε την παραπάνω διαδικασία είναι $O\left((\log n)^4\right)$.

Μια από τις πιο κλασσικές μεθόδους πιστοποίησης σύνθετου αριθμού είναι το ***κριτήριο Fermat***.

Σύμφωνα με το γνωστό ***Θεώρημα του Fermat***: με απαραίτητη προϋπόθεση ο p να είναι πρώτος και ο α , με $1 \le a < p$, οποισδήποτε ακέραιος τ.ω. (α, p)=1 τότε ισχύει:

$$a^{p-1} = 1 \pmod p .$$

Σε περίπτωση που βρούμε για ένα θετικό ακέραιο n συγκεκριμένο ακέραιο α, με $1 \le a < n$, τ.ω. να ισχύει: $a^{(n-1)} \not\equiv 1 \pmod n$ τότε λέμε ότι ο n είναι σύνθετος και ο α ονομάζεται ***F-μάρτυρας***. Την μέθοδο αυτή καλούμε *κριτήριο του Fermat.*

Σε διαφορετική περίπτωση που ικανοποιείται η σχέση $a^{n-1} = 1 \pmod n$ για α , με $1 \le a < n$, δεν μπορούμε να αποφανθούμε αν ο n είναι πρώτος ή όχι. Δηλαδή θα υπάρχουν και περιπτώσεις όπου για ένα μονό σύνθετο αριθμό n ένα στοιχείο α, με $1 \le a < n$, θα μας δίνει: $a^{n-1} = 1 \pmod n$, που όμως αυτό δεν θα αληθεύει. Ο α, $1 \le a < n$, με την ιδιότητα αυτή , ονομάζεται ***F-ψεύτης*** ή αλλιώς ***ψευδοπρώτος*** ως προς τη βάση α.

Οι τετριμμένοι F-ψεύτες για κάθε n μονό σύνθετο είναι οι: 1 και n-1.

Με λίγα λόγια είδαμε ότι το «αντίστροφο» του μικρού θεωρήματος του Fermat δεν ισχύει.

<u>Λήμμα 2.1:</u> (α) Αν $1 \le a < n$ ικανοποιεί την $a^r \bmod n = 1 \ (\text{για } r \ge 1)$ τότε $a \in \mathbb{Z}_n^*$.

(β) Αν ικανοποιείται η σχέση $a^{n-1} = 1 \pmod n$ για κάθε α , με $1 \le a < n$, τότε ο n είναι πρώτος.

Απόδειξη: (α) $a^r \bmod n = 1 \ (\text{για } r \ge 1)$ για κάποιο $r \ge 1 \Rightarrow \alpha \cdot \alpha^{r-1} \bmod n = 1 \Rightarrow a \in \mathbb{Z}_n^*$.

(β)Έστω $a^{n-1} = 1 \pmod n \ \ \forall a \in [1, n]$ άρα από το (α) έχουμε ότι $\mathbb{Z}_n^* = \{1, \ldots, n-1\}$ άρα ο n είναι πρώτος. ■

Συμπεραίνουμε επίσης ότι υπάρχει πάντα ένας F-μάρτυρας για τον σύνθετο περιττό n.

Παράδειγμα 2.2: Έστω $n = 91 = 7 \cdot 13$. Έχουμε λοιπόν:

πολ. 7	7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77, 84
πολ.13	13, 26, 39, 52, 65, 78
F-μάρτυρες στο $\mathbb{Z}_{91}^*$	2, 5, 6, 8, 11, 15, 18, 19, 20, 24, 31, 32, 33, 34, 37, 41, 44, 45, 46, 47, 50, 54, 57, 58, 59, 60, 67, 71, 72, 73, 76, 80, 83, 85, 86, 89
F-ψεύτες στο $\mathbb{Z}_{91}^*$	1, 3, 4, 9, 10, 12, 16, 17, 22, 23, 25, 27, , 29, 30, 36, 38, 40, 43, 48, 51, 53, 55, 61, 62, 64, 66, 68, 69, 74, 75, 79, 81, 82, 87, 88, 90

Παρατηρούμε ότι και τα πολλαπλάσια του 7 αλλά και τα πολλαπλάσια του 13 είναι επίσης F-μάρτυρες. Για παράδειγμα αν πάρω ένα πολλαπλάσιο του 7 ή του 13 έστω το 26 έχω: $26^{90} \bmod 91 = 2^{90} \cdot 13^{90} \bmod 91 = 64 \cdot 1 = 64 \neq 1 \bmod 91$ και άρα το 26 είναι F-μάρτυρας.

Για τους F-ψεύτες έχουμε: $3^{90} \bmod 91 = 1 \bmod 91$. Δηλαδή το 3 μας ψευδομαρτυρά ότι το 91 είναι πρώτος κάτι που όμως δεν ισχύει. ■

Ακολουθεί η πρώτη προσπάθεια πιθανοτικής πιστοποίησης πρώτου:

Αλγόριθμος 1 (Fermat Test)

Είσοδος : Μονός φυσικός αριθμός $n \geq 3$

Μέθοδος : 1.Επιλέγω τυχαία $\alpha \in \{2, ..., n - 2\}$

2. αν $\alpha^{n-1} \bmod n \neq 1$

3. τότε επιστροφή 1

4. αλλιώς επιστροφή 0

Η χρονική διάρκεια του πιο πάνω αλγορίθμου είναι της τάξεως log n σε αριθμητικές πράξεις και της τάξεως $(\log n)^3$ σε πράξεις bit. Για $n \geq 3$ μονό σύνθετο αριθμό που έχει τουλάχιστον έναν F-μάρτυρα α, το τεστ του Fermat αν εφαρμοστεί στον n δίνει απάντηση 1 με πιθανότητα μεγαλύτερη του ½.

Φυσικά ένας αλγόριθμος με πιθανότητα λάθους <½ δεν είναι και ότι καλύτερο.

Αν όμως επαναλαμβάναμε το τεστ του Fermat τότε σίγουρα θα πετυχαίναμε η πιθανότητα λάθους να είναι $< (1/2)^{\text{αριθμό επαναλήψεων}}$.

Οπότε για μεγάλο αριθμό επαναλήψεων η πιθανότητα γίνεται όσο μικρή θέλουμε που αυτό είναι κάτι που επιθυμούμε.

Αλγόριθμος 2 (Iterated Fermat Test)

Είσοδος : Μονός φυσικός αριθμός $n \geq 3$, φυσικός $l \geq 1$

Μέθοδος : 1. Επαναλαμβάνω l φορές :

2. α τυχαίο στοιχείο του $\{2, ..., n - 2\}$

3. αν $\alpha^{n-1} \bmod n \neq 1$ τότε επιστροφή 1

4. επιστροφή 0

Αν πάρουμε απάντηση 1 σαν αποτέλεσμα του αλγόριθμου 2 αυτό πάει να πει ότι ο αλγόριθμός μας βρήκε έναν F-μάρτυρα άρα n όχι πρώτος.

Έτσι, καταλήξαμε η πιθανότητα λάθους να είναι $\left(\frac{1}{2}\right)^l$.

Υπάρχουν όμως και κάποιοι δυσεύρετοι μεν άπειροι δε το πλήθος σύνθετοι αριθμοί που ξεφεύγουν από το τεστ του Fermat. Είναι οι λεγόμενοι αριθμοί Carmichael.

Οπότε δίνουμε τον πιο κάτω ορισμό:

Ορισμός: Αν για n ψευδοπρώτο, ικανοποιείται η σχέση $a^{n-1} = 1 \pmod{n}$ για κάθε α , με $1 \leq a < n$ και (α, n)=1, τότε ο n καλείται ***αριθμός Carmichael***. Έχει αποδειχθεί ότι υπάρχουν άπειροι αριθμοί Carmichael (*το 1994 από τους Alford – Granville – Pomerance*) και μάλιστα «ομοιόμορφα» κατανεμημένοι. Ο μικρότερος αριθμός Carmichael είναι ο $561 = 3 \cdot 11 \cdot 17$.

Βασική ιδιότητα των αριθμών *Carmichael* είναι ότι: κάθε αριθμός Carmichael είναι γινόμενο τουλάχιστον τριών (διαφορετικών) πρώτων παραγόντων.

Απόδειξη: Ας είναι n ένας αριθμός Carmichael. Τότε ο n είναι σύνθετος. Ας υποθέσουμε ότι $n = p \cdot q$, όπου p, q είναι πρώτοι με $p > q$. Τότε από το Θεώρημα 2.2 έχουμε ότι $p-1 | n-1$. Καθώς $n-1 = (p-1) \cdot q + q - 1$ παίρνουμε $p-1 | q-1$ και επομένως $p \leq q$ που είναι άτοπο. Άρα ο n έχει τουλάχιστον τρεις πρώτους παράγοντες. ■

Θεώρημα 2.3: Ένας περιττός σύνθετος ακέραιος n>3 είναι αριθμός Carmichael, αν και μόνον αν ο n είναι ελεύθερος τετραγώνου (δηλ. αν ο n δεν διαιρείται από το τετράγωνο ενός πρώτου) και κάθε πρώτος διαιρέτης p του n είναι τέτοιος, ώστε ο p-1 να διαιρεί τον n-1.

Απόδειξη: Ας υποθέσουμε ότι ο n είναι αριθμός Carmichael. Έστω p ένας πρώτος διαιρέτης του n, p^t η μεγαλύτερη δύναμη του p που διαιρεί τον n και g μια πρωταρχική ρίζα (mod p^t). Καθώς (p^t, n/p^t) = 1, υπάρχει ακέραιος b με

$$b \equiv g \pmod{p^t} \text{ και } b \equiv 1 \pmod{n/p^t} .$$

Τότε (b, p) =1, (b, n/ p^t) = 1 και επομένως (b, n) = 1. Καθώς ο n είναι αριθμός Carmichael και ο p^t διαιρέτης του, ισχύει:

$$b^{n-1} \equiv 1 \pmod{p^t}.$$

Επίσης, ο b είναι πρωταρχική ρίζα $\pmod{p^t}$. Άρα $\varphi(p^t) \mid n-1$ και επομένως $p^{t-1}(p-1) \mid n-1$. Συνεπώς, έχουμε $t = 1$ και $p-1 \mid n-1$.

Αντιστρόφως, ας υποθέσουμε ότι ο n είναι ελεύθερος τετραγώνου και για κάθε πρώτο διαιρέτη p του n ισχύει $p-1 \mid n-1$. Ας είναι α ακέραιος με (α, n)=1. Αν p είναι πρώτος διαιρέτης του n, τότε:

$$a^{p-1} \equiv 1 \pmod{p}.$$

και καθώς $p-1 \mid n-1$, έχουμε:

$$a^{n-1} \equiv 1 \pmod{p}.$$

Τέλος, επειδή ο n είναι ελεύθερος τετραγώνου, ισχύει:

$$a^{n-1} \equiv 1 \pmod{n}.$$

■

Κατασκευή (*J. Chernick 1939*): Αν t ακέραιος τ.ω. οι αριθμοί 6t+1, 12t+1 και 18t+1 είναι πρώτοι τότε σύμφωνα με το Θεώρημα 2.3, ο ακέραιος: $n=(6t+1)(12t+1)(18t+1)$ είναι ένας αριθμός Carmichael. Ο μικρότερος αριθμός που ικανοποιεί αυτή τη σχέση (όμως όχι ο μικρότερος αριθμός Carmichael – που είναι ο 561) είναι ο $1729=7\cdot 13\cdot 19$. ■

Ο Richard Pinch ανακάλυψε 8.241 αριθμούς Carmichael μέχρι το 10^{12}, 19279 μέχρι το 10^{13}, 44706 μέχρι το 10^{14} και 105212 μέχρι το 10^{15}.

Οι *20 μικρότεροι αριθμοί Carmichael* είναι:

$561=3\cdot 11\cdot 17$

$1105=5\cdot 13\cdot 17$

$1729=7\cdot 13\cdot 19$

$2465=5\cdot 17\cdot 29$

$2821=7\cdot 13\cdot 31$

$6601=7\cdot 23\cdot 41$

$8911=7\cdot 19\cdot 67$

$10.585=5\cdot 29\cdot 73$

$15.841=7\cdot 31\cdot 73$

$29.341=13\cdot 37\cdot 61$

$41.041=7\cdot 11\cdot 13\cdot 41$

$46.657=13\cdot 37\cdot 97$

$52.633=7\cdot 73\cdot 103$

$62.745=3\cdot 5\cdot 47\cdot 89$

$63.973=7\cdot 13\cdot 19\cdot 37$

$75.361=11\cdot 13\cdot 17\cdot 31$

$101.101=7\cdot 11\cdot 13\cdot 101$

$115.921=13\cdot 37\cdot 241$

$126.217=7\cdot 13\cdot 19\cdot 73$

$162.401=17\cdot 41\cdot 233$

Λήμμα 2.2: Αν p πρώτος και $1 \le a < p$ με $a^2 \bmod p = 1$ τότε $a = 1$ ή $a = p-1$.

Απόδειξη: Έχουμε $a^2 - 1 \bmod p = (a+1)(a-1) \bmod p = 0$ επομένως $p \mid (a+1)(a-1)$. Αφού ο p είναι πρώτος

$$p \mid a+1 \Rightarrow a+1 = kp \Rightarrow a = -1 \bmod p = p-1 \bmod p$$

ή $p \mid a-1 \Rightarrow a-1 = kp \Rightarrow a = 1 \bmod p$.

