Οι αλγόριθμοι RSA και Diffie-Hellman

Εισηγητής: Χρήστος Δαλαμάγκας
cdalamagkas@gmail.com

Άδεια χρήσης

Ατζέντα

- Εισαγωγή στη θεωρία αριθμών
- Πράξεις με την αριθμητική υπολοίπων
- Ο αλγόριθμος ΜΚΔ του Ευκλείδη
- Η συνάρτηση Euler
- Κρυπτογράφηση με τον RSA
- Ο αλγόριθμος ανταλλαγής κλειδιών Diffie-Helman

Εισαγωγή στη θεωρία αριθμών

Εισαγωγή στη θεωρία αριθμών

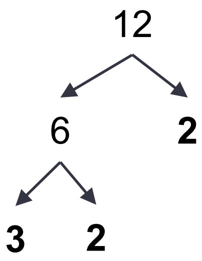
- Πρώτος αριθμός: Αυτός που έχει ως διαιρέτες μόνο το 1 και τον εαυτό του
- Κάθε ακέραιος αριθμός μπορεί να παραγοντοποιηθεί με μοναδικό τρόπο

$$\alpha = p_1^{a_i} * p_1^{a_i} * \cdots * p_t^{a_t}$$

p_i: πρώτοι αριθμοί,

a_i: θετικοί ακέραιοι

- $12 = 2^2 * 3^1$



Εισαγωγή στη θεωρία αριθμών

- Ο υπολογισμός του μέγιστου κοινού διαιρέτη δύο θετικών ακεραίων μπορεί να βρεθεί εύκολα εάν εκφράσουμε κάθε ακέραιο σε πρώτους παράγοντες

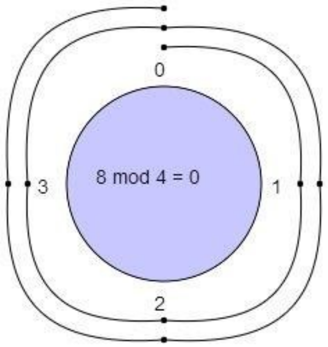
- $300 = 2^2 \times 3^1 \times 5^2$

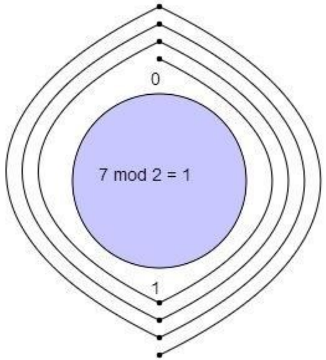
  $18 = 2^1 \times 3^2$

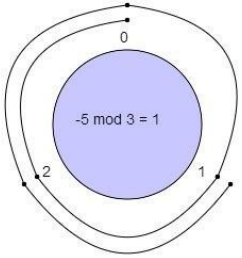
$$\gcd(18,300) = 2^1 \times 3^1 \times 5^0 = 6$$

Αριθμητική υπολοίπων

- α = 12, n = 5 → 12 = 2 * 5 + 2 r = 2
- α = -12, n = 5 → -12 = (-3) * 5 + 3 r = 3







Επομένως:

- 12 mod 5 = 2
- -12 mod 5 = 3

- Δύο ακέραιοι α, b είναι σύμφωνοι στο υπόλοιπο του n (congruent modulo n) εάν:

$$a \bmod n = b \bmod n \iff a \equiv b \bmod n$$

Αριθμητική υπολοίπων – Ιδιότητες

- $α \equiv b \bmod n$ εάν $n|(α - b)$.
  - π.χ. $23 \equiv 8 \bmod 5$ αφού $23 - 8 = 15 = 5 \times 3$.
  - π.χ. $-11 \equiv 5 \bmod 8$ αφού $-11 -5 = -16 = 8 \times (-2)$.
  - π.χ. $81 \equiv 0 \bmod 27$ αφού $81-0 = 81 = 27 \times 3$
- $α \equiv b \bmod n$ συνεπάγεται ότι $b \equiv α \bmod n$.
  - π.χ. $10 \equiv 20 \bmod 10$ και $20 \equiv 10 \bmod 10$.
- $α \equiv b \bmod n$ και $b \equiv c \bmod n$ συνεπάγεται ότι $α \equiv c \bmod n$.
  - π.χ. $10 \equiv 20 \bmod 10$ και $20 \equiv 50 \bmod 10$ τότε $10 \equiv 50 \bmod 10$.

