ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΚΡΥΠΤΟΓΡΑΦΙΑ

3η Διάλεξη

Κωνσταντίνου Ελισάβετ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

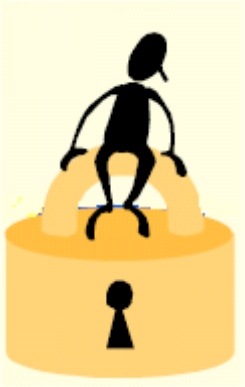
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

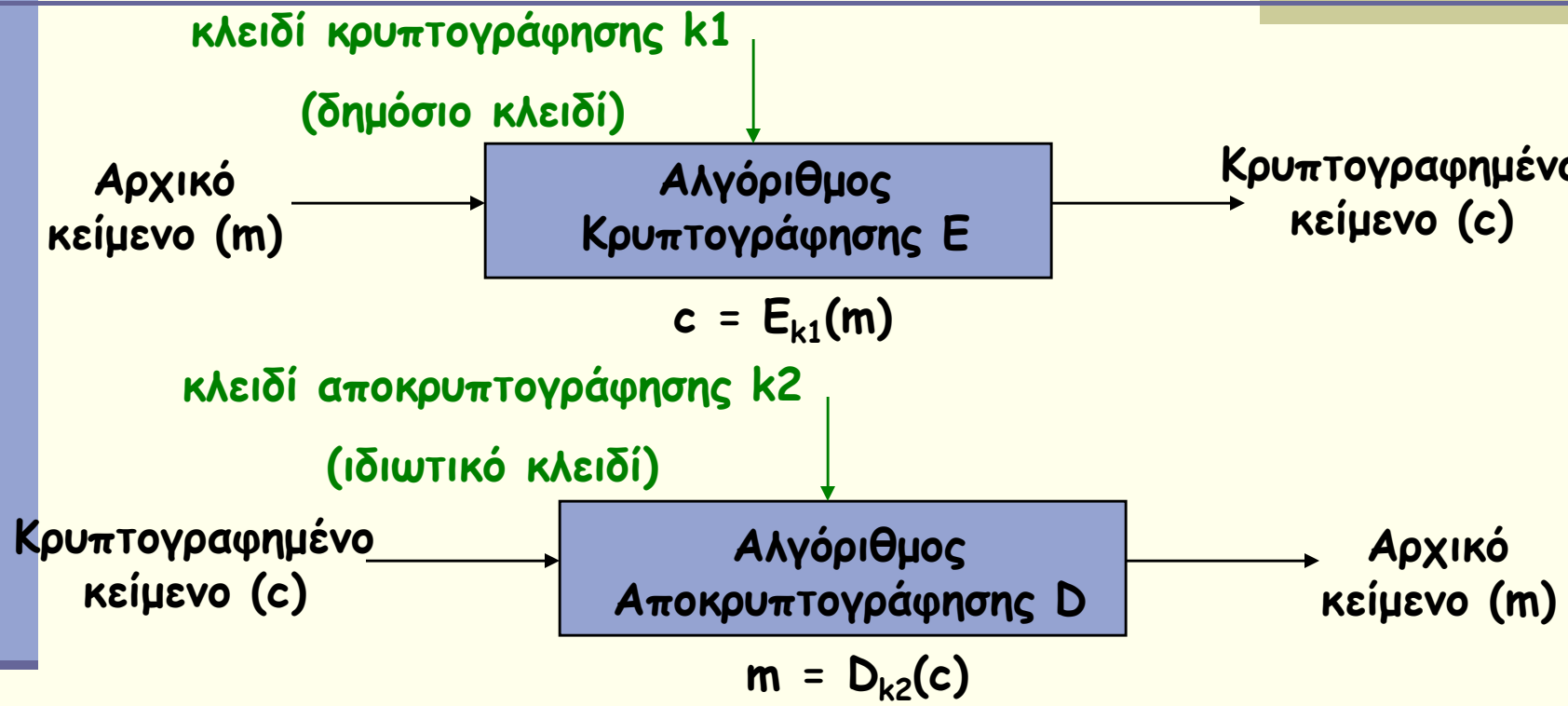
Κρυπτογραφία



Κωνσταντίνου Ελισάβετ
ekonstantinou@aegean.gr

http://www.icsd.aegean.gr/ekonstantinou

Ασύμμετρα Κρυπτοσυστήματα



Το κλειδί αποκρυπτογράφησης βρίσκεται δύσκολα από το αντίστοιχο κλειδί κρυπτογράφησης. Η δυσκολία βασίζεται σε κάποιο μαθηματικό πρόβλημα.