■

Αν λοιπόν βρούμε μη τετριμμένες ρίζες της μονάδας mod n τότε ο n είναι σίγουρα σύνθετος.

Παράδειγμα 2.3: Οι τετραγωνικές ρίζες του $1 \bmod 91$ είναι 1, 27, 64 και 90.

■

Γενικότερα από το ΚΘΥ αν $n = p_1 \cdot \ldots \cdot p_r$ για διακεκριμένους μονούς πρώτους $p_1, \ldots, p_r$ τότε υπάρχουν ακριβώς 2^r ρίζες της μονάδας mod n και συγκεκριμένα είναι οι αριθμοί $0 \le a < n$ που ικανοποιούν $a \bmod p_j \in \{1, p_j - 1\}$ για $1 \le j \le r$.

Πρόταση: Έστω ο πρώτος $p = 3 \bmod 4$ και ο ακέραιος y. Έστω $x = y^{\frac{p+1}{4}} \bmod p$.

1) Αν ο y έχει τετραγωνική ρίζα mod p τότε οι τ. ρίζες του $y \bmod p$ είναι $\pm x$.
2) Αν ο y δεν έχει τ. ρίζες mod p τότε ο $-y$ έχει και οι τ. ρίζες του $-y \bmod p$ είναι $\pm x$.

Απόδειξη: Υποθέτω $y \neq 0$, διαφορετικά έχουμε τετριμμένη περίπτωση. Από το θεώρημα του Fermat $y^{p-1} = 1 \bmod p$. Άρα $x^4 = y^{p+1} = y^2 \cdot y^{p-1} = y^2 \bmod p$ δηλαδή $\left(x^2 + y\right)\left(x^2 - y\right) = 0 \bmod p$ άρα $x^2 = \pm y \bmod p$. Επομένως είτε το y είτε το $-y$ είναι τετράγωνα mod p .

Έστω y και $-y$ τετράγωνα mod p δηλαδή $y = a^2$, $-y = b^2$ τότε $-1 = \left(\frac{a}{b}\right)^2 \bmod p$. Αν διαιρέσουμε κατά μέλη, δηλαδή το -1 είναι τετράγωνο mod p. Αλλά αφού $p = 3 \bmod 4$ αυτό είναι αδύνατο. Πράγματι, αν $p = 3 \bmod 4$ η εξίσωση $x^2 = -1 \bmod p$

δεν έχει λύσεις διότι αν είχε, δηλαδή αν υπήρχε τέτοιο x, τότε $\left(x^2\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \bmod p \Rightarrow x^{p-1} = -1 \bmod p$, αλλά $x^{p-1} = 1 \bmod p$ από Fermat.

Από $p = 3 \bmod 4$, έχω $p-1 = 2 \bmod 4$, $\frac{p-1}{2}$ μονός και $(-1)^{\frac{p-1}{2}} = -1$.

Άρα ακριβώς ένα από τα y και $-y$ έχει τετραγ. ρίζα mod p. Αν το y έχει, τότε $y = x^2$ και οι δύο ρίζες του $y \bmod p$ είναι $\pm x$. Αν το $-y$ έχει, τότε $x^2 = -y$ και οι δύο ρίζες του $-y$ είναι $\pm x$. ■

Παράδειγμα 2.4:

1. Αναζητούμε τις τ. ρίζες του $5 \bmod 11$, όπου $11 = 3 \bmod 4$.

   $\frac{p+1}{4} = 3$ άρα $x = 5^3 \bmod 11 = 4 \bmod 11$, άρα οι τ. ρίζες του $5 \bmod 11$ είναι ± 4.

   Πράγματι, $4^2 = 16 = 5 \bmod 11$.

2. Αναζητούμε τις τ. ρίζες του $x^2 = 71 \bmod 77$, όπου $77 = 7 \cdot 11$ σύνθετος.

   Άρα λύνω:

$x^2 = 71 = 1 \bmod 7$	$x^2 = 71 = 5 \bmod 11$
$x = \pm 1 \bmod 7$	$x = \pm 4 \bmod 11$ (από προηγ. παράδειγμα)

   Με το ΚΘΥ θα ενώσω τις δύο ισοδυναμίες:

   Η $\left.\begin{array}{ll} x = 1 \bmod 7 & \{1, 8, \boxed{15}, 22, \boxed{\boxed{29}}, 36, 43, 50, 57, 64, 71\} \\ x = 4 \bmod 11 & \{4, \boxed{15}, 26, 37, \boxed{\boxed{48}}, 59, 70\} \end{array}\right\} \Rightarrow x = 15 \bmod 77$.

   Η $\left.\begin{array}{l} x = -1 \bmod 7 \Rightarrow x = 6 \bmod 7 \quad \{6, 13, 20, 27, 34, 41, 48, 55, \boxed{\boxed{62}}, 69, 76\} \\ x = 4 \bmod 11 \{4, 15, 26, 37, \boxed{\boxed{48}}, 59, 70\} \end{array}\right\} \Rightarrow$

   $\Rightarrow x = 48 \bmod 77 \Rightarrow x = -29 \bmod 77$.

   Η $\left.\begin{array}{l} x = 1 \bmod 7 \quad \{1, 8, \boxed{15}, 22, \boxed{\boxed{29}}, 36, 43, 50, 57, 64, 71\} \\ x = -4 \bmod 11 \Rightarrow x = 7 \bmod 11 \{7, 18, \boxed{\boxed{29}}, 40, 51, \boxed{\boxed{62}}, 73\} \end{array}\right\}$

   $\Rightarrow x = 29 \bmod 77$.

$$\text{Η} \quad \left.\begin{array}{l} x=-1 \bmod 7 \\ x=-4 \bmod 11 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x=6 \bmod 7 \ \{6,13,20,27,34,41,48,55,\boxed{\boxed{62}},69,76\} \\ x=7 \bmod 11 \{7,18,\boxed{29},40,51,\boxed{\boxed{62}},73\} \end{array}\right\}$$

$$\Rightarrow x=62 \bmod 77 \Rightarrow x=-15 \bmod 77 .$$

Άρα $x=\pm 15 \bmod 77,\ x=\pm 29 \bmod 77$. ■

Αν λοιπόν $n=p\cdot q$ και έστω $x=\pm a,\ x=\pm b$ οι τέσσερις τετραγωνικές ρίζες της $x^2=y \bmod n$.

Από τα προηγούμενα προκύπτει ότι: $\left.\begin{array}{l} a=b \bmod p \\ a=-b \bmod q \end{array}\right\}$ ή $\left.\begin{array}{l} a=-b \bmod p \\ a=b \bmod q \end{array}\right\}$.

Το πρώτο σύστημα δίνει $p \mid a-b$ και $q \nmid a-b$.

Άρα $\text{ΜΚΔ}(a-b,n)=p$ από το Βασικό Κριτήριο και άρα βρήκαμε ένα **μη τετριμμένο παράγοντα** του n.

Οπότε συνεχίζοντας το Παράδειγμα 2.4 έχουμε: $15^2=29^2=71 \bmod 77$, άρα $\text{ΜΚΔ}(15-29,77)=7$ μας δίνει μη τετριμμένο παράγοντα του 77.

Από τα παραπάνω συμπεραίνουμε το εξής:

Έστω $n=p\cdot q$ με $p,\ q$ πρώτους και $p,\ q=3 \bmod 4$. Έστω ο y με $\text{ΜΚΔ}(y,n)=1$ με y να έχει τ. ρίζα mod n. Τότε η εύρεση των 4 ριζών $x=\pm a,\ x=\pm b$ της $x^2=y \bmod n$ είναι υπολογιστικά ισοδύναμη με την παραγοντοποίηση του n.

Άρα, εκτός αν ο n έχει πολλούς πρώτους, η τυχαία επιλογή του α δεν αποδίδει. Έτσι επιστρέφουμε πάλι πίσω στο τεστ του Fermat.

Αν n περιττός πρώτος τότε ο n-1 θα είναι της μορφής: $n-1=2^s d$, με d περιττό και s θετικό ακέραιο. Από το τεστ του Fermat θέλουμε να υπολογίζουμε το a^{n-1} το οποίο θα είναι ίσο με: $a^{n-1} \equiv \left(a^d \pmod n\right)^{2^s}$. Επομένως, μπορούμε να υπολογίσουμε το a^{n-1} σε s+1 βήματα.

Θέτουμε: $b_0=a^d \bmod n$, $b_i={b_{i-1}}^2 \bmod n$, $i=1,\ldots,s$, δηλαδή $b_s=a^{n-1} \bmod n$.

Παράδειγμα 2.5:

$$n = 325 = 5^2 \cdot 13$$
$$n-1 = 324 = 81 \cdot 2^2$$

Υπολογίζουμε (σε s+1=3 βήματα) όλα τα b_i δηλαδή τις δυνάμεις $a^{81}, a^{162}, a^{324} \bmod 325$, για διάφορα α.

α	$b_0 = a^{81}$	$b_1 = a^{162}$	$b_2 = a^{324}$
2	252	129	66
7	307	324	1
32	57	324	1
49	324	1	1
65	0	0	0
126	1	1	1
201	226	51	1
224	274	1	1

Παρατηρούμε ότι: το 2 είναι F-μάρτυρας $\in \mathbb{Z}_{325}^*$

ενώ το 65 είναι F-μάρτυρας $\notin \mathbb{Z}_{325}^*$.

Οι 7, 32, 49, 126, 201, 224 είναι F-ψεύτες για το 325.

Όμως στα δύο βήματα το $201^{162} = 51$ είναι μη τετριμμένη ρίζα της μονάδας άρα 325 όχι πρώτος. Στο ένα βήμα το $224^{81} = 274$ μας δίνει επίσης μη τετριμμένη ρίζα της μονάδας. Άρα πάλι 325 όχι πρώτος. Όμως για α = 7, 32, 49 και 126 δεν δίνουν περισσότερη πληροφορία αφού $7^{162} = 32^{162} = 49^{81} = -1 \bmod 325 = 324 \bmod 325$.

Έτσι βλέπουμε πως η ακολουθία $b_0, \ldots, b_k$ έχει τις εξής δυνατές μορφές:

Αν $b_i = 1$ ή $b_i = n-1$ τα υπόλοιπα στοιχεία $b_{i+1}, \ldots, b_k$ είναι όλα 1. Άρα η ακολουθία αρχίζει εν γένει με 0 ή με $b_0 \notin \{1, n-1\}$ και τελειώνει με 0 ή με 1. Τα δύο κομμάτια χωρίζονται (όχι υποχρεωτικά) από το n-1. Ο πιο κάτω πίνακας δείχνει όλες τις δυνατές περιπτώσεις των δυνάμεων $a^{n-1} \bmod n$.

b_0	b_1	...				...	b_{k-1}	b_k	**Περίπτωση**
1	1		1	1	1		1	1	1α
n-1	1		1	1	1		1	1	1β
*	*		*	n-1	1		1	1	1β
*	*		*	*	*		*	n-1	2
*	*		*	*	*		*	*	2
*	*		*	1	1		1	1	3
*	*		*	*	*		*	1	3

(όπου * : τυχόν στοιχείο $\notin \{1, n-1\}$)

Περίπτωση 1α: $b_0 = 1$

Περίπτωση 1β: $b_0 \neq 1$ αλλά $\exists i \leq k-1$ με $b_i = n-1$.

Και στις δύο υποπεριπτώσεις έχουμε $b_k = 1$ άρα δεν πήραμε πληροφορία αν ο n είναι πρώτος ή όχι.

Περίπτωση 2: Και στις δύο υποπεριπτώσεις έχουμε $b_k \neq 1$. Άρα ο n είναι σύνθετος και ο α είναι ένας F-μάρτυρας για τον n.

Περίπτωση 3: $b_k \neq 1$, $b_k = 1$, το n-1 δεν υπάρχει στην ακολουθία b_i. Θεωρώ το ελάχιστο $i \geq 1$ με $b_i = 1$. Από την υπόθεση $b_{i-1} \notin \{1, n-1\}$ άρα ο b_{i-1} είναι μη τετριμμένη ρίζα της μονάδας mod n. Άρα πάλι ο n σύνθετος. ■

Ορισμός: Έστω $n \geq 3$ μονός και γράφουμε $n-1 = 2^s d$ με d μονό και $s \geq 1$. Ο αριθμός α, $1 \leq a < n$ ονομάζεται ***A-μάρτυρας*** για τον n αν $a^d \bmod n \neq 1$ και $a^{d \cdot 2^s} \bmod n \neq n-1$ για όλα τα i με $0 \leq i \leq k$. Αν ο n σύνθετος και ο α δεν είναι A-μάρτυρας του n, τότε ο α λέγεται **A-ψεύτης** του n.

Λήμμα 2.3: Αν ο α είναι Α-μάρτυρας του n, τότε ο n είναι σύνθετος.