Αριθμητική υπολοίπων – Ιδιότητες

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$.
  - Π.χ. 11 mod 8 = 3, 15 mod 8 = 7
    [(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2
    με χρήση της ιδιότητας: (11 + 15) mod 8 = 26 mod 8 = 2
- $(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$.
  - Π.χ [(11 mod 8) - (15 mod 8)] mod 8 = 10 mod 8 = 2
    με χρήση της ιδιότητας: (11-15) mod 8 = -4 mod 8 = 4
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$.
  - Π.χ [(11 mod 8) × (15 mod 8)] mod 8 = 10 mod 8 = 5
    με χρήση της ιδιότητας: (11 × 15) mod 8 = 165 mod 8 = 5
- $a^b \bmod n = [(a \bmod n^{)b}] \bmod n$.

Παράδειγμα υπολογισμού

- 11^{12} mod 7

Ιδέα: Αξιοποιούμε την ιδιότητα [(a mod n) × (b mod n)] mod n = (a × b) mod n.

1. Εκφράζουμε τη δύναμη 12 ως δυνάμεις του 2: $7_{10} = 1100_2 = 2^3 + 2^2 = 8 + 4$
2. 11^{12} mod 13 = $11^{(8+4)}$ mod 7 = $11^8 * 11^4$ mod 7 =
   = (11^8 mod 7)*(11^4 mod 7) mod 7 =
   = 8 mod 7 = 1

11 mod 7 = 4

11^2 mod 7 = 4*4 mod 7 = 16 mod 7 = 2

11^4 mod 7 = 2*2 mod 7 = 4 mod 7 = 4

11^8 mod 7 = 4*4 mod 7 = 16 mod 7 = 2

Μέγιστος Κοινός Διαιρέτης και Αμοιβαίοι πρώτοι

- Great Common Divisor – gcd
- **Θεώρημα**: gcd(α, b) = gcd(b, α mod b).

    π.χ   gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11.

    gcd(18, 12) = gcd(12, 6) = gcd(6, 0) = 6.

    gcd(11, 10) = gcd(10, 1) = gcd(1, 0) = 1.

- Αμοιβαία πρώτοι ονομάζονται δύο ακέραιοι αριθμοί α, b εάν ο μόνος κοινός θετικός ακέραιος παράγοντας είναι ο 1:   gcd(α, b) = 1.

    π.χ. οι αριθμοί 8 και 15 είναι αμοιβαία πρώτοι

Ο αλγόριθμος του Ευκλείδη

gcd(A, B)

- Αν A = 0
    - gcd(A, B) = B, αφού gcd(0, B) = B
- Αν B = 0
    - gcd(A,B) = A, αφού gcd(A, 0) = A
- Αλλιώς,
    - γράψε το A σε μορφή υπολοίπων: A = B * Q + R
    - Υπολόγισε το gcd(B, R)

Εκτεκταμένος gcd

- Ταυτότητα bezout: Έστω d = gcd(a, b). Τότε υπάρχουν ακέραιοι x, y τέτοιοι ώστε: **ax + by = d**

- Συνήθως, θέλουμε να εκφράσουμε τα a, b του gcd(a, b) με ταυτότητα bezout

- Βρίσκουμε το ΜΚΔ μέσω του κανονικού αλγορίθμου Ευκλείδη

- Λύνουμε τις σχέσεις του gcd(a, b) από το τέλος ως την αρχή ώστε να εκφράσουμε το ΜΚΔ ως αλγεβρικό άθροισμα των a, b.