Κρυπτογραφία Δημόσιου Κλειδιού

Δοθέντος ενός δημόσιου κλειδιού e είναι υπολογιστικά αδύνατο να βρεθεί το ιδιωτικό κλειδί d.

Αλγόριθμος κρυπτογράφησης E_e = trapdoor one-way function με trapdoor information = d.

Π.χ. η $f(x) = x^3 \bmod n$ είναι μια trapdoor one-way function, όπου η trapdoor πληροφορία είναι οι παράγοντες p και q του n. Άρα, αν το μυστικό κλειδί του Bob είναι τα p, q και δημόσιο το n, τότε η Alice μπορεί να κρυπτογραφήσει το μήνυμα x ως $c = x^3 \bmod n$ και να το στείλει πίσω στον Bob. Στη συνέχεια, μόνο ο Bob που έχει την trapdoor πληροφορία μπορεί να βρει το x (δηλαδή να αντιστρέψει τη συνάρτηση).

Κρυπτογραφία Δημόσιου Κλειδιού

$c = x^3 \bmod n$

(s_A, P_A)

x = μήνυμα

(s_B, P_B)

$s_B = p, q$
$P_B = n$

Μόνο ο Bob μπορεί να αποκρυπτογραφήσει που κατέχει τα p, q. Αν γνωρίζεις το n (δημόσιο κλειδί), δεν μπορείς να βρεις τα p, q (ιδιωτικό κλειδί).

Integer factorization problem!!

Μαθηματικό Υπόβαθρο

Πρώτοι Αριθμοί

Ορισμός: Ένας θετικός αριθμός $p > 1$ καλείται πρώτος (prime) αν οι μόνοι διαιρέτες του είναι οι ακέραιοι ± 1 και $\pm p$. Ένας θετικός ακέραιος $n > 1$ που δεν είναι πρώτος καλείται σύνθετος (composite).

Δύο ακέραιοι n, m καλούνται πρώτοι μεταξύ τους (coprime) αν $gcd(n, m) = 1$.

Κάθε ακέραιος $n > 1$ αναλύεται μοναδικά ως $n = p_1^{e1} p_2^{e2} \ldots p_k^{ek}$ όπου κάθε p_i είναι ένας πρώτος αριθμός και e_i είναι η αντίστοιχη τάξη τους στο γινόμενο.

Πρώτοι Αριθμοί

Ορισμός: Έστω B ένας θετικός ακέραιος. Θα λέμε ότι ένας ακέραιος n είναι B-ομαλός (B-smooth) αν όλοι οι πρώτοι παράγοντές του είναι μικρότεροι ή ίσοι του B. Δηλαδή αν $n = p_1^{e1}p_2^{e2}...p_k^{ek}$ θα πρέπει κάθε $p_i <= B$.

Παράδειγμα: Το $20 = 2^2*5$ είναι 5-ομαλός, 10-ομαλός ή 12345-ομαλός, αλλά όχι 4-ομαλός ή 3-ομαλός.

Έστω ότι π(x) είναι το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι του x (π.χ. αν x = 15, τότε π(x) = 6 (2,3,5,7,11,13)). Ισχύει ότι

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

Η συνάρτηση φ(.) του Euler

Για κάθε ακέραιο n > 0, έστω φ(n) το πλήθος των ακεραίων στο διάστημα [1, n] που είναι **σχετικά πρώτοι με το n**. Η συνάρτηση φ(.) καλείται Euler phi function.

Ιδιότητες:

1) Αν **p είναι πρώτος**, τότε $\varphi(p) = p-1$.
2) Αν **gcd(n, m) = 1**, τότε $\varphi(nm) = \varphi(n)\varphi(m)$.
3) Αν $n = p_1^{e1}p_2^{e2}\ldots p_k^{ek}$ τότε $\varphi(n) = n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$.

Παράδειγμα:

$\varphi(20) = 20(1-1/2)(1-1/5) = 8$.

Πράγματι, οι αριθμοί στο [1,20] που είναι σχετικά πρώτοι με το 20 είναι οι 1,3,7,9,11,13,17 και 19.

Euler, 1707-1783

Ομάδες, Δακτύλιοι και Σώματα

Έστω Ε ένα μη κενό σύνολο. Καλούμε πράξη επί του Ε, μια απεικόνιση

$E \times E \longrightarrow E$.