Απόδειξη: Αν ο α Α-μάρτυρας του n τότε ισχύουν οι περιπτώσεις 2 και 3 άρα ο n σύνθετος. ■

Το λήμμα αυτό σε συνδυασμό με την τυχαία επιλογή του α από το $\{2,...,n-2\}$ ενδυναμώνουν το τεστ του Fermat και μας οδηγούν σε ένα άλλο κλασσικό, ισχυρότερο **κριτήριο** πιστοποίησης σύνθετου αριθμού είναι αυτό των ***Miller – Rabin***:

Κριτήριο Miller - Rabin

Είσοδος : Μονός φυσικός αριθμός $n \geq 3$

Μέθοδος : 1. Βρίσκω μονό d και $s \geq 1$, ώστε $n - 1 = d \cdot 2^s$

2. Επιλέγω τυχαίο $\alpha \in \{2, ..., n - 2\}$

3. $b \leftarrow \alpha^d \bmod n$

4. αν $b = 1$ ή $b = n - 1$ επιστροφή 0

5. επανάληψη $s - 1$ φορές

6. $b \leftarrow b^2 \bmod n$

7. αν $b = n - 1$ επιστροφή 0

8. αν $b = 1$ τότε επιστροφή 1

9. επιστροφή 1

Για να αποφανθούμε αν ο n είναι σύνθετος εργαζόμαστε ως εξής:

Επιλέγουμε τυχαίο ακέραιο a με $2 \leq a < n$.

Αν (α, n)>1, *τότε ο* n σύνθετος.

Αν (α, n)=1, *τότε υπολογίζουμε τις δυνάμεις* $b_i = b_{i-1}^{\,2} \bmod n$, $i = 1,...,s-1$ *με* $b_0 = a^d \bmod n$.

Αν $b_0 = a^d \bmod n \not\equiv \pm 1 (\bmod n)$ *και* $b_i = b_{i-1}^{\,2} \bmod n \not\equiv -1 (\bmod n)$ *(* $i = 1,...,s-1$*),* *τότε ο* n *είναι* σύνθετος.

Διαπιστώνουμε ότι ο χρόνος εκτέλεσης του κριτηρίου των Miller-Rabin είναι $O(\log n)^3$).

Παράδειγμα 2.6: Έστω n=561=3·11·17, όχι πρώτος. Αφού ο n είναι αριθμός Carmichael "ξεγελά" το κριτήριο Fermat. Ο n-1 μπορεί να γραφεί στη μορφή $n-1=560=2^4\cdot 35$. Κάνουμε τους υπολογισμούς για α=2:

$$b_0 = 2^{35} = 263(\mathrm{mod}\,561), b_1 = 2^{2\cdot 35} = 263^2 = 166(\mathrm{mod}\,561)$$
$$b_2 = 2^{4\cdot 35} = 166^2 = 67(\mathrm{mod}\,561),\ b_3 = 2^{8\cdot 35} = 67^2 = 1(\mathrm{mod}\,561).$$

■

Ορισμός: Αν n σύνθετος και $a^{n-1} = 1 \bmod n$ τότε λέμε ότι ο n είναι *ψευδοπρώτος* (ή και *F-ψεύτης*) ως προς την βάση α. Αν επιπλέον οι α, n είναι τέτοιοι ώστε ο n να ξεγελά το τεστ Miller-Rabin, τότε ο n καλείται ***ισχυρός ψευδοπρώτος*** ως προς την βάση α.

Ο 561 είναι ψευδοπρώτος ως προς τη βάση 2 αλλά όχι ισχυρός ψευδοπρώτος ως προς τη βάση 2.

Πρόταση 2.1: Αν n σύνθετος, τότε το σύνολο {1, ... ,n-1} περιέχει το πολύ (n-1)/4 ακεραίους που είναι πρώτοι προς τον n και δεν είναι μάρτυρες της συνθετότητάς του.

Μέσα από την παραπάτω πρόταση έπεται ότι η πιθανότητα ο n να είναι ψευδοπρώτος ως προς τυχαία ακέραια βάση α εφαρμόζοντας το κριτήριο Miller-Rabin είναι $\le \frac{1}{4}$. Οπότε, επαναλαμβάνοντας το κριτήριο τόσες φορές όσες θέλουμε, έστω r φορές, η πιθανότητα να λάθους για το κριτήριο, η πιθανότητα ακόμα και ο n να είναι ισχυρός ψευδοπρώτος γίνεται τόσο μικρή όσο θέλουμε $\le \frac{1}{4^r}$. Για παράδειγμα για r = 10 η πιθανότητα λάθους γίνεται $\le \frac{1}{2^{20}} \approx 0,000001$ και έτσι η πιθανότητα ο n να είναι πρώτος είναι $> 0,999999$.

Ορισμός: Έστω $a \in \mathbb{Z}$, $m \ge 2$ και (α, m)=1. Τότε ο α λέγεται ***τετραγωνικό υπόλοιπο*** (quadratic residue QR) mod m αν έχει τουλάχιστον μια τετραγωνική ρίζα mod m δηλ. υπάρχει x ($x \in \mathbb{Z}$) έτσι ώστε $a \equiv x^2 (\mathrm{mod}\, m)$. Αν (α, m)=1 και $a \notin QR$ τότε ο α καλείται ***μη-τετραγωνικό υπόλοιπο*** (quadratic nonresidue QNR) mod m.

Παρατηρήσεις:

i. $a \in QR$ είναι μια ιδιότητα όλων των αριθμών της κλάσης ισοδυναμίας του α οπότε δουλεύουμε στο $\{1, \ldots, m-1\}$.

ii. $-1 = m-1 \bmod m \in \{1, \ldots, m-1\}$.

iii. Οι αριθμοί α με $(a,n) > 1$ δεν είναι ούτε τετραγωνικά υπόλοιπα QR ούτε μη τετραγωνικά υπόλοιπα QNR.

Παράδειγμα 2.6: Για $m = 13$ τα QR (αν περιοριστούμε στο $\{1,\ldots,12\}$) είναι:

$1^2 = 1 = 12^2$

$2^2 = 4 = 11^2$

$3^2 = 9 = 10^2$

$4^2 = 3 = 9^2$ δηλαδή $\begin{cases} QR : \{1,3,4,9,1012\} \\ QNR : \{2,5,6,7,8,11\} \end{cases}$, $|QR| = |QRN|$.

$5^2 = 12 = 8^2$

$6^2 = 10 = 7^2$

Για $m = 26$ όμως βλέπουμε ότι το πλήθος των QR δεν συμπίπτει με το πλήθος των QNR διότι ο 26 δεν είναι πρώτος. $QR \bmod 26 : 1,3,9,17,23,25$ ■

Έτσι βλέπουμε ότι η συμπεριφορά ενός πρώτου αριθμού χαρακτηρίζεται από μισά QR, μισά QNR.

Θεώρημα 2.4 (***Κριτήριο Euler***): Αν p περιττός πρώτος τότε το QR είναι υποομάδα της πολλαπλασιαστικής ομάδας του $\mathbb{Z}_p^*$ τάξης $\frac{p-1}{2}$. Επίσης αν $a \in \mathbb{Z}_p^*$ έχουμε:

$$a^{\frac{p-1}{2}} = \begin{cases} 1, \text{ αν } \alpha \in QR \\ -1, \text{ αν } \alpha \notin QR \end{cases}.$$

Απόδειξη: Αφού p πρώτος τότε $\mathbb{Z}_p^*$ κυκλική ομάδα. Έστω ότι g γεννήτορας (αλλά και πρωταρχική ρίζα) της $\mathbb{Z}_p^*$. Τότε $\mathbb{Z}_p^* = \{1, g^1, g^2, ..., g^{p-2}\}$. Αφού g πρωταρχική ρίζα $g^{p-1} = 1$ δηλ. $\left(g^{\frac{p-1}{2}}\right)^2 = 1$ και $g^{\frac{p-1}{2}} \neq 1$. Οπότε αναγκαστικά $g^{\frac{p-1}{2}} = -1$ αφού το $1 \in \mathbb{Z}_p^*$ δεν έχει μη τετριμμένες τετραγωνικές ρίζες (p πρώτος). Τα τετράγωνα στην $\mathbb{Z}_p^*$ ομάδα είναι τα στοιχεία g^{2i} $0 \le i \le p-1$ που είναι $\frac{p-1}{2}$ το πλήθος στοιχεία. Ένα στοιχείο g^{2i} ικανοποιεί την $\left(g^{2i}\right)^{\frac{p-1}{2}} = g^{i(p-1)} = \left(g^{p-1}\right)^i = 1$. Ενώ το στοιχείο g^{2i+1} ικανοποιεί την $\left(g^{2i+1}\right)^{\frac{p-1}{2}} = g^{i(p-1)} \cdot g^{\frac{p-1}{2}} = -1 \cdot 1$. ■

Η διαδικασία αυτή μας κάνει εύκολο τον υπολογισμό τετραγωνικών ριζών για τους μισούς περίπου πρώτους. Αν $p \ge 3$ πρώτος και $p = 3 \bmod 4$ θεωρούμε τον γεννήτορα g της $\mathbb{Z}_p^*$ και $a = g^{2i}$ ένα τυχαίο QR στοιχείο στη $\mathbb{Z}_p^*$.

Τότε $x = a^{\frac{p+1}{4}} = g^{i\frac{(p-1)}{2}+i} = \left(g^{\frac{p-1}{2}}\right) \cdot g^i = (-1)^i \cdot g^i$, αλλά $x^2 = (-1)^{2i} \cdot g^{2i} = 1 \cdot a = a$

δηλαδή το x είναι τετραγωνική ρίζα του α (η άλλη τετραγωνική ρίζα του α είναι η $p - x$). Επομένως για να βρω x από το α δεν χρειάζεται ο γεννήτορας g.

Δείξαμε έτσι το λήμμα:

<u>Λήμμα 2.4:</u> Αν p μονός πρώτος με $p = 3 \bmod 4$ τότε για κάθε $a \in \mathbb{Z}_p^*$ που είναι τετραγωνικό υπόλοιπο ($a \notin QR_p$) το στοιχείο $x = a^{\frac{p+1}{4}}$ ικανοποιεί την $x^2 = a \bmod p$ (είναι τετραγωνική ρίζα).

Για τους αριθμούς $p = 1 \bmod 4$ τα πράγματα είναι πιο δύσκολα, αλλά υπάρχουν ικανοποιητικοί πιθανοτικοί αλγόριθμοι.

Παράδειγμα 2.7: Έστω $p=11$. Το $a=3$ είναι QR αλλά όχι γεννήτορας. Τότε $a^5 \bmod 11 = 3^5 \bmod 11 = 1 \bmod 11$ άρα από το κριτήριο Euler είναι QR. Επειδή $11 = 3 \bmod 4$ έχουμε τετραγωνικές ρίζες του 3.

$3^{\frac{11+1}{4}} \bmod 11 = 3^3 \bmod 11 = 5 \bmod 11$ (η άλλη ρίζα είναι η 11-5=6).

Πράγματι $3^5 = 1 \bmod 11$ αλλά $QR = \{1,3,4,5,9\}$.

■

Ορισμός: Έστω α ακέραιος και p>2 πρώτος. Το ***σύμβολο Legendre*** $\left(\frac{a}{p}\right)$ ορίζεται ως:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{αν p} \mid \alpha \\ 1, & \text{αν ο α είναι quadratic residue mod p} \\ -1, & \text{αν ο α είναι quadratic nonresidue mod p} \end{cases}$$

Ιδιότητες: Για p>2 ισχύουν τα εξής

a) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ για $a,b \in Z$.

b) $\left(\frac{a \cdot b^2}{p}\right) = \left(\frac{a}{p}\right)$ για $a,b \in Z$ και $p \nmid b$.

c) $\left(\frac{a + c \cdot p}{p}\right) = \left(\frac{a}{p}\right)$ για $a,c \in Z$.

$\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$ για $a \in Z$.

d) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

e) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ για μονό πρώτο p ή και $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{αν p} = \pm 1 \bmod 8 \\ -1, & \text{αν p} = \pm 3 \bmod 8 \end{cases}$

Παράδειγμα 2.8: $\left(\frac{2}{29}\right) = (-1)^{\frac{841-1}{8}} = (-1)^{105} = -1$.

$\left(\frac{-1}{29}\right) = (-1)^{\frac{28}{2}} = (-1)^{14} = 1$.

■

Ορισμός: Το ***σύμβολο Jacobi*** είναι η γενίκευση του συμβόλου Legendre για σύνθετους περιττούς αριθμούς. Έστω α ακέραιος και n σύνθετος περιττός αριθμός του οποίου η παραγοντοποίηση σε γινόμενο πρώτων παραγόντων είναι $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$. Το σύμβολο Jacobi $\left(\frac{a}{n}\right)$ ορίζεται ως το γινόμενο των συμβόλων Legendre για τους πρώτους παράγοντες του n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \cdot \left(\frac{a}{p_2}\right)^{k_2} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{k_r}.$$

Παρατηρήσεις:

i. Αν n πρώτος τότε το σύμβολο Jacobi συμπίπτει με το σύμβολο Legendre.

ii. Αν (α, n)>1 και $p_i | \alpha$ για κάποιο i τότε: $\left(\frac{a}{p_i}\right)^{k_i} = 0 \Rightarrow \left(\frac{a}{n}\right) = 0$. Επομένως, το σύμβολο Jacobi έχει ενδιαφέρον όταν (α, n)=1.

iii. Αν (α, n)=1 το σύμβολο Jacobi δεν δίνει πληροφορία αν $a \in QR \bmod n$ ή όχι.

iv. Από τον ορισμό συμπεραίνουμε ότι το σύμβολο Jacobi είναι πολλαπλασιαστικό και για το α και για το n, ότι τα τετράγωνα αγνοούνται και στο α και στο n , ότι το $\left(\frac{a}{n}\right)$ υπολογίζεται εύκολα για $a = -1$ κλπ όπως περιγράφουμε στις πιο κάτω ιδιότητες.

