ΑΛΓΟΡΙΘΜΟΙ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΜΕΡΟΣ Ι

ΒΑΣΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ & ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΑΛΓΟΡΙΘΜΟΙ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

- Οι κρυπτογραφικές μέθοδοι βασίζονται σε υπολογιστικά δύσκολα προβλήματα, τα οποία όμως απαιτούν αποδοτικούς αλγορίθμους για τις βοηθητικές πράξεις τους.
- Θα συζητήσουμε για βασικούς αλγόριθμους θεωρίας αριθμών και εξειδικευμένους αλγορίθμους για κρυπτογραφικά προβλήματα, όπως: **ο έλεγχος πρώτων, η παραγοντοποίηση και ο διακριτός λογάριθμος.**

ΑΛΓΟΡΙΘΜΟΣ ΕΠΑΝΑΛΑΜΒΑΝΟΜΕΝΟΥ ΤΕΤΡΑΓΩΝΙΣΜΟΥ

- Χρησιμοποιείται για τον αποδοτικό υπολογισμό μεγάλων δυνάμεων modulo n, δηλαδή $\alpha^E \ (mod\ n)$.
- Η βασική ιδέα είναι η ανάλυση του εκθέτη E σε δυαδική μορφή και η εκτέλεση διαδοχικών τετραγωνισμών και πολλαπλασιασμών.
- **Πολυπλοκότητα:** Έχει πολυπλοκότητα O(logE), πολύ πιο αποδοτική από την απλή διαδοχική εκτέλεση E πολλαπλασιασμών.

ΠΑΡΑΔΕΙΓΜΑ 1: ΕΠΑΝΑΛΑΜΒΑΝΟΜΕΝΟΣ ΤΕΤΡΑΓΩΝΙΣΜΟΣ

- **Πρόβλημα:** Υπολογίστε το $3^{23} \pmod{13}$.
- **Λύση:** Ο εκθέτης $23 = 16 + 4 + 2 + 1 = (10111)_2$.
- Υπολογισμός δυνάμεων του 2:
  - $3^1 \equiv 3 \pmod{13}$
  - $3^2 \equiv 9 \pmod{13}$
  - $3^4 \equiv 9^2 = 81 \equiv 3 \pmod{13}$
  - $3^8 \equiv 3^2 = 9 \pmod{13}$
  - $3^{16} \equiv 9^2 = 81 \equiv 3 \pmod{13}$
- **Τελικό αποτέλεσμα:** $3^{23} = 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^1 \equiv 3 \cdot 3 \cdot 9 \cdot 3 = 243 \equiv \mathbf{9} \pmod{13}$.

ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ ΕΥΚΛΕΙΔΗ

- Χρησιμοποιείται για τον υπολογισμό του Μέγιστου Κοινού Διαιρέτη (ΜΚΔ) δύο ακεραίων a,b, δηλαδή gcd(a,b).
- Βασίζεται στην ιδιότητα: gcd(a,b)=gcd(b,a(modb)).
- Είναι από τους παλαιότερους και πιο αποδοτικούς αλγορίθμους

ΕΚΤΕΤΑΜΕΝΟΣ ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ ΕΥΚΛΕΙΔΗ

- Εκτός από τον gcd(a,b), βρίσκει και ακέραιους x,y (συντελεστές Bézout) τέτοιους ώστε ax+by=gcd(a,b).
- Είναι κρίσιμος για τον υπολογισμό του πολλαπλασιαστικού αντίστροφου α^{-1} (modn), ο οποίος υπάρχει αν gcd(a,n)=1.
- Αν gcd(a,n)=1, τότε ax+ny=1, και άρα $ax \equiv 1 (\mathrm{mod}\ n)$, δηλαδή x είναι ο αντίστροφος του a.

ΠΑΡΑΔΕΙΓΜΑ 2: ΑΝΤΙΣΤΡΟΦΟΣ ΜΕ ΕΚΤΕΤΑΜΕΝΟ ΑΛΓΟΡΙΘΜΟ ΤΟΥ ΕΥΚΛΕΙΔΗ

- **Πρόβλημα:** Υπολογίστε τον πολλαπλασιαστικό αντίστροφο του $28 \pmod{51}$.

- **Λύση:** Εφαρμόζουμε τον Εκτεταμένο Ευκλείδειο Αλγόριθμο για $\gcd(51, 28)$.