Ορισμός: Ένα ζεύγος (G, *), όπου G είναι ένα μη κενό σύνολο και * μια πράξη επί του G, καλείται ομάδα (group) αν η πράξη * έχει τις εξής ιδιότητες:

1) $x*(y*z) = (x*y)*z$ για κάθε $x,y,z \in G$.
2) Υπάρχει $g \in G$ τέτοιο ώστε για κάθε $x \in G$ να ισχύει $x*g = x = g*x$.
3) Για κάθε $x \in G$ υπάρχει ένα $x' \in G$ τέτοιο ώστε $x*x' = g = x'*x$.

Το g είναι το μοναδικό στοιχείο που έχει την ιδιότητα (2) και καλείται ουδέτερο στοιχείο της ομάδας.

Για κάθε x το στοιχείο x' είναι μοναδικό και καλείται συμμετρικό του x.

Ομάδες, Δακτύλιοι και Σώματα

Αν η πράξη * είναι αντιμεταθετική, δηλαδή ισχύει $x*y = y*x$ για κάθε $x, y \in G$, τότε η ομάδα καλείται αντιμεταθετική ή αβελιανή (abelian).

Ορισμός: Ένας δακτύλιος (ring) είναι μια τριάδα $(A, +, *)$, που αποτελείται από ένα μη κενό σύνολο A και από δύο πράξεις:

- μια πρόσθεση +: $A \times A \to A$, $(x,y) \to x+y$
- έναν πολλαπλασιασμό *: $A \times A \to A$, $(x,y) \to xy$

έτσι ώστε να ισχύουν τα εξής:

1) Το ζεύγος $(A, +)$ είναι αβελιανή ομάδα.
2) $x(yz) = (xy)z$ για κάθε $x,y,z \in A$.
3) Υπάρχει μονάδα, δηλαδή υπάρχει στοιχείο g του A τέτοιο ώστε $gx = x = xg$ για κάθε x που ανήκει στο A. Το g θα συμβολίζεται και ως 1.
4) $x(y+z) = xy+xz$ και $(y+z)x = yx+zx$ για κάθε x,y,z στο A.

Ομάδες, Δακτύλιοι και Σώματα

Ένα στοιχείο α του δακτυλίου Α καλείται αντιστρέψιμο αν υπάρχει α΄ στο Α τέτοιο ώστε α*α΄ = 1 = α΄*α. Το α΄ καλείται αντίστροφο του α και συμβολίζεται με α^{-1}.

Ορισμός: Ένας αντιμεταθετικός δακτύλιος καλείται σώμα (field) αν κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο.

Για παράδειγμα, ο δακτύλιος Q των ρητών αριθμών είναι σώμα, ενώ ο δακτύλιος Z των ακεραίων δεν είναι.

Ισοδυναμίες και Ισοτιμίες

Έστω Σ ένα μη κενό σύνολο. Ένα υποσύνολο S του Σ x Σ καλείται σχέση ισοδυναμίας, αν έχει τις εξής ιδιότητες:

1) $(x, x) \in S$ για κάθε $x \in \Sigma$ (ανακλαστική)

2) αν $(x, y) \in S \Rightarrow (y, x) \in S$ (συμμετρική)

3) αν $(x, y) \in S$ και $(y, z) \in S \Rightarrow (x, z) \in S$ (μεταβατική)

Δύο στοιχεία που συνδέονται με μια σχέση ισοδυναμίας καλούνται ισοδύναμα.

Κλάση ισοδυναμίας (equivalence class) ενός στοιχείου α του Σ, είναι το σύνολο $[\alpha] = \{x \in \Sigma \mid (x, \alpha) \in S\}$

Ισοδυναμίες και Ισοτιμίες

Ορισμός: Έστω n ένας θετικός ακέραιος. Ο ακέραιος a καλείται ισότιμος (congruent) με τον ακέραιο b modulo n, συμβολικά

$$a \equiv b \bmod n$$

αν n | a-b (δηλαδή αν η ποσότητα a-b διαιρείται με το n) ή διαφορετικά αν a = kn + b για κάποιον ακέραιο k. Αν το n δεν διαιρεί το a-b, τότε ο a καλείται ανισότιμος με τον b modulo n, συμβολικά

$$a \not\equiv b \bmod n$$

Παραδείγματα:

$24 \equiv 9 \bmod 5$ $24 \equiv 39 \bmod 5$

$24 \equiv 4 \bmod 5$ $-11 \equiv 3 \bmod 7$ $-4 \equiv -13 \bmod 9$

Ισοδυναμίες και Ισοτιμίες

Η σχέση ισοτιμίας $\equiv$ είναι μία σχέση ισοδυναμίας στο $\mathbb{Z}$ (σύνολο ακεραίων). Δηλαδή ισχύουν τα εξής:

1) $a \equiv a \bmod n$ για κάθε a στο $\mathbb{Z}$
2) $a \equiv b \bmod n \implies b \equiv a \bmod n$
3) αν $a \equiv b \bmod n$ και $b \equiv c \bmod n \implies a \equiv c \bmod n$
4) αν $a \equiv a_1 \bmod n$ και $b \equiv b_1 \bmod n \implies a + b \equiv a_1 + b_1 \bmod n$ και $ab \equiv a_1 b_1 \bmod n$

Για κάθε a που ανήκει στο $\mathbb{Z}$, η κλάση ισοδυναμίας του a είναι η $[a] = \{x \in \mathbb{Z} \mid x \equiv a \bmod n\}$ και καλείται κλάση ισοτιμίας ή κλάση υπολοίπων του a mod n.

Ισοδυναμίες και Ισοτιμίες

Ορισμός: Οι ακέραιοι modulo n, συμβολίζονται με Z_n και είναι το σύνολο των κλάσεων ισοδυναμίας των {0, 1, 2, ..., n-1}. Όλες οι πράξεις στο Z_n γίνονται modulo n.

Το σύνολο Z_n αποτελεί αντιμεταθετικό δακτύλιο.

Αν το n είναι πρώτος, τότε το σύνολο Z_n είναι σώμα (συνήθως συμβολίζεται με F_p και καλείται πρώτο πεπερασμένο σώμα).

γιατί??

Ισοδυναμίες και Ισοτιμίες

Παραδείγματα:

1) Έστω ο δακτύλιος Z_{25}. Αυτός αποτελείται από τα στοιχεία {0, 1, 2, ..., 24}. Αν a = 8 και b = 13 είναι δύο στοιχεία του Z_{25}, υπολογίστε τα αποτελέσματα των πράξεων a+b, a-b, και ab.

Λύση:

a+b = 8+13 = 21 ≡ 21 mod 25

a-b = 8-13 = -5 ≡ 20 mod 25

ab = 8*13 = 104 ≡ 4 mod 25

2) Ποια από τα παρακάτω είναι σωστά?

31 ≡ 53 mod 22, 31 = 53 mod 22

7 ≡ 21 mod 14, 7 = 21 mod 14

21 ≡ 7 mod 14, 21 = 7 mod 14

Ισοδυναμίες και Ισοτιμίες

Πώς ορίζεται η διαίρεση στο Z_n?

Ένα στοιχείο a του Z_n λέμε ότι είναι αντιστρέψιμο αν υπάρχει ένας αριθμός x στο Z_n για τον οποίο ισχύει ότι

$$ax \equiv 1 \bmod n$$

Δεν έχουν όλοι οι αριθμοί στο Z_n αντίστροφο. Συγκεκριμένα, ένας αριθμός a στο Z_n αντιστρέφεται αν και μόνο αν $\gcd(a, n) = 1$.

Άρα, για να μπορεί να οριστεί η πράξη a/b στο Z_n θα πρέπει το b να αντιστρέφεται.

Ισοδυναμίες και Ισοτιμίες

Παράδειγμα:

Έστω τα στοιχεία a = 7 και b = 9 του δακτυλίου $\mathbb{Z}_{14}$. Υπολογίστε τα a/b και b/a.

Λύση:

Αρχικά πρέπει να δούμε αν τα a και b αντιστρέφονται. Ισχύει ότι gcd(a, 14) = 7 και gcd(b, 14) = 1. Άρα ορίζεται μόνο η πράξη a/b. Το $b^{-1} = 9^{-1} \equiv 11 \bmod 14$ (γιατί $9*11 \equiv 1 \bmod 14$).

Άρα, $a/b = 7*11 = 77 \equiv 7 \bmod 14$.

Ερώτημα: Γιατί το $\mathbb{Z}_n$ αποτελεί σώμα αν το n είναι πρώτος?

Ισοδυναμίες και Ισοτιμίες

Ορισμός: Αν n > 1 είναι ένας φυσικός αριθμός και a ένας ακέραιος τέτοιος ώστε gcd(a, n) = 1, τότε ο μικρότερος θετικός ακέραιος r με την ιδιότητα

$$a^r \equiv 1 \bmod n$$

καλείται τάξη (order) του a mod n.