Ιδιότητες: Για n, m περιττούς ακεραίους ≥ 3 και α, b ακεραίους ισχύουν τα εξής:

a) $\left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$.

b) $\left(\frac{a \cdot b^2}{n}\right) = \left(\frac{a}{n}\right)$ αν ΜΚΔ(b, n)=1.

c) $\left(\frac{a}{m \cdot n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{a}{m}\right)$.

d) $\left(\frac{a}{n \cdot m^2}\right) = \left(\frac{a}{n}\right)$ αν ΜΚΔ(α, m)=1.

e) $\left(\frac{a + c \cdot n}{n}\right) = \left(\frac{a}{n}\right)$ για ακεραίους c. Παρόμοια $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right)$.

f) $\left(\frac{2^{2k} \cdot a}{n}\right) = \left(\frac{a}{n}\right)$ και $\left(\frac{2^{2k+1} \cdot a}{n}\right) = \left(\frac{2}{n}\right) \cdot \left(\frac{a}{n}\right)$, $k \geq 1$.

g) $\left(\frac{0}{n}\right)=0$, $\left(\frac{1}{n}\right)=1$, $\left(-\frac{1}{n}\right)=(-1)^{\frac{n-1}{2}}$ $(n\,\text{μονός})$, $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$.

Παράδειγμα 2.9: $\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)^{\frac{8}{8}}\cdot(-1)^{\frac{24}{8}}=(-1)(-1)=1$ ενώ $2\notin QR \bmod 15$ διότι $QR \bmod 15=\{1,4,6,9.10\}$. ■

Θεώρημα 2.5: (**τετραγωνικός νόμος αντιστροφής**)

Αν $p\neq q$ μονοί πρώτοι τότε $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Απόδειξη: (Eisenstein). ■

Παράδειγμα 2.10: Έστω οι ισοδυναμίες $283=17 \bmod 19,\ 19=2 \bmod 17$.

Αφού $a=b \bmod p \Leftrightarrow \left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ η πρώτη ισοδυναμία δίνει $\left(\frac{283}{19}\right)=\left(\frac{17}{19}\right)$ και η δεύτερη $\left(\frac{19}{17}\right)=\left(\frac{2}{17}\right)$, αλλά $\left(\frac{17}{19}\right)\left(\frac{19}{17}\right)^{QRL}=(-1)^{\frac{16}{2}\cdot\frac{18}{2}}=(-1)^{8\cdot 9}=(-1)^{72}=1$ άρα $\left(\frac{17}{19}\right)$, $\left(\frac{19}{17}\right)$ ομόσημα.

Άρα $\left(\frac{283}{19}\right)=\left(\frac{17}{19}\right)=\left(\frac{19}{17}\right)=\left(\frac{2}{17}\right)=(-1)^{\frac{17^2-1}{8}}=(-1)^{\frac{288}{8}}=(-1)^{36}=1$.

Όμως $\left(\frac{283}{19}\right)\left(\frac{19}{283}\right)^{QRL}=(-1)^{\frac{18}{2}\cdot\frac{282}{2}}=(-1)^{9\cdot 141}=(-1)^{1269}=-1$ και αφού $\left(\frac{283}{19}\right)=1\Rightarrow\left(\frac{19}{283}\right)=-1$.

Αρά η εξίσωση $x^2=19 \bmod 283$ δεν έχει λύση αφού το $19\notin QR \bmod 283$ (αφού το σύμβολο Legendre ισούται με -1).

(Το 283 δεν είναι πρώτος). ■

Παράδειγμα 2.11: Θέλουμε να υπολογίσουμε τα ακόλουθα σύμβολα Legendre:

a) $\left(\frac{2}{29}\right)$, b) $\left(-\frac{1}{29}\right)$, c) $\left(\frac{5}{29}\right)$, d) $\left(\frac{11}{29}\right)$, e) $\left(\frac{2}{127}\right)$, f) $\left(-\frac{1}{127}\right)$, g) $\left(\frac{5}{127}\right)$, h) $\left(\frac{11}{127}\right)$.

Οι 29 και 127 είναι πρώτοι οπότε έχουμε σύμβολα Legendre.

Έχω $QR \bmod 29 = \{1,4,5,6,7,9,13,16,20,22,23,24,25,28\}$.

a) $\left(\frac{2}{29}\right) = -1$ αφού $p = 29 \bmod 8 = 5 \bmod 8 = -3 \bmod 8$.

b) $\left(-\frac{1}{29}\right) = (-1)^{\frac{29-1}{2}} = (-1)^{\frac{28}{2}} = (-1)^{14} = +1$.

c) $\left(\frac{5}{29}\right) = 1$ διότι $5 \in QR$.

d) $\left(\frac{11}{29}\right) = -1$ διότι $11 \in QNR$.

e) $\left(\frac{2}{127}\right) = 1$ διότι $p = 127 = 7 \bmod 8 = -1 \bmod 8$.

f) $\left(-\frac{1}{127}\right) = (-1)^{\frac{127-1}{2}} = (-1)^{63} = -1$.

g) $\left(\frac{5}{127}\right) = -1$ (κριτήριο Euler).

$5^{63} \bmod 127 = \left(5^3\right)^{21} = (-2)^{21} \bmod 127$

$= (-2)(-2)^{10}(-2)^{10} \bmod 127 = -2 \cdot 8 \cdot 8 = -128 = -1 \bmod 127.$

Επομένως, $\left(\frac{5}{127}\right) = -1.$

h) $\left(\frac{11}{127}\right) =$ κριτήριο Euler $= 1.$

$11^{63} \bmod 127 = \left(11^3\right)^{21} = 1331^{21} \bmod 127$

$= 61 \cdot 38^{10} \bmod 127 = 61 \cdot 47 \cdot 87 \bmod 127 = 1 \bmod 127.$

■

Παράδειγμα 2.12: Θέλουμε να υπολογίσουμε το σύμβολο Jacobi:

$$\text{a)}\ \left(\frac{21}{221}\right),\ \text{b)}\ \left(\frac{215}{253}\right),\ \text{c)}\ \left(\frac{631}{1099}\right),\ \text{d)}\ \left(\frac{1050}{1573}\right),\ \text{e)}\ \left(\frac{89}{197}\right).$$

a) $$\left(\frac{21}{221}\right)=\left(\frac{21}{13}\right)\cdot\left(\frac{21}{17}\right)=\left(\frac{21}{221}\right)=\left(\frac{3}{13}\right)\cdot\left(\frac{7}{13}\right)\cdot\left(\frac{3}{17}\right)\cdot\left(\frac{7}{17}\right)=-1$$

$$\left(\frac{3}{13}\right):3^6 \bmod 13=\left(3^3\right)^2=1^2=1 \bmod 13\Rightarrow 3\in QR \bmod 13.$$

$$\left(\frac{7}{13}\right):7^6 \bmod 13=\left(7^3\right)^2=(343)^2 \bmod 13=5^2 \bmod 13=25 \bmod 13=-1$$
$$\Rightarrow 7\in QNR \bmod 13.$$

$$\left(\frac{3}{17}\right):3^8 \bmod 17=3^5\cdot 3^3 \bmod 17=5\cdot 10=50 \bmod 17=-1$$
$$\Rightarrow 3\in QNR \bmod 17.$$

$$\left(\frac{7}{17}\right):7^8 \bmod 17=7^2\cdot 7^3\cdot 3^3 \bmod 17=15\cdot 3\cdot 3=135 \bmod 17=16 \bmod 17=-1 \bmod 17$$

$$\Rightarrow 7\in QNR \bmod 17.$$

b) $$\left(\frac{215}{253}\right)=\left(\frac{43\cdot 5}{23\cdot 11}\right)=\left(\frac{43}{23}\right)\cdot\left(\frac{5}{23}\right)\cdot\left(\frac{43}{11}\right)\cdot\left(\frac{5}{11}\right)$$

Έχω $\left(\frac{43}{23}\right)=\left(\frac{20}{23}\right)=-1$ διότι $QR \bmod 23=\{1,2,3,4,6,8,9,12,13,16,18\}$.

$$\left(\frac{5}{23}\right)=-1.$$

$$\left(\frac{5}{11}\right)=1\ \ \left(4^2=16=5 \bmod 11\right)$$

$$\left(\frac{43}{11}\right)=\left(\frac{10}{11}\right)=-1\quad QR \bmod 11=\{1,3,4,5,9\}.$$

Άρα $\left(\frac{215}{253}\right)=-1$.

c) $\left(\frac{631}{1099}\right)=\left(\frac{631}{157}\right)\cdot\left(\frac{631}{7}\right)=\left(\frac{3}{157}\right)\cdot\left(\frac{1}{7}\right).$

$1099=$ πολ.7 διότι $109-2\cdot 9=109-18=91=$ πολ.7 $\left(\text{κριτήριο του}7\right).$

Αλλά $\left(\frac{3}{157}\right)\cdot\left(\frac{157}{3}\right)\overset{QRL}{=}(-1)^{1\cdot 78}=1$, άρα $\left(\frac{3}{157}\right),\left(\frac{157}{3}\right)$ ομόσημα.

Όμως $\left(\frac{157}{3}\right)=\left(\frac{1}{3}\right)=1$ άρα $\left(\frac{3}{157}\right)=1.$

Έτσι $\left(\frac{631}{1099}\right)=1\cdot 1=1.$

d) $\left(\frac{1050}{1573}\right)=\left(\frac{2}{1573}\right)\cdot\left(\frac{525}{1573}\right)=(-1)\cdot\left(\frac{525}{1573}\right)$ διότι $1573=-3\bmod 8.$

$1573\overset{\text{ΘΘΑ}}{=}11^2\cdot 13.$

$1050=2\cdot 3\cdot 5^2\cdot 7.$

$$\left(\frac{525}{1573}\right)=\left(\frac{3\cdot 5^2\cdot 7}{11^2\cdot 13}\right)=\left(\frac{3}{11^2}\right)\cdot\left(\frac{3}{13}\right)\cdot\left(\frac{5^2}{11^2}\right)\cdot\left(\frac{5^2}{13}\right)\cdot\left(\frac{7}{11^2}\right)\cdot\left(\frac{7}{13}\right)$$

$$=\left(\frac{3}{11}\right)^2\cdot\left(\frac{3}{13}\right)\cdot\left(\frac{5}{11}\right)^2\cdot\left(\frac{7}{11}\right)^2\cdot\left(\frac{7}{13}\right)=1\cdot\left(\frac{3}{13}\right)\cdot 1\cdot 1\cdot 1\cdot\left(\frac{7}{13}\right)=-1.$$

Τα $QR\bmod 13:\{1,3,4,9,10,12\}$, άρα $\left(\frac{3}{13}\right)=1$, $\left(\frac{7}{13}\right)=-1$ και $\left(\frac{1050}{1573}\right)=(-1)\cdot(-1)\cdot 1.$

Στηριχτήκαμε στην ιδιότητα του συμβόλου Legendre $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ όπου p πρώτος και $p\nmid ab$. Για α=b έχουμε $\left(\frac{a^2}{p}\right)=\left(\frac{a}{p}\right)^2$ παρόμοια και στον παρονομαστή.

e) Το $\left(\frac{89}{197}\right)$ είναι σύμβολο Legendre διότι 89, 197 πρώτοι.

$\left(\frac{89}{197}\right)\cdot\left(\frac{197}{89}\right)\overset{QRL}{=}(-1)^{44\cdot 98}=+1$ άρα $\left(\frac{89}{197}\right),\left(\frac{197}{89}\right)$ ομόσημα.

$$\left(\frac{89}{197}\right)=\left(\frac{197}{89}\right)=\left(\frac{19}{89}\right)=\left(\frac{13}{19}\right)=\left(\frac{19}{13}\right)=\left(\frac{6}{13}\right)=\left(\frac{2}{13}\right)\cdot\left(\frac{3}{13}\right)=(-1)\cdot 1=-1,$$

αφού $\left(\frac{19}{89}\right)\cdot\left(\frac{89}{19}\right)^{QRL}=(-1)^{9\cdot 44}=+1$ άρα ομόσημα.

$\left(\frac{13}{19}\right)\cdot\left(\frac{19}{13}\right)^{QRL}=(-1)^{6\cdot 9}=+1$ άρα ομόσημα.