  1. $51 = 1 \cdot 28 + 23$
  2. $28 = 1 \cdot 23 + 5$
  3. $23 = 4 \cdot 5 + 3$
  4. $5 = 1 \cdot 3 + 2$
  5. $3 = 1 \cdot 2 + \mathbf{1}$

- Αναστρέφουμε τις πράξεις για να βρούμε τους συντελεστές x, y ώστε $51y$ 1.
  - $1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5$
  - $1 = 2 \cdot (23 - 4 \cdot 5) - 1 \cdot 5 = 2 \cdot 23 - 9 \cdot 5$
  - $1 = 2 \cdot 23 - 9 \cdot (28 - 1 \cdot 23) = 11 \cdot 23 - 9 \cdot 28$
  - $1 = 11 \cdot (51 - 1 \cdot 28) - 9 \cdot 28 = 11 \cdot 51 - \mathbf{20} \cdot 28$

- $-20 \cdot 28 \equiv 1 \pmod{51}$. Ο αντίστροφος είναι $-20 \equiv \mathbf{31} \pmod{51}$.

ΜΕΡΟΣ ΙΙ

ΑΛΓΟΡΙΘΜΟΙ ΠΡΩΤΩΝ & ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ

PRIMALITY (ΕΛΕΓΧΟΣ ΠΡΩΤΩΝ) ΚΑΙ FACTORING (ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ)

- **Primality Testing:** Το πρόβλημα του ελέγχου αν ένας αριθμός N είναι πρώτος. Χρησιμοποιείται για την παραγωγή μεγάλων πρώτων αριθμών (π.χ., στο RSA). Υπάρχουν αποδοτικοί αλγόριθμοι (π.χ., Miller-Rabin).
- **Factoring:** Το πρόβλημα της εύρεσης των πρώτων παραγόντων ενός σύνθετου αριθμού N. Η δυσκολία του είναι η βάση ασφαλείας του κρυπτοσυστήματος RSA. Είναι ένα υπολογιστικά δύσκολο πρόβλημα.

ΑΛΓΟΡΙΘΜΟΙ ΕΛΕΓΧΟΥ ΠΡΩΤΩΝ (PRIMALITY TESTING)

- **Probabilistic:** Αλγόριθμοι που δίνουν απάντηση με υψηλή πιθανότητα (π.χ., Miller-Rabin, Fermat Test). Είναι ταχύτεροι και πιο συχνά χρησιμοποιούμενοι στην πράξη.
- **Deterministic:** Αλγόριθμοι που δίνουν σίγουρη απάντηση, όπως ο AKS (Agrawal-Kayal-Saxena). Ο AKS είναι ο πρώτος πολυωνυμικός ντετερμινιστικός αλγόριθμος.

FERMAT PRIMALITY TEST

- **Θεωρητική Βάση:** Μικρό Θεώρημα του Fermat: Αν p είναι πρώτος και $\gcd(a, p) = 1$, τότε $a^{p-1} \equiv 1 \pmod{p}$.
- **Έλεγχος:** Επιλέγουμε τυχαία μια βάση a. Αν $a^{N-1} \not\equiv 1 \pmod{N}$, τότε ο N είναι σίγουρα σύνθετος.
- **Αδυναμία:** Υπάρχουν σύνθετοι αριθμοί (αριθμοί Carmichael) για τους οποίους $a^{N-1} \equiv 1 \pmod{N}$ για όλες τις βάσεις a που είναι σχετικά πρώτες με το N.

MILLER-RABIN PRIMALITY TEST

- Ο πιο δημοφιλής πιθανοτικός αλγόριθμος για τον έλεγχο πρώτων.
- Είναι πιο ισχυρός από το Fermat Test, καθώς δεν υπάρχουν "ψευδοπρώτοι" για όλες τις βάσεις (όπως οι αριθμοί Carmichael).
- **Ασφάλεια:** Αν ο αριθμός N είναι σύνθετος, τότε για κάθε τυχαία επιλογή βάσης α, η πιθανότητα να μην εντοπιστεί ως σύνθετος είναι το πολύ 1/4. Επαναλαμβάνοντας τον έλεγχο k φορές, η πιθανότητα λάθους μειώνεται στο $1/4^k$.

ΑΛΓΟΡΙΘΜΟΙ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ (FACTORING ALGORITHMS)

- Οι αλγόριθμοι παραγοντοποίησης είναι κρίσιμοι για την κρυπτανάλυση του RSA.
- **Απλοί Αλγόριθμοι:** Δοκιμαστική διαίρεση (Trial Division).
- **Εξειδικευμένοι Αλγόριθμοι:**

1. Pollard's ρ-Method: Κατάλληλη για αριθμούς με μικρό παράγοντα.

2. Quadratic Sieve (QS) / Number Field Sieve (NFS): Οι πιο αποδοτικοί αλγόριθμοι για μεγάλους αριθμούς.

ΜΕΘΟΔΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ρ ΤΟΥ POLLARD

- **Σκοπός:** Εύρεση ενός μικρού παράγοντα ρ ενός σύνθετου αριθμού N.
- **Βασική Ιδέα:** Βασίζεται στο Παράδοξο των Γενεθλίων (Birthday Paradox) για να βρει δύο αριθμούς x_i, x_j τέτοιους ώστε $x_i \equiv x_j \pmod{\rho}$, αλλά $x_i \not\equiv x_j \pmod{N}$. Αυτό σημαίνει ότι $\gcd(|x_i - x_j|, N)$ θα δώσει τον παράγοντα ρ.