Το μικρό θεώρημα Fermat

- Εάν ο p είναι πρώτος και ο α θετικός ακέραιος που δεν διαιρείται με τον p τότε ισχύει: $\alpha^{p-1} \equiv 1 \bmod p$ δηλαδή $\alpha^{p-1} \bmod p = 1$

- Εναλλακτικά:

$$\alpha^{p} \equiv \alpha \bmod p \quad \text{δηλαδή} \quad \alpha^{p} \bmod p = \alpha$$

Συνάρτηση Euler

- Είναι η συνάρτηση φ(n) που δηλώνει τον αριθμό των θετικών ακεραίων που είναι μικρότεροι από τον n και αμοιβαία πρώτοι με τον n.

  - π.χ. φ(37)
    ο αριθμός 37 είναι πρώτος → όλοι οι αριθμοί από τον 1 έως και το 36 είναι αμοιβαία πρώτοι με τον 37 → φ(37) = 36.
  - π.χ. φ(35)
    ο αριθμός 35 δεν είναι πρώτος, επομένως θα πρέπει να καταγραφούν όλοι οι ακέραιοι που είναι αμοιβαία πρώτοι με τον 35 → 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33 και 34. Άρα φ(35) = 24.

Συνάρτηση Euler

- Εάν ένας ακέραιος p είναι πρώτος ισχύει: $\varphi(p) = p - 1$

$$\varphi(n) = \varphi(pq) = \varphi(p) \times \varphi(q) = (p - 1) \times (q - 1)$$

- Σύμφωνα με το θεώρημα του Euler, για κάθε α και n που είναι αμοιβαία πρώτοι ισχύει:

$$a^{\varphi(n)} \bmod n = 1$$

- Εναλλακτικά:

$$a^{\varphi(n) + 1} \bmod n = a$$

- Για τον RSA:

$$m^{\varphi(n) + 1} = m^{(p - 1)(q - 1) + 1} \equiv m \bmod n.$$

Ο αλγόριθμος RSA

Εισαγωγή στον RSA

- Ασύμμετρος αλγόριθμος κρυπτογράφησης
- Δημόσιο και ιδιωτικό κλειδί
- Κρυπτογράφηση: Δέχεται απλό κειμενο, εφαρμόζει το δημόσιο κλεδί, παράγει κρυπτογράφημα
- Αποκρυπτογράφηση: Δέχεται κρυπτογράφημα, εφαρμόζει ιδιωτικό κλειδί, ανακτά απλό κείμενο
- Συμβολισμοί:
  - C: Κρυπτογράφημα
  - M: Απλό κείμενο
  - n: Το μέγεθος του απλού κειμένου και του κρυπτογραφήματος
  - e: Αριθμός που γνωρίζει καιο αποσοτλέας και ο παραλήπτης
  - d: Αριθμός που γνωρίζει μόνο ο παραλήπτης

Εισαγωγή στον RSA

- PUB = {e, n}: Δημόσιο κλειδί
- PRI = {d, n}: Ιδιωτικό κλειδί

- Κρυπτογράφηση:

$$C = M^e \bmod n$$

- Αποκρυπτογράφηση:

$$\mathrm{M} = C^d \bmod n = M^{ed} \bmod n$$

Απαιτήσεις RSA

- Πρέπει να υπάρχουν τιμές e, d, n ώστε $M^{ed} = M \bmod n$ για κάθε $M < n$
- Να είναι εύκολος ο υπολογισμός των M^e και C^d για κάθε $M < n$
- Να είναι αδύνατος ο υπολογισμός του d με δεδομένα τα e, n