Άρα $\left(\frac{89}{197}\right)=-1.$ ■

$\frac{a}{n}$	3	5	7	9	11	13	15	17	19	21	23	25	27	29
3	0	–	+	0	–	+	0	–	+	0	–	+	0	–
5	–	0	–	+	+	–	0	–	+	+	–	0	–	+
7	–	–	0	+	+	–	+	–	–	0	+	+	–	+
9	0	+	+	0	+	+	0	+	+	0	+	+	0	+
11	+	+	–	+	0	–	+	–	–	–	+	+	+	–
13	+	–	–	+	–	0	–	+	–	–	+	+	+	+
15	0	0	–	0	–	–	0	+	+	0	+	0	0	–
17	–	–	–	+	–	+	+	0	+	+	–	+	–	–
19	–	+	+	+	+	–	–	+	0	–	+	+	–	–
21	0	+	0	0	–	–	0	+	–	0	–	+	0	–
23	+	–	–	+	–	+	–	–	–	–	0	+	+	+
25	+	0	+	+	+	+	0	+	+	+	+	0	+	+
27	0	–	+	0	–	+	0	–	+	0	–	+	0	–
29	–	+	+	+	–	+	–	–	–	–	+	+	–	0

Πίνακας: Ο πίνακας $\left(\frac{a}{n}\right)$ για $a,\ n\in(1,\ldots,29)$.

Η διαγώνια έχει μόνο 0.

Το + συμβολίζει +1 και το – συμβολίζει -1.

Μια άλλη μορφή του νόμου τετραγωνικής αντιστρεπτότητας είναι:

$$\left(\frac{m}{n}\right)=\begin{cases}\left(\frac{n}{m}\right), & av\ n=1\bmod 4\ \text{ είτε }\ m=1\bmod 4\\ -\left(\frac{n}{m}\right), & av\ n=3\bmod 4\ \ \underline{\text{και}}\ \ m=3\bmod 4\end{cases}$$

όπως φαίνεται και από τον πιο πάνω Πίνακα μια μικρά n, m.

Παράδειγμα 2.13: Θέλουμε να υπολογίσουμε το σύμβολο Legendre $\left(\frac{773}{1373}\right)$ όπου 773, 1373 είναι πρώτοι αριθμοί.

$$\left(\frac{773}{1373}\right)\cdot\left(\frac{1373}{773}\right)=(-1)^{\left(\frac{773-1}{2}\right)\cdot\left(\frac{1373-1}{2}\right)}=(-1)^{386\cdot 886}=+1 \text{ άρα ομόσημα.}$$

$$\left(\frac{773}{1373}\right)=\left(\frac{1373}{773}\right)=\left(\frac{600}{773}\right)=\left(\frac{2^2\cdot 150}{773}\right)=\left(\frac{150}{773}\right)$$

$$\underset{4\cdot\alpha+173}{=}\left(\frac{150}{173}\right)=\left(\frac{2}{173}\right)\cdot\left(\frac{75}{173}\right)=(-1)\cdot\left(\frac{75}{173}\right), \text{ ο } 173 \text{ είναι πρώτος.}$$

$$\text{Αλλά } \left(\frac{75}{173}\right)=\left(\frac{3\cdot 5^2}{173}\right)=\left(\frac{3}{173}\right)\cdot\left(\frac{5^2}{173}\right)=\left(\frac{3}{173}\right) \text{και} \left(\frac{3}{173}\right)\cdot\left(\frac{173}{3}\right)=(-1)^{1\cdot 86}=+1,$$

$$\text{άρα ομόσημα : } \left(\frac{3}{173}\right)=\left(\frac{173}{3}\right)=\left(\frac{2}{3}\right)=(-1) \quad \text{διότι } 173=-3 \bmod 8.$$

$$\text{Άρα } \left(\frac{773}{1373}\right)=(-1)\cdot(-1)=+1.$$

■

Παρόμοιο αποτέλεσμα θα είχαμε αν υπολόγιζα το $773^{686} \bmod 1373=1$ (από κριτήριο Euler).

Αν τυποποιήσω τις διαδικασίες του παραδείγματος έχω:

$$\left(\frac{773}{1373}\right)\overset{(6)}{=}\left(\frac{600}{773}\right)\overset{(4)}{=}\left(\frac{150}{173}\right)\overset{(5)}{=}-\left(\frac{75}{173}\right)\overset{(6)}{=}-\left(\frac{23}{75}\right)$$

$$\overset{(7)}{=}\left(\frac{6}{23}\right)\overset{(5)}{=}-\left(\frac{3}{23}\right)\overset{(7)}{=}-\left(\frac{2}{3}\right)\overset{(5)}{=}\left(\frac{1}{3}\right)\overset{(3)}{=}1$$

όπου τα βήματα (1),...,(7) περιγράφονται από τον πίνακα και ακολούθως από τον αλγόριθμο.

<u>Βήματα υπολογισμού συμβόλου Jacobi</u> $\left(\frac{a}{n}\right)$ για περιττό $n \geq 3$ και α οποιοδήποτε ακέραιο:

1. Αν $\alpha \notin \{1, n-1\}$ το αποτέλεσμα λαμβάνεται $\left(\frac{a \bmod n}{n}\right)$.
2. Αν α=0 τότε $\left(\frac{a}{n}\right) = 0$.
3. Αν α=1 τότε $\left(\frac{a}{n}\right) = 1$.
4. Αν $4 \mid \alpha$ τότε $\left(\frac{a}{n}\right) = \left(\frac{a/4}{n}\right)$.
5. Αν $2 \mid \alpha$ τότε $\left(\frac{a}{n}\right) = \begin{cases} \left(\frac{a/2}{n}\right), \text{αν } n \bmod 8 \in \{1,7\} \\ -\left(\frac{a/2}{n}\right), \text{αν } n \bmod 8 \in \{3,5\} \end{cases}$.
6. Αν α=1mod4 ή n=1mod4 τότε $\left(\frac{a}{n}\right) = \left(\frac{n \bmod a}{a}\right)$.
7. Αν α=3mod4 και n=3mod4 τότε $\left(\frac{a}{n}\right) = -\left(\frac{n \bmod a}{a}\right)$.

Αλγόριθμος για το σύμβολο Jacobi

Είσοδος : ακέραιος α, μονός φυσικός αριθμός $n \geq 3$

Μέθοδος : 0. b, c, s ακέραιοι

1. $b \leftarrow \alpha \bmod n; c \leftarrow n;$
2. $s \leftarrow 1$
3. ενόσω $b \geq 2$ επανέλαβε
    4. ενόσω $4 \mid b$ επανέλαβε $b \leftarrow b / 4$
    5. αν $2 \mid b$ τότε
        6. αν $c \bmod 8 \in \{3,5\}$ τότε $s \leftarrow (-s)$
        7. $b \leftarrow b / 2$
    8. αν $b = 1$ τότε έξοδος από τον βρόγχο
    9. αν $b \bmod 4 = c \bmod 4 = 3$ τότε $s \leftarrow (-s)$
    10. $(b, c) \leftarrow (c \bmod b, b);$
11. επέστρεψε $s \cdot b;$

Δείξαμε έτσι δύο τρόπους ελέγχου τετραγωνικού υπολοίπου modp.

i. $a^{\frac{p-1}{2}}$ με fast exponentiation,

ii. υπολογισμός του $\left(\frac{a}{p}\right)$ με τον πιο πάνω αλγόριθμο .

Καταλήγουμε λοιπόν στο εξής λήμμα:

Λήμμα 2.5: Αν p περιττός πρώτος τότε $a^{\frac{p-1}{2}} \cdot \left(\frac{a}{p}\right) \bmod p = 1$ για κάθε $a \in \{1,...,p-1\}$.

Ορισμός: Έστω n μονός σύνθετος. Ένας αριθμός α με $1 \le a \le n$ λέγεται ***E-μάρτυρας*** του n(από το κριτήριο του Euler) αν $a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \neq 1$. Αλλιώς λέγεται **E-ψεύτης**.

Παράδειγμα 2.14: Έστω ο σύνθετος $n = 325 = 13 \cdot 5^2$.

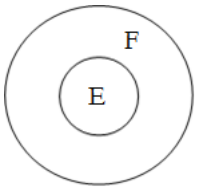
Για $a = 15$ έχουμε $(15,325) = 5$ άρα $\left(\frac{15}{325}\right) = 0$. Ο 15 λοιπόν είναι ένας Ε=μάρτυρας του 325.

Για $a = 2$ έχουμε $2^{162} \bmod 325 = 129$, άρα ο 2 είναι Ε-μάρτυρας του 325.

Όμως για $a = 7$, έχουμε $7^{162} \bmod 325 = 324 = -1 \bmod 325$ και $\left(\frac{7}{325}\right) = \left(\frac{7}{5^2 \cdot 13}\right) = \left(\frac{7}{5}\right)^2 \cdot \left(\frac{7}{13}\right) = \left(\frac{7}{13}\right) = -1$ διότι $7 \notin QR \bmod 13$.

Άρα ο 7 είναι Ε-ψεύτης για τον 325. ■

Λήμμα 2.6: Έστω ο μονός σύνθετος $n \ge 3$ τότε κάθε Ε-ψεύτης του n είναι επίσης και F-ψεύτης του n.



Απόδειξη: Αν ο α είναι Ε-ψεύτης τότε $a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \bmod n = 1$ αλλά αφού $\left(\frac{a}{n}\right) = +1$ ή $\left(\frac{a}{n}\right) = -1$ τότε τετραγωνίζοντας έχω $1 = \left[a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right)\right]^2 \bmod n = a^{n-1} \bmod n$.

Άρα ο α είναι και F-ψεύτης.

Λήμμα 2.7: Έστω $n \geq 3$ μονός σύνθετος.

Τότε το σύνολο $L_n^E = \{a \mid a$ είναι Ε - ψεύτης του n$\}$ είναι γνήσια υποομάδα του $\mathbb{Z}_n^*$.

Από το Λήμμα αυτό προκύπτει ότι το πλήθος των Ε-ψευτών του n είναι γνήσιος διαιρέτης του $\left|\mathbb{Z}_n^*\right| = \varphi(n)$ άρα τουλάχιστον τα μισά στοιχεία του $\mathbb{Z}_n^*$ είναι Ε-μάρτυρες.

Πιο κάτω παραθέτουμε το ***κριτήριο των Solovay-Strassen***:

Κριτήριο των Solovay - Strassen

Είσοδος : μονός ακέραιος αριθμός n ≥ 3

Μέθοδος : 1. Έστω α τυχαία επιλογή από το {2, ..., n - 2}

2. Εάν $a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right) \bmod n \neq 1$

3. τότε επέστρεψε 1

4. αλλιώς επέστρεψε 0.

Ο υπολογισμός του συμβόλου Jacobi $\left(\frac{a}{n}\right)$ γίνεται από τον αλγόριθμο (*Αλγόριθμος για το σύμβολο Jacobi*) και η εκθετοποίηση $a^{\frac{n-1}{2}} \bmod n$ γίνεται με fast exponentiation. Η χρονική πολυπλοκότητα του πιο πάνω αλγορίθμου είναι . Η πιθανότητα ένας αριθμός να μην είναι πρώτος και να πάρουμε σαν αποτέλεσμα από τον αλγόριθμο το 0 (δηλαδή το αποτέλεσμα που παίρνουμε όταν ο αριθμός μας είναι πρώτος) είναι μικρότερη από $\frac{1}{2}$.

Κεφάλαιο 3:

Παραγοντοποίηση ακεραίων

Εισαγωγή:

Ένα από τα ανοιχτά ερωτήματα της σύγχρονης θεωρίας αριθμών είναι το πρόβλημα της παραγοντοποίησης μεγάλων ακεραίων, δηλαδή της εύρεσης αλγορίθμου παραγοντοποίησης σε πολυωνυμικό χρόνο. Στην "σκιά" αυτού του προβλήματος αναπτύχθηκε η κρυπτογραφία δημόσιου κλειδιού και ειδικότερα του κρυπτοσυστήματος RSA.

Φανταστείτε να πρέπει να αποφανθούμε αν ο αριθμός $2^{127}-1$ είναι πρώτος ή όχι και αν είναι να τον παραγοντοποιήσουμε.

Με τη μέθοδο του Ερατοσθένη θα μας πάρει περίπου 41 χρόνια για να διαπιστώσουμε ότι ο $2^{127}-1$ είναι πράγματι πρώτος!

Όπως αναφέραμε και πιο πριν ***η μέθοδος των διαδοχικών διαιρέσεων*** αποτελεί την πιο παλιά αλλά απλή μέθοδο ανάλυσης ενός ακεραίου σε γινόμενο πρώτων. Σύμφωνα με την μέθοδο αυτή για να διαπιστώσουμε αν ένας αριθμός n είναι πρώτος πρέπει να ελέγξουμε αν διαιρείται από όλους τους πρώτους $\leq \sqrt{n}$. Έτσι βρίσκουμε όλους τους πρώτους παράγοντες του ακεραίου μας και παίρνουμε την πρωτογενή ανάλυση του n.

Η δυσκολία όμως έγγειται όταν έχουμε να παραγοντοποιήσουμε ένα αριθμό που είναι γινόμενο μεγάλων πρώτων παραγόντων.

Σήμερα, οι πλέον αποτελεσματικοί αλγόριθμοι παραγοντοποίησης είναι το *κόσκινο των σωμάτων αλγεβρικών αριθμών* και η *μέθοδος των ελλειπτικών καμπυλών* τους οποίους όμως δεν θα μελετήσουμε στην παρούσα εργασία.