(η τάξη ορίζεται μόνο για τα αντιστρέψιμα στοιχεία του Z_n)

Ορισμός: Η πολλαπλασιαστική ομάδα του Z_n είναι η $Z_n^* = \{a \in Z_n \mid gcd(a, n) = 1\}$. Δηλαδή η πολλαπλασιαστική ομάδα αποτελείται από τα αντιστρέψιμα στοιχεία του Z_n. Η τάξη $|Z_n^*|$ του Z_n^* είναι ίση με φ(n).

Δύο Βασικά Θεωρήματα

Θεώρημα του Euler:
Αν $a \in Z_n^*$ τότε $a^{\varphi(n)} \equiv 1 \bmod n$.

Η τάξη οποιουδήποτε στοιχείου του Z_n^* είναι είτε ίση με φ(n) ή διαιρεί ακριβώς το φ(n).

Μικρό Θεώρημα του Fermat:
Έστω p ένας πρώτος αριθμός. Αν gcd(a, p) = 1 για κάποιον ακέραιο αριθμό a, τότε $a^{p-1} \equiv 1 \bmod p$.

Fermat, 1601-1665

Γεννήτορες Ομάδων

Αν για κάποιο στοιχείο α του Z_n^* η τάξη του είναι ίση με φ(n), τότε το στοιχείο αυτό καλείται γεννήτορας του Z_n^*.

Δηλαδή ισχύει ότι $Z_n^* = \{a^i \bmod n \mid 0 \le i \le \varphi(n) - 1\}$.

Κάθε ομάδα που έχει έναν τουλάχιστον γεννήτορα καλείται κυκλική.

Πώς δημιουργείται ένας γεννήτορας για μια κυκλική ομάδα?

→ αν μια κυκλική ομάδα έχει τάξη t, τότε κάθε γεννήτορας θα έχει τάξη t

→ η τάξη οποιουδήποτε άλλου στοιχείου της ομάδας θα πρέπει να διαιρεί ακριβώς το t

Αλγόριθμος Δημιουργίας Γεννήτορα

ΑΛΓΟΡΙΘΜΟΣ 1.2.1 ***Μέθοδος υπολογισμού ενός γεννήτορα*** a ***μιας κυκλικής ομάδας*** G ***με τάξη*** t.
Είσοδος: *Η ομάδα* G *και η τάξη της* $t = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.
Έξοδος: *Ένας γεννήτορας* a *της ομάδας* G.

1. Επέλεξε ένα τυχαίο $a \in G$
2. **Για** $i = 1$ μέχρι k **υπολόγισε**
{
   $s = a^{\frac{t}{p_i}}$
   αν $s = 1$ **τότε** πήγαινε στο βήμα 1
}
3. Επέστρεψε στην έξοδο το a.

Παρατηρήσεις πάνω στον Αλγόριθμο

1) Αν η ομάδα G είναι ίση με Z_p^* όπου p είναι ένας πρώτος αριθμός, τότε η τάξη t = p-1 και όλες οι πράξεις a^{t/p_i} γίνονται modulo p.
2) Αν η ομάδα G είναι ίση με Z_n^* όπου n είναι ένας σύνθετος αριθμός, τότε η τάξη t = φ(n) και όλες οι πράξεις a^{t/p_i} γίνονται modulo n.
3) Τέλος, για να βρεθούν οι πρώτοι παράγοντες της τάξης της ομάδας θα πρέπει να εφαρμοστεί ένας αλγόριθμος παραγοντοποίησης. Εναλλακτικά, αν ζητείται να δημιουργηθεί γεννήτορας για μια ομάδα Z_p^* όπου p είναι ένας πρώτος αριθμός, τότε αρκεί να βρεθεί ένα p_1 τέτοιο ώστε η τάξη $t = p-1 = 2p_1$.

Κινέζικο Θεώρημα Υπολοίπου

Κινέζικο Θεώρημα Υπολοίπου (Chinese Remainder Theorem - CRT):

Αν οι ακέραιοι n_1, n_2, …, n_k είναι ανά δύο πρώτοι μεταξύ τους, τότε το σύστημα των ισοτιμιών

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$
$$.$$
$$.$$
$$x \equiv a_k \bmod n_k$$

έχει μοναδική λύση modulo $n = n_1 n_2 \ldots n_k$.

Η λύση των παραπάνω ισοτιμιών υπολογίζεται από τον αλγόριθμο του Gauss.

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i \pmod{n} \qquad N_i = n/n_i \qquad M_i = N_i^{-1} \pmod{n_i}.$$

Διάβασμα…

Σημειώσεις μαθήματος, Κεφάλαια 2.4 και 2.5 του Handbook of Applied Cryptography, βιβλιογραφικές αναφορές που υπάρχουν στις σημειώσεις