Παραγωγή κλειδιών RSA

Επίλεξε q, p	p, q πρώτοι αριθμοί
Υπολόγισε n	n = p * q
Υπολόγισε φ	φ(n) = (p-1) * (q-1)
Επίλεξε ακέραιο e	$\mathrm{gcd}(\varphi(\mathrm{n}), \mathrm{e}) = 1; \quad 1 < e < \varphi(n)$
Υπολόγισε d	$d \equiv e^{-1} \, mod \; \varphi(n)$
Δημόσιο κλειδί	e, n
Ιδιωτικό κλειδί	d, n

Κρυπτογράφηση

$$C = M^e \; mod \;\; n$$

Αποκρυπτογράφηση

$$M = C^d \; mod \;\; n = M^{ed} \; mod \;\; n$$

1ο Παράδειγμα RSA

- $p = 3, \quad q = 11$
- $n = p*q = 33$
- $\varphi(n) = \varphi(pq) = \varphi(p) * \varphi(q) = (p-1) * (q-1) = 2 * 10 = 20$
- Συνήθης επιλογή είναι το 3 ή το 65537. Για μας, $e = 3$
- Εφαρμόζουμε τον εκτεταμένο Ευκλείδη για τον υπολογισμό του d:

$de \bmod \varphi(n) = 1 \rightarrow 3x + 20y = 1$

gcd(20, 3)

$20 = \mathbf{3}*(6) + \mathbf{2}$ $\quad\quad 1 = 3 + \mathbf{2}*(-1)$ $\quad\quad d = 7$

$3 = \mathbf{2}*(1) + \mathbf{1}$ $\quad\quad = 3 + (20+3*(-6))*(-1)$

$2 = 1*(2) + \mathbf{0}$ $\quad\quad = 3 + 20*(-1) + 3*(6)$

$= 3*(\mathbf{7}) + 20*(-1)$

1ο Παράδειγμα RSA

- PUB = {e, n} = {3, 20}
- PRI = {d, n} = {7, 20}
- Κρυπτογράφηση του μηνύματος M = 7
  - $C = 7^3 \bmod 33 = 13.$
- Αποκρυπτογράφηση του κρυπτογραφήματος C = 13:
  - $M = 13^7 \bmod 33 = (13^4 \times 13^2 \times 13) \bmod 33 = (16 \times 4 \times 13) \bmod 33 = 7.$
  - $13 \bmod 33 = 13$
  - $13^2 \bmod 33 = 13*13 \bmod 33 = 4$
  - $13^4 \bmod 33 = 13^2 * 13^2 \bmod 33 = 4*4 \bmod 33 = 16$

2ο Παράδειγμα RSA

- p = 17, q = 11
- n = p*q = 187
- φ(n) = φ(pq) = φ(p) * φ(q) = (p-1) * (q-1) = 2 * 10 = 160
- Συνήθης επιλογή είναι το 3 ή το 65537. Για μας, **e = 3**. (Αν και θα μπορούσαμε e=7)
- Εφαρμόζουμε τον εκτεταμένο Ευκλείδη για τον υπολογισμό του d:

de mod φ(n) = 1 → 3x + 160y = 1

gcd(160, 3)

160 = **3***(53) + **1** → 1 = 160 + **3***(-53) d = 107

3 = **1***(3) + **0** Αφού -53<0 → d = 160 – 53 = 107

2ο Παράδειγμα RSA

- PUB = {e, n} = {3, 187}
- PRI = {d, n} = {107, 187}
- Κρυπτογράφηση του μηνύματος M = 88
  - $C = 88^3 \bmod 187 = 44$
- Αποκρυπτογράφηση του κρυπτογραφήματος C = 44:

$M = 44^{107} \bmod 187 = (44^{64} \times 44^{32} \times 44^{8} \times 44^{2} \times 44) \bmod 187 = (154 \times 154 \times 33 \times 66 \times 44) \bmod 187 = \mathbf{88}$