ΠΑΡΑΔΕΙΓΜΑ 3: ΜΕΘΟΔΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ρ ΤΟΥ POLLARD

- **Πρόβλημα:** Εφαρμόστε τη μέθοδο παραγοντοποίησης ρ για παραγοντοποίηση του αριθμού 77.
- **Λύση:** Έστω συνάρτηση $f(x) = x^2 + 1 \pmod{77}$.
- Επιλέγουμε αρχική τιμή $x_0 = 2$.
- **Βήμα 1:** $i = 1.\ x_1 = f(x_0) = 2^2 + 1 = 5.$
- **Βήμα 2:** $i = 2.\ x_2 = f(x_1) = 5^2 + 1 = 26 \pmod{77}.$
- **Βήμα 3:** $i = 3.\ x_3 = f(x_2) = 26^2 + 1 = 677 \equiv 61 \pmod{77}.$
- **Έλεγχος ΜΚΔ (για $i = 1$):**
  - $i = 1: x_2 = 26, x_1 = 5.\ \gcd(|x_2 - x_1|, 77) = \gcd(|26 - 5|, 77) = \gcd(21, 77) = \mathbf{7}.$
- **Αποτέλεσμα:** Βρέθηκε ο παράγοντας **7**. Οι παράγοντες του 77 είναι 7 και 11.

ΜΕΡΟΣ ΙΙΙ

ΑΛΓΟΡΙΘΜΟΙ ΔΙΑΚΡΙΤΟΥ ΛΟΓΑΡΙΘΜΟΥ & ΠΡΟΧΩΡΗΜΕΝΑ ΘΕΜΑΤΑ

ΑΛΓΟΡΙΘΜΟΙ ΓΙΑ ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ

- **Ορισμός:** Ο αριθμός a είναι τετραγωνικό υπόλοιπο modulo n αν υπάρχει x τέτοιο ώστε $x^2 \equiv a \pmod{n}$.
- **Εφαρμογή:** Το πρόβλημα εύρεσης τετραγωνικών ριζών modulo σύνθετο αριθμό (π.χ. Rabin Cryptosystem) είναι εξίσου δύσκολο με την παραγοντοποίηση.
- **Σύμβολα Legendre/Jacobi:** Χρησιμοποιούνται για τον αποδοτικό έλεγχο αν ένας αριθμός είναι τετραγωνικό υπόλοιπο (χωρίς απαραίτητα να βρίσκουν τη ρίζα).

ΑΛΓΟΡΙΘΜΟΙ ΔΙΑΚΡΙΤΟΥ ΛΟΓΑΡΙΘΜΟΥ (DLOG)

- **Πρόβλημα DLOG:** Δίνεται μια ομάδα G (συνήθως Z_p^* και στοιχεία α,β $\in$ G. Να βρεθεί ο εκθέτης x τέτοιος ώστε $\alpha^x \equiv \beta \pmod p$.
- **Σημασία:** Η δυσκολία επίλυσης του DLOG είναι η βάση ασφαλείας για κρυπτοσυστήματα όπως το ElGamal και το Diffie-Hellman Key Exchange.

BABY-STEP GIANT-STEP ALGORITHM (BSGS)

- **Σκοπός:** Επίλυση του προβλήματος DLOG σε χρόνο $O(\sqrt{N} \cdot \log N)$, όπου N είναι η τάξη της ομάδας.
- **Βασική Ιδέα:** Αναλύουμε το x ως $x = im - j$, όπου $m \approx \sqrt{N}$. Η εξίσωση $\alpha^x = \beta$ γίνεται $\alpha^{im} \equiv \beta\alpha^j \pmod{p}$.
- Υπολογίζουμε και αποθηκεύουμε τις τιμές $\beta\alpha^j$ ("Baby Steps") και μετά υπολογίζουμε τις τιμές α^{im} ("Giant Steps") μέχρι να βρούμε μια σύγκρουση (match).