Συνεχίζουμε με μια επίσης παλιά ***μέθοδο παραγοντοποίησης*** αυτήν ***του Fermat*** η οποία βασίζεται στην εξής ιδέα:

> *Εκφράζουμε τον ακέραιο αριθμό n που θέλουμε να παραγοντοποιήσουμε σαν διαφορά δύο τετραγώνων.*

Αφού n μονός τότε αν $n = u \cdot v$ τότε και u, v μονοί. Οπότε αν $n = u \cdot v = x^2 - y^2 = (x+y) \cdot (x-y)$ τότε λύνοντας το σύστημα των δύο εξισώσεων που προκύπτουν: $\begin{cases} u = x + y \\ v = x - y \end{cases}$ θα έχουμε: $\begin{cases} x = \dfrac{u+v}{2} \\ y = \dfrac{u-v}{2} \end{cases}$.

Για να παραγοντοποιήσουμε λοιπόν έναν ακέραιο n παίρνουμε: k φυσικό τ.ω.

$k = \left[\sqrt{n}\right] + 1,\ \ k+1 = \left[\sqrt{n}\right] + 2,\ \ \ldots\ ,\ \ k+m = \left[\sqrt{n}\right] + m + 1$ και υπολογίζουμε το $(k+m)^2 - n$ μέχρι να πετύχουμε ακέραιο y τέτοιο ώστε να ισχύει $(k+m)^2 - n = y^2$. Έτσι $n = (x+y) \cdot (x-y)$. Ουσιαστικά το m αντιπροσωπεύει τις *δοκιμές*.

Δυστυχώς όμως η μέθοδος αυτή είναι αποτελεσματική για ακεραίους u, v που είναι αρκετά κοντά μεταξύ τους. Σε αντίθεση περίπτωση θα χρειαστούμε ένα μεγάλος πλήθος δοκιμών m. Έτσι θα μελετήσουμε την ***γενίκευση της μεθόδου του Fermat*** η οποία εξυπηρετεί ακριβώς εκείνα τα u, v που βρίσκονται αρκετά μακριά.

<u>Παράδειγμα 3.1:</u> Θέλουμε να παραγοντοποιήσουμε τον αριθμό n=670661. Θέτουμε $k = \left[\sqrt{n}\right] + 1 = \left[\sqrt{670661}\right] + 1 = 819, \ldots$. Υπολογίζουμε το $(k+m)^2 - n$ μέχρι να πετύχουμε ακέραιο y τέτοιο ώστε να ισχύει $(k+m)^2 - n = y^2$. Βρίσκουμε $819^2 - 670661 = 10^2$. Επομένως, $n = (x+y) \cdot (x-y) \Leftrightarrow 670661 = 829 \cdot 809$. ■

Η ***γενίκευση της μεθόδου παραγοντοποίησης του Fermat*** βασίζεται στην εξής ιδέα:

Επιλέγουμε ένα μικρό θετικό ακέραιο k και θέτουμε $t = \left[\sqrt{k \cdot n}\right] + 1,\ \left[\sqrt{k \cdot n}\right] + 2, \ldots$ και υπολογίζουμε το $t^2 - k \cdot n$ μέχρι να βρούμε ακέραιο s τέτοιο ώστε: $t^2 - k \cdot n = s^2$. Τότε θα έχουμε $k \cdot n = (t+s) \cdot (t-s)$.

Αφού t, s βρίσκονται αρκετά μακριά τότε $k < t - s < t + s < n$ άρα $1 < \text{ΜΚΔ}(t \pm s, n) < n$ και οι $t \pm s$ είναι γνήσιοι παράγοντες του n.

Αν $t \pm s$ τ.ω. $t^2 \equiv s^2 (\mathrm{mod}\, n)$ και $t \not\equiv \pm s (\mathrm{mod}\, n)$ τότε οι μέγιστοι κοινοί διαιρέτες $(t \pm s, n)$ δίνουν μη τετριμμένους παράγοντες του n.

Παράδειγμα 3.2: Θέλουμε να παραγοντοποιήσουμε τον αριθμό n=329345.

Επιλέγουμε μικρό θετικό ακέραιο k=3 και θέτουμε $t = \left[\sqrt{3 \cdot 329345}\right] + 1 = 994, \ldots$.

Υπολογίζουμε το $t^2 - k \cdot n = s^2$ δηλαδή $994^2 - 3 \cdot 329345 = 1$.

Επομένως $k \cdot n = (t+s) \cdot (t-s) \Leftrightarrow 3 \cdot 329345 = (994+1) \cdot (994-1) = 995 \cdot 993$.

Στην συνέχεια υπολογίζουμε τον μέγιστο κοινό διαιρέτη $(329345, 995) = 995$.

Οπότε $329345 = 331 \cdot 995$. ■

Η απλή μέθοδος του Fermat θέλει πολύ περισσότερες δοκιμές.

Το 1641 ο Frenicle ρώτησε τον Fermat αν μπορεί να παραγοντοποιήσει έναν αριθμό n ο οποίος γράφεται σαν άθροισμα δύο τετραγώνων με δύο διαφορετικούς τρόπους.

Δεν ξέρουμε τελικά τι απάντησε ο Fermat όμως το 1745 ο ***Euler*** έδειξε ότι

αν $n = a^2 + b^2 = c^2 + d^2$ τότε ο n παραγοντοποιείται ως εξής:

$$n = \frac{\left[(a-c)^2 + (b-d)^2\right] \cdot \left[(a+c)^2 + (b-d)^2\right]}{4 \cdot (b-d)^2} \ .$$

Παράδειγμα 3.3: Θέλουμε να παραγοντοποιήσουμε τον αριθμό $n = 2501$.

$n = 2501 = 50^2 + 1^2 = 49^2 + 10^2 \Rightarrow a = 50,\ b = 1,\ c = 49,\ d = 10$.

$$n = \frac{\left[(50-49)^2 + (1-10)^2\right] \cdot \left[(50+49)^2 + (1-10)^2\right]}{4 \cdot (1-10)^2} = \frac{\left[1^2 + 9^2\right] \cdot \left[99^2 + 9^2\right]}{4 \cdot 9^2} = \frac{82 \cdot 9882}{4 \cdot 81}$$

$$= \left(\frac{82}{2}\right) \cdot \left(\frac{9882}{2 \cdot 81}\right) = 41 \cdot 61 \ .$$

■

Μια συστηματική μέθοδος εύρεσης ακεραίων s και t με $t^2 \equiv s^2 (\mathrm{mod}\, n)$ και $t \not\equiv \pm s (\mathrm{mod}\, n)$ είναι αυτή του Dixon (1981).

Αλγόριθμος του Dixon:

Ας είναι n ένας σύνθετος περιττός ακέραιος. Για να βρούμε ένα μη τετριμμένο παράγοντα του n ακολουθούμε τα εξής βήματα:

1. Επιλέγουμε ένα θετικό ακέραιο y και θεωρούμε την βάση παραγοντοποίησης B που σχηματίζεται από όλους τους πρώτους $p_1, \ldots, p_{\pi(y)}$ που είναι $\leq y$.
2. Αν κανένας από τους πρώτους $p_1, \ldots, p_{\pi(y)}$ δεν διαιρεί τον n, τότε βρίσκουμε ακέραιους b_i με $1 \leq b_i \leq n$ $(i = 1, \ldots, \pi(y)+2)$ που είναι B-προσαρμοσμένοι ως προς τον n.
3. Αν $b_i^2 \equiv (-1)^{a_{i0}} p_1^{a_{i1}} \ldots p_{\pi(y)}^{a_{i\pi(y)}} (\mathrm{mod}\, n)$, τότε αντιστοιχούμε στο b_i το διάνυσμα $u_i = (u_{i0}, \ldots, u_{i\pi(y)})$ του $\mathbb{Z}_2^{\pi(y)+1}$ θέτοντας $u_{ij} = 0$ αν ο a_{ij} είναι άρτιος και $u_{ij} = 1$ αν ο a_{ij} είναι περιττός (0, 1 τα στοιχεία του $\mathbb{Z}_2$).
4. Προσδιορίζουμε ένα υποσύνολο I του $\{i = 1, \ldots, \pi(y)+2\}$ τέτοιο ώστε: $\sum_{i \in I} u_i = 0$.
5. Υπολογίζουμε τα γινόμενα $b = \prod_{i \in I} b_i$, $c = p_1^{\gamma_1} \ldots p_{\pi(y)}^{\gamma_{\pi(y)}}$ όπου $2\gamma_j = \sum_{i \in I} a_{i,j}$.
6. Αν $b \not\equiv \pm c (\mathrm{mod}\, n)$ υπολογίζουμε τον $\mathrm{ΜΚΔ}(b+c, n)$ που δίνει μη τετριμμένο παράγοντα του n. Αν $b \equiv \pm c (\mathrm{mod}\, n)$ επιλέγουμε άλλο σύνολο $I \subset \{i = 1, \ldots, \pi(y)+2\}$ ή παίρνουμε ένα μεγαλύτερο ακέραιο y και επαναλαμβάνουμε την διαδικασία.

Η ορθότητα του αλγορίθμου είναι εύκολο να διαπιστωθεί. Στο τέταρτο βήμα, καθώς το πλήθος των διανυσμάτων u_i $(i = 1, \ldots, \pi(y)+2)$ είναι μεγαλύτερο από την διάσταση του διανυσματικού χώρου $\mathbb{Z}_2^{\pi(y)+1}$, τα διανύσματα αυτά είναι γραμμικώς εξαρτημένα. Επομένως το σύνολο I υπάρχει πάντοτε και είναι δυνατόν να προσδιοριστεί εύκολα με απαλοιφή. Από την κατασκευή των ακεραίων b και c έχουμε $b^2 \equiv c^2 (\mathrm{mod}\, n)$ και $b \not\equiv \pm c (\mathrm{mod}\, n)$ και κατά συνέπεια, στην περίπτωση όπου $b \not\equiv \pm c (\mathrm{mod}\, n)$, ο $\mathrm{ΜΚΔ}(b+c, n)$ είναι ένας μη τετριμμένος παράγοντας του n.

Καθώς οι πρώτοι $p_1, \ldots, p_{\pi(y)}$ δεν διαιρούν τον n, έχουμε $(b,n)=1$. Έτσι αν ο n έχει r πρώτους παράγοντες $(r \geq 2)$, τότε, η πολυωνυμική ισοτιμία $X^2 \equiv \mathrm{b}^2 \pmod{n}$ έχει ακριβώς 2^r λύσεις. Οπότε, η πιθανότητα να έχουμε $b^2 \equiv c^2 \pmod{n}$ ισούται με $\frac{1}{2^r}$.

Ένας απλός τρόπος εύρεσης ακεραίων b_i είναι να δοκιμάζουμε ακέραιους της μορφής $\left[\sqrt{k \cdot n}\right] + j \;\; (j = 0, 1, \ldots, k = 1, 2, \ldots)$. Ο μικρότερος κατ'απόλυτη τιμή ακέραιος της κλάσης του τετραγώνου τέτοιων ακεραίων $(\mathrm{mod}\, n)$ είναι αρκετά μικρός και κατά συνέπεια έχουν μεγάλη πιθανότητα να είναι B-προσαρμοσμένοι ως προς τον n.

Στην περίπτωση που έχει επιλεγεί κατάλληλη βάση παραγοντοποίησης, ο χρόνος εκτέλεσης του αλγόριθμου είναι $O\left(e^{\sqrt{\log n \log n \log n}}\right)$. Δηλαδή, ο αλγόριθμος του Dixon είναι υποεκθετικού χρόνου.

Παράδειγμα 3.3: Θα παραγοντοποιήσουμε τον $n = 849239$.

Έχουμε $\sqrt{n} = \sqrt{849239} = 921,5\ldots$.

Θεωρούμε τις τιμές του $t = 922, 923, \ldots$ και υπολογίζουμε τον μικρότερο θετικό της κλάσης $t^2 \bmod n$. Έχουμε λοιπόν:

$$922^2 = 5 \cdot 13^2 \bmod n$$
$$933^2 = 2 \cdot 5^4 \cdot 17 \bmod n$$
$$937^2 = 2 \cdot 5 \cdot 13^2 \cdot 17 \bmod n \;.$$

Οι ενδιάμεσοι αριθμοί δίνουν μεγάλους πρώτους παράγοντες mod n (> από το 17) ενώ εμείς θέλουμε να έχουν μικρούς πρώτους παράγοντες.

Π.χ. $923^2 = 13^2 \cdot 71^2 \bmod n$ όμως $71 \notin B$.

Πολλαπλασιάζοντας τις τρεις ισοδυναμίες κατά μέλη έχουμε:

$$923^2 \cdot 933^2 \cdot 937^2 = 2^2 \cdot 5^6 \cdot 13^4 \cdot 17^2 \bmod n \;.$$

Αν $t = 922 \cdot 933 \cdot 937$ και $s = 2 \cdot 5^3 \cdot 13^2 \cdot 17$ έχουμε $t^2 = s^2 \bmod n$ και $t \neq \pm s \bmod n$. Κατόπιν υπολογίζουμε τους μέγιστους κοινούς διαιρέτες $(t+s,n) = 1229$ και $(t-s,n) = 691$, οι οποίοι μας δίνουν δύο γνήσιους παράγοντες του n. ■

Παράδειγμα 3.4: Θα παραγοντοποιήσουμε τον $n = 93623\ (= 373 \cdot 251)$.

Θεωρώ τη βάση $B = \{-1, 2, 3, 5, 7, 11, 13\}$ με 7 στοιχεία άρα θα προσπαθήσω να βρω 8 B-προσαρμοσμένους ακεραίους ως προς τον $n = 93623$.

