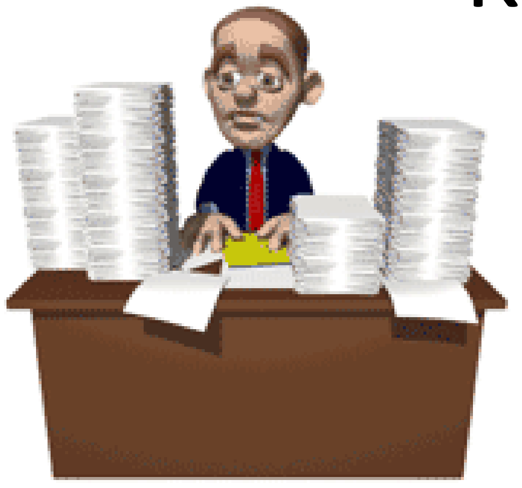
Κρυπτογραφία
02/05/2025



Κρυπτογραφια Δημοσιου Κλειδιου (Rabin, Merkle-Hellman)

Στα προηγούμενα επεισόδια

- $(Z_n, +)$, $(Z^*_n, \cdot)$: ομάδες
- $ax \equiv b \pmod{n}$
- $x \equiv a_i \pmod{n_i}$ με $gcd(n_i, n_j) = 1$ για $i \neq j$
- $x \equiv a^b \pmod{n}$
- Μονόδρομη συνάρτηση
- Συνάρτηση trapdoor
- Diffie – Hellman
- RSA

RSA – Δημιουργία κλειδιού (Επανάληψη)

- Κάθε χρήστης:
  - «διαλέγει» 2 μεγάλους πρώτους αριθμούς p και q
  - υπολογίζει $n=pq$ και $\phi(n)=(p-1)(q-1)$
  - επιλέγει τυχαίο e με $2<e<\phi(n)$ και $\gcd(e,\phi(n)) = 1$
  - υπολογίζει το μοναδικό d για το οποίο $ed \equiv 1 \pmod{\phi(n)}$
- Δημόσιο κλειδί χρήστη: (n, e)
- Ιδιωτικό κλειδί χρήστη: d

RSA – (Άπο)Κρυπτογράφηση (Επανάληψη)

- Η Αλίκη θέλει να στείλει το μήνυμα m στον Μπόμπο
- Πρώτα βλέπει το δημόσιο κλειδί (n_B,e_B) του Μπόμπου
- Μετατρέπει το m σε ακέραιο στο διάστημα $[1,n_B-1]$
- Υπολογίζει $c=m^{eB} \bmod n_B$ και το στέλνει στον Μπόμπο

- Ο Μπόμπος υπολογίζει $m = c^{dB} \bmod n_B$
- Μετατρέπει το m σε κείμενο

RSA – είναι όλα τα μηνύματα ασφαλή;

- Έστω $p = 5$, $q = 17$
  - $n = ?$, $\phi(n) = ?$

RSA – είναι όλα τα μηνύματα ασφαλή;

- Έστω $p = 5$, $q = 17$
  - $n = pq = 85$, $\phi(n) = 64$
- Έστω $e = 33$ (ισχύει $\gcd(33,64) = 1$)
  - $d = ?$

Ευκλείδης2 (Παράδειγμα)

- gcd(a,b) με a=33, b=64

a	b	⌊a/b⌋	gcd	x	y
33	64	0			

Ευκλείδης2 (Παράδειγμα)

a	b	⌊a/b⌋	gcd	x	y
33	64	0			
64	33	1			

Ευκλείδης2 (Παράδειγμα)

a	b	⌊a/b⌋	gcd	x	y
33	64	0			
64	33	1			
33	31	1			
31	2	15			
2	1	2			
1	0	-			

Ευκλείδης2 (Παράδειγμα)

a	b	⌊a/b⌋	gcd	x	y
33	64	0			
64	33	1			
33	31	1			
31	2	15			
2	1	2			
1	0	-	1	1	0

- Θυμηθείτε

gcd(a,0) = a με ax+0y = a να ικανοποιείται για x=1, y=0
x = y' και y = x' - ⌊a/b⌋y'

Ευκλείδης2 (Παράδειγμα)

a	b	⌊a/b⌋	gcd	x	y
33	64	0			
64	33	1			
33	31	1			
31	2	15			
2	1	2	1	0	1
1	0	-	1	1	0

- Θυμηθείτε

gcd(a,0) = a με ax+0y = a να ικανοποιείται για x=1, y=0
x = y’ και y = x’ - ⌊a/b⌋y’

Ευκλείδης2 (Παράδειγμα)

a	b	⌊a/b⌋	gcd	x	y
33	64	0	1	-31	16
64	33	1	1	16	-31
33	31	1	1	-15	16
31	2	15	1	1	-15
2	1	2	1	0	1
1	0	-	1	1	0

- Θυμηθείτε

gcd(a,0) = a με ax+0y = a να ικανοποιείται για x=1, y=0
x = y’ και y = x’ - ⌊a/b⌋y’

RSA – είναι όλα τα μηνύματα ασφαλή;

- Έστω p = 5, q = 17
  - n = pq = 85, φ(n) = 64
- Έστω e = 33 (ισχύει gcd(33,64) = 1)
  - d = 33
- Έστω m = 5
  - c = ?