$44 \bmod 187 = 44$

$107_{10} = 110101_2$

$44^2 \bmod 33 = 44 \times 44 \bmod 187 = 66$

$44^4 \bmod 33 = 66 \times 66 \bmod 187 = 55$

$44^8 \bmod 33 = 33$

$44^{16} \bmod 33 = 154$

$44^{32} \bmod 33 = 154$

$44^{64} \bmod 33 = 154$

Τι κρατάμε για τον RSA

- Το μαθηματικό του υπόβαθρο είναι η αριθμητική υπολοίπων και η θεωρία αριθμών
- Η ασφάλειά του βασίζεται στην παραγωγή δυο μεγάλων πρώτων αριθμών
- **Modulus** (n) ονομάζεται το γινόμενο των δυο πρώτων αριθμών και καθορίζει το μέγεθος του ιδιωτικού κλειδιού (πχ 2048 bits). Το n είναι δημόσιο.
- Η ασφάλειά του κινδυνεύει αν κάποιος παραγοντοποιήσει το n
- Ασφαλές κλειδί σήμερα θεωρείται αυτό με μέγεθος >= 2048 bits

Ο αλγόριθμος Diffie-Hellman

Εισαγωγή στον Diffie-Hellman

- Αλγόριθμος για τη συμφωνία ενός κοινού κλειδιού συμμετρικής κρυπτογράφησης
- Επιτρέπει σε δυο οντότητες να συμφωνήσουν σε ένα κοινό κλειδί κρυπτογράφησης μέσω ενός μη ασφαλούς καναλιού μεταφοράς
- Τα δυο άκρα πρέπει να έχουν το ίδιο κλειδί, ενώ η επικοινωνία τους γίνεται μέσω μη ασφαλούς καναλιού μεταφοράς
- Τα δυο άκρα είναι άγνωστα μεταξύ τους, δεν έχουν άλλους τρόπους επικοινωνίας εκτός από το μη ασφαλές κανάλι επικοινωνίες
- Και πώς συνεννοούνται για το κοινό κλειδί;

Περιγραφή Diffie-Hellman

- Τα δυο άκρα συμφωνούν σε δυο δημόσιους μεγάλους αριθμούς
  - p: Πρώτος αριθμός
  - g: Πρωτογενής ρίζα του p, δηλαδή δεν έχει κοινούς παράγοντες με το p υψωμένος σε οποιαδήποτε ακέραια δύναμη mod n
- Το άκρο Α επιλέγει έναν αριθμό a και στέλνει στον Β το αποτέλεσμα της πράξης g^a mod p
- Το άκρο Β επιλέγει έναν αριθμό b και στέλνει στον Α το αποτέλεσμα της πράξης g^b mod p
- Το άκρο Α υπολογίζει το κλειδί ως $(g^b \bmod p)^a \bmod p \rightarrow$ **g^{ba} mod p**
- Το άκρο Β υπολογίζει το κλειδί ως $(g^a \bmod p)^b \bmod p \rightarrow$ **g^{ab} mod p**

Παράδειγμα Diffie-Hellman

- Έστω $p = 23$ και $g = 5$. Ο αριθμός 5 είναι πρωτογενής ρίζα του 23
- Το άκρο Α επιλέγει έναν τυχαίο αριθμόι $a = 6$ και στέλνει στον Β την παράσταση $g^a \bmod p = 5^6 \bmod 23 = 8$
- Το άκρο Β επιλέγει έναν τυχαίο αριθμό $b = 15$ και στέλνει στον Α το αποτέλεσμα της παράστασης $g^b \bmod p = 5^{15} \bmod 23 = 19$
- Ο Α υπολογίζει το μυστικό κλειδί $(g^b \bmod p)^a \bmod p = 19^6 \bmod 23 = 2$
- Ο Β υπολογίζει το μυστικό κλειδί $(g^a \bmod p)^b \bmod p = 8^{15} \bmod 23 = 2$