ΠΑΡΑΔΕΙΓΜΑ 4: ΜΕΘΟΔΟΣ ΒΑΣΕΩΝ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΓΙΑ DLOG

- **Πρόβλημα:** Η μέθοδος των βάσεων παραγοντοποίησης (Index Calculus) στοχεύει στην εύρεση του διακριτού λογαρίθμου. Δίνεται $B = \{-1, 2, 3, 5\}$, βρείτε έναν παράγοντα του $N = 33$ χρησιμοποιώντας $b_i \in \{6, 8, 9, 12, 14, 15\}$ (σχετικό παράδειγμα άσκησης 4.9).
- **Λύση (Αρχή):** Η μέθοδος δημιουργεί ένα σύστημα γραμμικών εξισώσεων για τους λογαρίθμους των στοιχείων της βάσης B.
- **Εύρεση Παράγοντα του 33:** Για τον $N = 33$, $\sqrt{33} \approx 5.7$.
  - $b_i = 6$: $6^2 = 36 \equiv 3 \pmod{33}$. Έχουμε $6^2 - 3 = 33$.
  - $\gcd(6 - 3, 33) = \gcd(3, 33) = 3$.
  - $\gcd(6 + 3, 33) = \gcd(9, 33) = 3$.
- **Αποτέλεσμα:** Βρέθηκε ο παράγοντας **3**. Αυτή η αρχή (εύρεση ομαλών αριθμών) είναι κεντρική στις μεθόδους Factor Base/Index Calculus.

ΠΑΡΑΔΕΙΓΜΑ 5: ΑΣΦΑΛΕΙΑ ΤΩΝ BITS ΤΟΥ ΔΙΑΚΡΙΤΟΥ ΛΟΓΑΡΙΘΜΟΥ DLOG

- **Παρατήρηση:** Ας υποθέσουμε ότι το πρόβλημα DLOG είναι δύσκολο να λυθεί.
- **Το Τελευταίο Bit (LSB):** Η εύρεση του **τελευταίου bit (LSB)** του διακριτού λογαρίθμου $\log_\alpha \beta$ είναι ένα **εύκολο πρόβλημα.**
- **Άλλα Bits:** Αντίθετα, η εύρεση οποιουδήποτε άλλου bit (του i-οστού bit από το τέλος, για $i \geq 2$) είναι **εξίσου δύσκολη** με την πλήρη επίλυση του προβλήματος DLOG.
- **Συνέπεια:** Αυτό δείχνει ότι, ενώ η πλήρης γνώση του κλειδιού είναι δύσκολη, μια μικρή πληροφορία (το LSB) μπορεί να διαρρεύσει εύκολα χωρίς να παραβιαστεί η συνολική ασφάλεια του DLOG.

ΣΥΝΟΨΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Οπότε στην παρούσα ανάλυση επικεντρωθήκαμε στους θεμελιώδεις αλγορίθμους της θεωρίας αριθμών, οι οποίοι είναι απαραίτητοι τόσο για την αποδοτικότητα όσο και για την ασφάλεια των κρυπτογραφικών συστημάτων δημοσίου κλειδιού.

Βασικοί Αριθμητικοί Αλγόριθμοι: Παρουσιάστηκαν αποδοτικοί αλγόριθμοι για βασικές πράξεις, όπως:

- **Ο Αλγόριθμος Επαναλαμβανόμενου Τετραγωνισμού** για γρήγορο υπολογισμό δυνάμεων modulo.
- **Ο Αλγόριθμος του Ευκλείδη** και ο **Εκτεταμένος Αλγόριθμος του Ευκλείδη** για τον υπολογισμό του Μέγιστου Κοινού Διαιρέτη (ΜΚΔ) και του πολλαπλασιαστικού αντιστρόφου modulo.

ΣΥΝΟΨΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Προβλήματα Υπολογιστικής Δυσκολίας: Είδαμε αλγόριθμους επίλυσης των «σκληρών» προβλημάτων της θεωρίας αριθμών, στα οποία βασίζεται η ασφάλεια των κρυπτοσυστημάτων:

- **Έλεγχος Πρώτων (Primality Testing):** Παρουσιάστηκαν οι Αλγόριθμοι Ελέγχου Πρώτων, οι οποίοι είναι κρίσιμοι για τη δημιουργία των μεγάλων πρώτων αριθμών που χρησιμοποιούνται στο RSA.
- **Παραγοντοποίηση (Factoring):** Εξετάστηκαν οι Αλγόριθμοι Παραγοντοποίησης 5(π.χ. μέθοδος *ρ*, μέθοδος βάσεων παραγοντοποίησης), καθώς η δυσκολία της παραγοντοποίησης μεγάλων σύνθετων αριθμών είναι η βάση του RSA.

ΣΥΝΟΨΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ

- **Διακριτός Λογάριθμος (Discrete Logarithm - DLOG):** Παρουσιάστηκαν οι Αλγόριθμοι Διακριτού Λογαρίθμου. Η δυσκολία επίλυσης του DLOG αποτελεί τη βάση ασφαλείας του ElGamal και του Diffie-Hellman. Επισημαίνεται ότι η εύρεση του τελευταίου bit (LSB) του διακριτού λογαρίθμου είναι εύκολη, αλλά η εύρεση οποιουδήποτε άλλου bit είναι εξίσου δύσκολη με την επίλυση του πλήρους προβλήματος DLOG.
- **Τετραγωνικά Υπόλοιπα:** Κάναμε μια μικρή αναφορά σε Αλγόριθμους για Τετραγωνικά Υπόλοιπα.

ΣΥΝΟΨΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Καταλήγουμε στα εξής συμπεράσματα:

1. Θεμελίωση της Ασφάλειας: Η ασφάλεια των σύγχρονων ασύμμετρων κρυπτοσυστημάτων (δημοσίου κλειδιού) εξαρτάται άμεσα από την υπολογιστική δυσκολία της επίλυσης συγκεκριμένων μαθηματικών προβλημάτων, κυρίως του DLOG και του προβλήματος παραγοντοποίησης. Η ύπαρξη αποδοτικών αλγορίθμων (π.χ., ο αλγόριθμος του Shor στην Κβαντική Κρυπτογραφία) για την επίλυση αυτών των προβλημάτων αποτελεί τη μεγαλύτερη απειλή για τα υπάρχοντα συστήματα.

ΣΥΝΟΨΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ

2. Αποδοτικότητα: Η πρακτική εφαρμογή της κρυπτογραφίας εξαρτάται από την πολυωνυμική πολυπλοκότητα των βασικών αριθμητικών πράξεων. Η χρήση αλγορίθμων όπως ο επαναλαμβανόμενος τετραγωνισμός επιτρέπει την εκτέλεση κρυπτογραφικών πράξεων σε λογικό χρόνο.

3. Επιλεκτική Ασφάλεια: Η κρυπτογραφική ισχύς μπορεί να είναι άνιση εντός του ίδιου προβλήματος. Για παράδειγμα, η «διαρροή» ακόμα και ενός μόνο bit (του LSB) του διακριτού λογαρίθμου δεν θέτει σε κίνδυνο την ασφάλεια του πλήρους κλειδιού, καθώς η εύρεση των υπόλοιπων bits παραμένει εξίσου δύσκολη με την πλήρη επίλυση του προβλήματος DLOG. Αυτό αναδεικνύει τη σημασία της λεπτομερούς κρυπταναλυτικής μελέτης ακόμα και σε επίπεδο bits.

ΕΡΩΤΗΣΕΙΣ ΚΑΙ ΚΡΙΤΙΚΗ ΣΚΕΨΗ

1. Συγκρίνετε τον Miller-Rabin Test με τον Fermat Test. Ποια είναι η κρίσιμη αδυναμία του Fermat που επιλύει ο Miller-Rabin και γιατί είναι σημαντικό αυτό για την κρυπτογραφία;

2. Εξηγήστε γιατί η δυσκολία του Factoring (Παραγοντοποίηση) και του Discrete Logarithm Problem (DLOG) είναι τόσο θεμελιώδης για την ασφάλεια των κρυπτοσυστημάτων Δημοσίου Κλειδιού.

3. Ο Εκτεταμένος Αλγόριθμος του Ευκλείδη είναι ένας ντετερμινιστικός αλγόριθμος. Γιατί είναι απαραίτητος, παρά το γεγονός ότι οι περισσότεροι "δύσκολοι" κρυπτογραφικοί αλγόριθμοι είναι πιθανοτικοί (π.χ., Primality Tests);

ΠΡΟΒΛΗΜΑΤΑ ΕΞΑΣΚΗΣΗΣ

- **Πρόβλημα 1 - (Επαναλαμβανόμενος Τετραγωνισμός):** Υπολογίστε την τιμή της δύναμης $10^{27.200.000.023} \pmod{35}$ με όσο το δυνατόν λιγότερες πράξεις.
- **Πρόβλημα 2 - (Παραγοντοποίηση):** Βρείτε τους παράγοντες του αριθμού 143 εφαρμόζοντας τη μέθοδο $x^2 \equiv y^2 \pmod{N}$ (Διαφορά Τετραγώνων), η οποία σχετίζεται με τις μεθόδους βάσεων παραγοντοποίησης.