RSA – είναι όλα τα μηνύματα ασφαλή;

- Έστω p = 5, q = 17
  - n = pq = 85, φ(n) = 64
- Έστω e = 33 (ισχύει gcd(33,64) = 1)
  - d = 33
- Έστω m = 5
  - c = 5^{33} mod 85 = …
  - c = 5
  - Σύμπτωση;

RSA – είναι όλα τα μηνύματα ασφαλή;

- Έστω $p = 5$, $q = 17$
  - $n = pq = 85$, $\phi(n) = 64$
- Έστω $e = 33$ (ισχύει $\gcd(33,64) = 1$)
  - $d = 33$
- Έστω $m = 5$
  - $c = 5^{33} \bmod 85 = \ldots$
  - $c = 5$
  - Σύμπτωση;
- Για κάθε πιθανό m, ισχύει $m = m^{33} \bmod 85$

RSA – είναι όλα τα μηνύματα ασφαλή;

- Έστω p = 5, q = 17
  - n = pq = 85, ϕ(n) = 64
- Έστω e = 33 (ισχύει gcd(33,64) = 1)
  - d = 33
- Έστω m = 5
  - $c = 5^{33} \bmod 85 = \ldots$
  - c = 5
  - Σύμπτωση;
- Για κάθε πιθανό m, ισχύει $m = m^{33} \bmod 85$
- Υπάρχουν (1+gcd(e-1,p-1))(1+gcd(e-1,q-1)) «σταθερά» μηνύματα, δηλαδή μηνύματα που κρυπτογραφούνται στον ευατό τους

RSA – Ομομορφική ιδιότητα

- $c_1 = m_1^e \bmod n$
- $c_2 = m_2^e \bmod n$
- $c_1 c_2 = (m_1 m_2)^e \bmod n = c_{12}$
- Αν βλέπω την κρυπτογράφηση του m μπορώ να δημιουργήσω την κρυπτογράφηση του $m \cdot t$ ακόμα και αν δεν ξέρω το m
  - Malleability

RSA – Ομομορφική ιδιότητα

- $c_1 = m_1^e \bmod n$
- $c_2 = m_2^e \bmod n$
- $c_1 c_2 = (m_1 m_2)^e \bmod n = c_{12}$
- Αν βλέπω την κρυπτογράφηση του m μπορώ να δημιουργήσω την κρυπτογράφηση του $m \cdot t$ ακόμα και αν δεν ξέρω το m
  - Malleability
- Το m κρυπτογραφείται ως $c = m^e \bmod n$
- Ο αντίπαλος κρυπτογραφεί το $m \cdot t$ για κάθε t: $(mt)^e \bmod n = c \cdot t^e \bmod n$

Η απλή μορφή του RSA είναι ανασφαλής

- $c = m^{eB} \bmod n_B$ --- $m = c^{dB} \bmod n_B$
- Αν m και e_B είναι μικρά, τότε;
- e χρήστες με κοινό e αρκούν για να «πέσει» το m
- Χρήστες με κοινό n: $(c_1^{-1})^{-w} c_2^{v} \equiv m \pmod{n}$
- Man in the middle attack
- Ομομορφική ιδιότητα και Malleability

Πρωτόκολλο Rabin

- Michael O. Rabin (1979)
  - Θυμηθείτε: Diffie – Hellman (1976), RSA (1977)
- Βασίζεται στη δυσκολία εύρεσης τετραγωνικών ριζών
  - modulo έναν σύνθετο ακέραιο
- Υπολογιστικά ισοδύναμο με παραγοντοποίηση
  - Το RSA δεν είναι
- Υπάρχει πάντοτε λύση;
  - $x^2 \equiv 1 \pmod{13}$ =>
    - $x \equiv 1 \pmod{13}$
    - $x \equiv 12 \pmod{13}$
  - $x^2 \equiv 2 \pmod{13}$
  - Δεν έχει ακεραίες λύσεις