Παρατηρώ ότι και τα 7 στοιχεία της B δεν διαιρούν τον n. Δοκιμάζω $\lfloor \sqrt{kn} \rfloor + j$ με $j, k = 1, ..., 9$.

Έχουμε:

$\sqrt{n} \simeq 305,9...$ άρα αρχίζω με $b_1 : 306^2 = 93636 = 13 \bmod n \in B$

$\sqrt{2n} \simeq 432,...$ ο $b_2 : 433^2 = 187.489 = 243 = 3^5 \bmod n,\ 3 \in B$

$\sqrt{3n} < 530$ ο $b_3 : 531^2 = 281.961 = 1092 = 2^2 \cdot 3 \cdot 7 \cdot 13 \in B,$

και ο $b_4 : 537^2 = 288.369 = 7500 = 2^2 \cdot 3 \cdot 5^4 \in B$

$\sqrt{4n} < 612$ και ο $b_5 : 612^2 = 374.544 = 52 = 2^2 \cdot 13 \in B$

$\sqrt{5n} < 750$ και δεν δίνει ανάλυση $\in B$ κανένας αριθμός στο διάστημα $750 \ldots 759$

$\sqrt{6n} \sim 809,...$ και ο $b_6 : 809^2 = 654.481 = -880 = -2^4 \cdot 5 \cdot 11 \in B$

$\sqrt{7n} \sim 865,...$ και ο $b_7 : 866^2 = 749.956 = 972 = 2^4 \cdot 3^5 \in B$

$\sqrt{8n} \sim 917,...$ και ο $b_8 : 918^2 = 842.724 = 117 = 3^5 \cdot 13 \in B$

οπότε έχω στο $\mathbb{Z}_2^7$ τα 8 διανύσματα:

$u_1 = (0\ 0\ 0\ 0\ 0\ 0\ 1)$ $u_5 = (0\ 0\ 0\ 0\ 0\ 0\ 1)$

$u_2 = (0\ 0\ 1\ 0\ 0\ 0\ 0)$ $u_6 = (1\ 0\ 0\ 1\ 0\ 1\ 0)$

$u_3 = (0\ \underline{0}\ 1\ 0\ 1\ 0\ 1)$ το 2^2 έδωσε 0 $u_7 = (0\ 0\ 1\ 0\ 0\ 0\ 0)$

$u_4 = (0\ 0\ 1\ 0\ 0\ 0\ 0)$ $u_8 = (0\ 0\ 0\ 0\ 0\ 0\ 1)$

Θεωρώ το γραμμικό ομογενές σύστημα $x_1\overline{u_1} + x_2\overline{u_2} + \ldots + x_8\overline{u_8} = 0 \bmod 2$.

Έχουμε:

$$\left.\begin{array}{c} x_6 = 0 \\ x_2 + x_3 + x_4 + x_7 = 0 \\ x_3 = 0 \\ x_1 + x_3 + x_5 + x_8 = 0 \end{array}\right\} \bmod 2 \ .$$

Μία λύση του συστήματος είναι:

$$\begin{aligned} &x_1 = x_5 = 1 \\ &x_2 = x_3 = x_4 = x_6 = x_7 = x_8 = 0 \ . \end{aligned}$$

Άρα το $I = \{x_1, x_5\}$. Θα υπολογίσω τα b, c.

$$b = \prod_{i \in I} b_i = b_1 b_5 = 306.612 = 187.272 \ .$$
$$c^2 = 13 \cdot 2^2 \cdot 13 \Rightarrow c^2 = 2^2 \cdot 13^2 \Rightarrow c = 26 \ .$$

Αλλά $187.272 = 26 \bmod n$ [πράγματι $187.272 - 26 = 187.246 = 2 \cdot 93623$] άρα δεν μπορούμε να υπολογίσουμε μη τετριμμένο παράγοντα του n.

Βρίσκω μια άλλη λύση του συστήματος δηλαδή την:

$$\left.\begin{array}{l} x_2 = x_4 = 1 \\ x_1 = x_3 = x_5 = x_6 = x_7 = x_8 = 0 \end{array}\right\} I'$$

Τότε $b = 433 \cdot 537 = 232.521$

και $c^2 = 3^5 \cdot 2^2 \cdot 3 \cdot 5^4 = 2^2 \cdot 3^6 \cdot 5^4 = \left(2 \cdot 3^3 \cdot 5^2\right)^2 \Rightarrow c = 2 \cdot 3^3 \cdot 5^2 = 1350$.

Αλλά $232.521 = 45.275 \bmod n \Rightarrow b \neq \pm c \bmod n$.

Άρα $\text{ΜΚΔ}(b + c, n) = (233.871,\ 93.623)$

233.871	93.623
46.625	93.623
46.625	373
0	373

Άρα $\text{ΜΚΔ} = 373.$

Άρα $93.623 = 373 \cdot 251$.

■

Όταν έχουμε να κάνουμε με σύνθετους ακέραιους οι οποίοι έχουν ένα πρώτο παράγοντα p τέτοιον ώστε ο p-1 να είναι γινόμενο μικρών πρώτων τότε ένας αποτελεσματικός αλγόριθμος είναι ο αλγόριθμος p-1 του Pollard (1974).

Αλγόριθμος p-1 του Pollard:

Ας είναι n ένας σύνθετος περιττός ακέραιος. Ακολουθούμε τα εξής βήματα:

1. Επιλέγουμε ένα θετικό ακέραιο B και υπολογίζουμε το γινόμενο
$$k = \prod_{q \le B} q^{\left[\log_q B\right]},$$
όπου q διατρέχει το σύνολο των πρώτων $\le B$.
2. Επιλέγουμε έναν ακέραιο α με $1 < a < n$ και υπολογίζουμε τον μέγιστο κοινό διαιρέτη $\delta = (\alpha, n)$.
3. Αν $\delta > 1$, τότε ο δ είναι ένας μη τετριμμένος παράγοντας του n. Αν $\delta = 1$, τότε υπολογίζουμε τον μέγιστο κοινό διαιρέτη $d = (a^k - 1, n)$.
4. Αν $1 < d < n$, τότε ο d είναι ένας μη τετριμμένος παράγοντας του n. Αν $d = 1$ ή n, τότε επιλέγουμε έναν άλλο ακέραιο B και επαναλαμβάνουμε την παραπάνω διαδικασία.

Αν λοιπόν ο p είναι πρώτος παράγοντας του n και κάθε δύναμη πρώτου που διαιρεί τον p-1 είναι $\le B$ τότε ο p-1 διαιρεί τον k. Άρα $a^k \equiv 1 (\mathrm{mod}\, p)$. Επομένως ο p διαιρεί τον $a^k - 1$. Έτσι αν $d \ne n$, τότε $1 < d < n$ και επομένως ο d είναι ένας μη τετριμμένος παράγοντας του n.

Παράδειγμα 3.5:

1. Θέλουμε να παραγοντοποιήσουμε τον αριθμό $n = 1.241.143$.
Ας πάρουμε $B = 13$.
Τότε $k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 360.360$.
Κατόπιν υπολογίζουμε τον $\text{ΜΚΔ}(2^k - 1, n) = 547$. Άρα $n = 2269 \cdot 547$ που είναι και οι δύο πρώτοι.
2. Θέλουμε να παραγοντοποιήσουμε τον αριθμό $n = 1.127.041$.
Παίρνουμε $B = 19$.
Τότε $k = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 232.792.560$.
Κατόπιν υπολογίζουμε τον $\text{ΜΚΔ}(2^k - 1, n) = 761$. Άρα $n = 1481 \cdot 761$ που είναι και οι δύο πρώτοι. ■

Πολυπλοκότητα:

Αφού κάθε παράγοντας του k είναι μικρότερος της βάσης B, $k < B^B$ και ο k υπολογίζεται σε χρόνο $O\left((B\log B)^2\right)$.

Ο $\text{ΜΚΔ}(a,n)$ υπολογίζεται σε χρόνο $O\left((\log n)^2\right)$ και ο $\text{ΜΚΔ}\left(a^k-1,n\right)$ υπολογίζεται σε χρόνο $O\left((1+\log k)(\log n)^2+\log n\right)$. Οπότε, ο χρόνος που απαιτείται για να παραγοντοποίησουμε το n με τον p-1 αλγόριθμο Pollard είναι συνολικά $O\left(B^2(\log B)^2(\log n)^2\right)$. Έτσι αν $B=O\left((\log n)^i\right)$ με i θετικό ακέραιο ο αλγόριθμος είναι πολυωνυμικού χρόνου σαν συνάρτηση του logn, όμως τέτοια επιλογή του B μειώνει αρκετά την πιθανότητα επιτυχίας. Αν όμως αυξήσουμε δραστικά το μέγεθος της βάσης B, ο αλγόριθμος αποδεικνύεται επιτυχής αλλά πολύ πιο αργός.

Είναι αρκετά εύκολο να κατασκευάσουμε ακεραίους οι οποίοι να παραγοντοποιούνται δύσκολα από αυτή τη μέθοδο. Για παράδειγμα μπορούμε να βρούμε μεγάλους πρώτους p_1 και q_1 έτσι ώστε οι ακέραιοι $p=2p_1+1$ και $q=2q_1+1$ να είναι πρώτοι. Οπότε, ο ακέραιος $n=p\cdot q$ δεν θα μπορεί ναπαραγοντοποιηθεί με τον p-1 αλγόριθμο.

Σήμερα, ο ***αλγόριθμος του Lenstra***, μια γενίκευση και βελτίωση της διαδικασίας του Pollard (παραγοντοποίηση με ελλειπτικές καμπύλες) αποτελεί πολύ πιο χρήσιμη μέθοδο από αυτήν του Pollard.

Συνεχίζουμε με τον ***αλγόριθμο Pollard Rho*** ή αλλιώς με την ***μέθοδο Monte Carlo*** όπως είναι γνωστός.

Βασική Ιδέα: Έστω p ο μικρότερος πρώτος διαιρέτης του n, και $x,\ x'$ ακέραιοι στο $\mathbb{Z}_n$ τ.ω. $x \neq x'$ και $x \equiv x' \bmod p$. Τότε $p \leq \text{ΜΚΔ}(x-x', n) < n$ και έτσι υπολογίζοντας τον ΜΚΔ βρίσκουμε έναν μη τετριμμένο παράγοντα του n. Υποθέτουμε τώρα ότι θέλουμε να παραγοντοποιήσουμε τον n επιλέγοντας πρώτα ένα τυχαίο υποσύνολο X του $\mathbb{Z}_n$ και υπολογίζοντας έπειτα τους $\text{ΜΚΔ}(x-x', n)$ για όλα τα x, x' στο X, με $x \neq x'$. Η μέθοδος θα ήταν όμως επιτυχής μόνο στην περίπτωση που η απεικόνιση $x \to x \bmod p$ οδηγεί σε μία τουλάχιστον «σύγκρουση» για το $x \in X$. Η περίπτωση αυτή στηρίζεται στο *παράδοξο των γενεθλίων* το οποίο περιγράφουμε πιο κάτω.

Ορισμός: Μια σύγκρουση (collision) της συνάρτησης f είναι ένα ζεύγος (x, x') στο πεδίο ορισμού για το οποίο ισχύει $x \neq x'$ και $f(x) = f(x')$.

Το ***παράδοξο των γενεθλίων*** στη θεωρία πιθανοτήτων αναφέρεται σε ένα πρόβλημα το οποίο κατά την κοινή λογική έχει μια απίθανη απάντηση. Μία από τις μορφές του προβλήματος είναι:

> *Σε μία ομάδα 23 ατόμων τι πιθανότητα υπάρχει δύο από αυτά τα άτομα να έχουν την ίδια ημέρα γενέθλια;*

Η "πιθανά προφανής" απάντηση είναι 23/365=0,063 δηλαδή έξι τοις εκατό. Η μαθηματική λύση όμως μας δίνει 50%!

Ακόμα πιο εντυπωσιακά το ποσοστό γίνεται 99% με μόνο 57 άτομα ενώ είναι 100% με 367 άτομα, συμπεριλαμβανομένων και αυτών που έχουν γεννηθεί στις 29 Φεβρουαρίου!

Από μαθηματικής άποψης, αν μια συνάρτηση f παράγει μια τιμή μεταξύ n διαφορετικών τιμών με την ίδια πιθανότητα και το n είναι αρκετά μεγάλο, τότε υπολογίζοντας τη συνάρτηση για ένα πλήθος περίπου 1,17 διαφορετικών εισόδων περιμένουμε να βρούμε ένα ζεύγος εισόδων x και x' $(x \neq x')$ τέτοια ώστε $f(x) = f(x')$.

Παραγοντοποίηση μονού ακεραίου n:

Θεωρούμε τη συνάρτηση $f(x)=x^2+a$ όπου α μικρή σταθερά, συνήθως $a=1$.

Έστω $x_1 \in \mathbb{Z}_n$ και $X \subseteq \mathbb{Z}_n$ με

$$X=\left\{x_1, x_2, ..., x_m \mid x_j = f\left(x_{j-1}\right) \bmod n \ \ \forall j=2,...m\right\}.$$

Σκοπός είναι η εύρεση δύο διαφορετικών τιμών $x_i, x_j \in X$ τέτοιες ώστε $\text{ΜΚΔ}\left(x_j - x_i, n\right) > 1$. Κάθε φορά που υπολογίζουμε έναν καινούριο όρο x_j της ακολουθίας, μπορούμε να υπολογίζουμε τους $\text{ΜΚΔ}\left(x_j - x_i, n\right)$ για όλα τα $i < j$.

Αυτό όμως θα απαιτούσε $\binom{|X|}{2} = \binom{m}{2}$ υπολογισμούς, περισσότερους από $p/2$.

Ο αριθμός των υπολογισμών αυτών για εύρεση μη τετριμμένου παράγοντα του n μπορεί να μειωθεί και σ' αυτό ακριβώς έγκειται η μέθοδος Pollard Rho.

Έστω μια σύγκρουση $x_i \equiv x_j (\bmod p)$. Η f είναι πολυωνυμική συνάρτηση με ακέραιους συντελεστές οπότε $f(x_i) \equiv f\left(x_j\right) (\bmod p)$. Από την κατασκευή του υποσυνόλου X

έχουμε ότι $x_i = f\left(x_{j-1}\right) (\bmod p) \quad \forall j=2,...m$. Τότε

$$x_{i+1} \bmod p = \left(f\left(x_i\right) \bmod n\right) \bmod p = f\left(x_i\right) \bmod p, \text{ αφού } p \mid n.$$

Ομοίως $x_{j+1} \bmod p = \left(f\left(x_j\right) \bmod n\right) \bmod p = f\left(x_j\right) \bmod p$.

Έτσι θα έχουμε $x_{i+1} \equiv x_{j+1} (\bmod p)$ και επαναλαμβάνοντας τη διαδικασία καταλήγουμε στα εξής σημαντικά αποτελέσματα:

Αν $x_i \equiv x_j (\bmod p)$ τότε $x_{i+\delta} \equiv x_{j+\delta} (\bmod p), \ \forall \delta \geq 0$. (1)

Θέτοντας $l = j-1$ τότε $x_{i'} \equiv x_{j'} (\bmod p)$ αν $j' > i' \geq i$ και $j' - i' \equiv 0 \bmod l$. (2)

Αν $x_i \equiv x_j (\bmod p)$ τότε $x_{i'} \equiv x_{2i'} (\bmod p), \ \forall i' = 0 \bmod l$ και $i' \geq i$. (3)

Αλγόριθμος p του Pollard (αλγόριθμος Po):

1. Επιλέγουμε $x_1 \in \mathbb{Z}_n$, και υπολογίζουμε το $x_2 = f(x_1) = x_1^2 + 1 \pmod{n}$.
   Υπολογίζουμε τον $\text{ΜΚΔ}(x_2 - x_1, n) = p$.
   Αν $p = 1$ προχωράμε στο βήμα 2.

2. Υπολογίζουμε τους ακεραίους $x_i = f(x_{i-1}) \bmod n$ και $x_{2i} = f(x_{2i-1}) \bmod n$ και βρίσκουμε τον $\text{ΜΚΔ}(x_{2i} - x_i, n) = p$ για $i = 2$.
   Αν $i < p < n$ τότε $x_i \equiv x_{2i} \pmod{p}$ και p είναι μη τετριμμένος παράγοντας του n.
   Αν $p = n$ ο αλγόριθμος επιστρέφει μήνυμα «αποτυχία».
   Αν $p = 1$ επαναλαμβάνουμε το βήμα 2 για $i = 3$, έπειτα για $i = 4$ κ.ο.κ.

<u>Πολυπλοκότητα αλγορίθμου Pollard Rho:</u>

Αν $x_i \equiv x_j \pmod{p}$ τότε μεταξύ των l ακεραίων $i, \ldots, j-1$ θα υπάρχει κάποιο $i' \geq i$ πολλαπλάσιο του $l = j - 1$ και από τη σχέση (3) θα έχουμε ότι $x_{i'} \equiv x_{2i'} \pmod{p}$. Οπότε πράγματι ο αλγόριθμος θα εντοπίσει μία σύγκρουση (όχι κατ' ανάγκη την πρώτη) και θα δώσει ένα μη τετριμμένο παράγοντα του n, τον $p = \text{ΜΚΔ}(x_{2i'} - x_{i'}, n)$.

Ο i' εντοπίζεται το πολύ σε j βήματα, άρα στη χειρότερη περίπτωση ο αλγόριθμος απαιτεί j επαναλήψεις για να βρει μία σύγκρουση και επομένως να δώσει τον παράγοντα p. Ο αναμενόμενος αριθμός επαναλήψεων μειώνεται στις $\sqrt{p}$ και επειδή $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα προκύπτει $O(n^{1/4})$.

Είναι πιθανό ο αλγόριθμος να μην εντοπίσει έναν μη τετριμμένο παράγοντα του n. Αυτό όμως συμβαίνει μόνο στην περίπτωση που οι τιμές x και x' που εμφανίζουν την πρώτη σύγκρουση, ικανοποιούν στην ουσία τη σχέση $x \equiv x' \bmod n$ αντί απλά της $x \equiv x' \bmod p$. Η πιθανότητα για αυτήν την περίπτωση είναι περίπου p/n, αρκετά μικρή αν ο n είναι μεγάλος (γιατί $p < \sqrt{n}$). Αν ο αλγόριθμος αποτύχει με αυτό τον τρόπο τότε επαναλαμβάνουμε τα βήματα επιλέγοντας διαφορετική αρχική τιμή ή διαφορετική συνάρτηση f.

Παράδειγμα 3.6:

Έστω $n = 7171,\ f(x) = x^2 + 1$ και $x_1 = 1$. Ζητείται παραγοντοποίηση του n.

Βήμα 1: $x_1 = 1,\ x_2 = f(x_1) = 1^1 + 1 = 2 \bmod 7171,$

$$\gcd(2-1, 7171) = \gcd(1, 7171) = 1.$$

Βήμα 2: $x_2 = 2,\ x_2 = f(x_2) = 2^2 + 1 = 5 \bmod 7171,$

$$x_4 = f(x_3) = 5^2 + 1 = 26 \bmod 7171, \quad \gcd(x_4 - x_2, n) = \gcd(24, 7171) = 1.$$

Βήμα 3: $x_3 = 5\ x_5 = f(x_4) = 26^2 + 1 = 677 \bmod 7171,$

$$x_6 = f(x_5) = 677^2 + 1 = 458330 \bmod 7171 = 6557,$$

$$\gcd(x_6 - x_3, n) = \gcd(6552, 7171) = 1.$$

Βήμα 4: $x_4 = 26,\ x_5 = 677,\ x_6 = 6557$

$$x_7 = f(x_6) = 6557^2 + 1 = 42994250 = 4105 \bmod 7171,$$

$$x_8 = f(x_7) = 4105^2 + 1 = 16851026 = 6347 \bmod 7171,$$

$$\gcd(x_8 - x_4, n) = \gcd(6321, 7171) = 1.$$

Βήμα 5: $x_5 = 677,\ x_6 = 6557,\ x_7 = 4105,\ x_1 = 6347 \bmod 7171,$

$$x_9 = f(x_8) = 6347^2 + 1 = 40284410 = 4903 \bmod 7171,$$

$$x_{10} = f(x_9) = 4903^2 + 1 = 24039410 = 2218 \bmod 7171,$$

$$\gcd(x_{10} - x_5, n) = \gcd(1541, 7171) = 1.$$

Βήμα 6: $x_6 = 6557,\ \ x_7 = 4105,\ \ x_8 = 6347,\ \ x_9 = 4903,\ \ x_{10} = 2218,$

$x_{11} = f(x_{10}) = 2218^2 + 1 = 4919525 = 219 \bmod 7171,$

$x_{12} = f(x_{11}) = 219^2 + 1 = 47962 = 219 \bmod 7171,$

$\gcd(x_6 - x_{12}, n) = \gcd(2116, 7171) = 1.$

Βήμα 7: $x_7 = 4105,\ \ x_8 = 6347,\ \ x_9 = 4903,\ \ x_{10} = 2218,\ \ x_{11} = 219,\ \ x_{12} = 4936,$

$x_{13} = f(x_{12}) = 4936^2 + 1 = 24364097 = 4210 \bmod 7171,$

$x_{14} = f(x_{13}) = 4210^2 + 1 = 17724101 = 4560 \bmod 7171,$

$\gcd(x_{14} - x_7, n) = \gcd(455, 7171) = 1.$

Βήμα 8: $x_8 = 6347,\ \ x_9 = 4903,\ \ x_{10} = 2218,\ \ x_{11} = 219,\ \ x_{12} = 4936,\ \ x_{13} = 4210,$

$x_{14} = 4560,$

$x_{15} = f(x_{14}) = 4560^2 + 1 = 20793601 = 4782 \bmod 7171,$

$x_{16} = f(x_{15}) = 4872^2 + 1 = 23736385 = 375 \bmod 7171,$

$\gcd(x_8 - x_{16}, n) = \gcd(5972, 7171) = 1.$

Βήμα 9:

$x_9 = 4903,\ \ x_{10} = 2218,\ \ x_{11} = 219,\ \ x_{12} = 4936,\ \ x_{13} = 4210,\ \ x_{14} = 4560,$

$x_{15} = 4872,\ \ x_{16} = 375,$

$x_{17} = f(x_{16}) = 375^2 + 1 = 140626 = 4377 \bmod 7171,$

$x_{18} = f(x_{17}) = 4377^2 + 1 = 19158130 = 4389 \bmod 7171,$

$\gcd(x_9 - x_{18}, n) = \gcd(514, 7171) = 1.$

Βήμα 10: $x_{10} = 2218,\ x_{11} = 219,\ x_{12} = 4936,\ x_{13} = 4210,\ x_{14} = 4560,$

$x_{15} = 4872,\ x_{16} = 375,\ x_{17} = 4377,\ x_{18} = 4389,$

$x_{19} = f(x_{18}) = 4389^2 + 1 = 19263322 = 2016 \bmod 7171,$

$x_{20} = f(x_{19}) = 2016^2 + 1 = 4064257 = 5471 \bmod 7171,$

$\gcd(x_{20} - x_{10}, n) = \gcd(3253, 7171) = 1.$

Βήμα 11: $x_{11} = 219,\ x_{12} = 4936,\ x_{13} = 4210,\ x_{14} = 4560,\ x_{15} = 4872,\ x_{16} = 375,$

$x_{17} = 4377,\ x_{18} = 4389,\ x_{19} = 2016,\ x_{20} = 5471,$

$x_{21} = f(x_{20}) = 5471^2 + 1 = 29931842 = 88 \bmod 7171,$

$x_{22} = f(x_{21}) = 88^2 + 1 = 7745 = 574 \bmod 7171,$

$\gcd(x_{22} - x_{11}, n) = \gcd(355, 7171) = 71.$

Άρα τελικά, μετά από 11 επαναλήψεις ο αλγόριθμος εντόπισε τη σύγκρουση $x_{11} \equiv x_{12} (\bmod p) = 6$ και τον μη τετριμμένο παράγοντα $p = 71$ του 7171. Έτσι, $n = 7171 = 71 \times 101$. Η πρώτη σύγκρουση είναι η $x_7 \bmod 71 = x_{18} \bmod 71 = 58$. ■

Βιβλιογραφία

1. Κουκουβίνος Χ., Παπαϊωάννου Α., «Κρυπτογραφία», Ε.Μ.Π., Αθήνα 2007.

2. Κουκουβίνος Χ., Παπαϊωάννου Α., «Θεωρία Πληροφοριών και Κωδίκων», Ε.Μ.Π., Αθήνα 2002.

3. Κουκουβίνος Χ., Παπαϊωάννου Α., «Θεωρία Σχεδιασμών», Ε.Μ.Π., Αθήνα 2002.

4. Menezes A., van Oorschot P. Vanstone S., "Handbook of Applied Cryptografy", 1996.

5. Πουλάκης Δ., «Θεωρία Αριθμών», Ζήτης, 2004.

6. Πουλάκης Δ., «Κρυπτογραφία», Ζήτης, 2004.

7. Singh S., Κώδικες και Μυστικά, Τραυλός 2003 (ιστορική αναδρομή κρυπτολογίας).

8. Stinson D., "Cryptografy. Theory and Practice", third ed., Chapman and Hall, 2006.

9. Ε. Ζάχος, «Αλγόριθμοι και πολυπλοκότητα», Ε.Μ.Π., 2003.

10. Ε. Ζάχος, «Εισαγωγή στη Θεωρία Αριθμών και την Κρυπτολογία», Ε.Μ.Π., 2003.

11. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 780, 1996.

12. Bruce Schneier, Applied Cryptography, 2nd edition, Wiley, 758, 1996

13. Douglas R. Stinson, Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), 1st edition, CRC Press, 434, 1995.

14. Wenbo Mao, Modern Cryptography: Theory and Practice, 1st edition, Prentice Hall PTR, 740, 2003.

15. William Stallings, Cryptography and Network Security: Principles and Practice, 2nd Edition, Prentice Hall, 569, 1998.

16. Henk C.A. van Tilborg, Fundamentals of Cryptology : A Professional Reference and Interactive Tutorial, 1 edition, Springer, 512, 1999.

17. David Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Scribner, 1200, 1996.

18. Β.Α. Κάτος - Γ.Χ. Στεφανίδης, Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, ΖΥΓΟΣ, 396, 2003.