Τετραγωνικά υπόλοιπα

- Ένας ακέραιος a είναι τ.υ. modulo n αν η ισοδυναμία $x^2 \equiv a \pmod{n}$ έχει λύση
- Π.χ. για n=8 τα τ.υ. είναι 0,1,4. Γιατί;

x	x^2	$x^2 \bmod 8$
0	0	0
1	1	1
2	4	4
3	9	1
4	16	0
5	25	1
6	36	4
7	49	1

Τετραγωνικά υπόλοιπα

- Συνήθως παίρνουμε ότι ένας a στο Z^*_n είναι τ.υ. modulo n αν υπάρχει x στο Z^*_n έτσι ώστε $x^2 \equiv a \pmod{n}$
- Ο a στο Z^*_p είναι τ.υ. modulo πρώτο αριθμό p ανν $a^{(p-1)/2} \equiv 1 \pmod{p}$
  - Π.χ. για p=7 τα τ.υ. είναι 0 (ειδική περιπτώση),1,2,4. Γιατί;
  - Για κάποιο p έχουμε (p-1)/2 ακεραίους (ή (p + 1)/2, περιλαμβάνοντας το 0) που είναι τ.υ.
  - (p-1)/2 ακέραιοι δεν είναι (βγαίνει απο το κριτήριο Euler)
- Έστω n = pq (p,q: πρώτοι). Ο a στο Z^*_n είναι τ.υ. modulo n ανν είναι τ.υ. modulo p και είναι τ.υ. modulo q
  - (p-1)(q-1)/4 είναι τ.υ., 3(p-1)(q-1)/4 δεν είναι

Τετραγωνική ρίζα

- $x^2 \equiv a \pmod p$, με $p \equiv 3 \pmod 4$ και a τ.υ.
  - Λύσεις: $a^{(p+1)/4} \bmod p$, $- a^{(p+1)/4} \bmod p$
  - Π.χ. $x^2 \equiv 4 \pmod 7$, $x=\pm 4^{(7+1)/4} \bmod 7=2$ ή 5
- $x^2 \equiv a \pmod{pq}$, με $p \equiv q \equiv 3 \pmod 4$
  - Λύσε $r^2 \equiv a \pmod p$
  - Λύσε $s^2 \equiv a \pmod q$
  - Βρες c,d έτσι ώστε $cp+dq = 1$
    - Πως;
  - $x = (rdq+scp) \bmod pq$, $y = (rdq-scp) \bmod pq$
    - Κινέζικο θεώρημα υπολοίπων
  - Λύσεις: x, -x, y, -y

Τετραγωνική ρίζα

- $x^2 \equiv a \pmod{p}$, με $p \equiv 3 \pmod{4}$ και a τ.υ.
  - Λύσεις: $a^{(p+1)/4} \bmod p$, $- a^{(p+1)/4} \bmod p$
  - Π.χ. $x^2 \equiv 4 \pmod{7}$, $x=\pm 4^{(7+1)/4} \bmod 7=2$ ή 5
- $x^2 \equiv a \pmod{pq}$, με $p \equiv q \equiv 3 \pmod{4}$
  - Λύσε $r^2 \equiv a \pmod{p}$
  - Λύσε $s^2 \equiv a \pmod{q}$
  - Βρες c,d έτσι ώστε $cp+dq = 1$
    - extended Euclid
  - $x = (rdq+scp) \bmod pq$, $y = (rdq-scp) \bmod pq$
    - Κινέζικο θεώρημα υπολοίπων
  - Λύσεις: x, -x, y, -y

Τετραγωνική ρίζα-Παράδειγμα

- $x^2 \equiv 4 \pmod{7*11}$, με $p \equiv q \equiv 3 \pmod 4$
  - Λύνω $r^2 \equiv 4 \pmod 7$
  - $r=\pm 4^{(7+1)/4} \bmod 7=2$ ή 5
  - Λύνω $s^2 \equiv 4 \pmod{11}$
  - $s=\pm 4^{(11+1)/4} \bmod 11=9$ ή 2
  - Βρίσκω c,d έτσι ώστε 7c+11d = 1
    - extended Euclid (11,7) => c=-3,d=2

a	b	⌊a/b⌋	gcd	d	c
11	7	1	1	2	-3
7	4	1	1	-1	2
4	3	1	1	1	-1
3	1	3	1	0	1
1	0	-	1	1	0

Τετραγωνική ρίζα-Παράδειγμα

- x = (2*2*11+9*(-3)*7) mod 77
- =(44-189) mod 77
- =-145 mod 77=9
- y = (2*2*11-9*(-3)*7) mod 77=
- =(44+189) mod 77
- =233 mod 77=2
- Λύσεις: x, -x, y, -y
- x_1= 9 mod 77 = 9
- x_2= -9 mod 77 = 68
- y_1= 2 mod 77 = 2
- y_2= -2 mod 77 = 75

Rabin: Δημιουργία κλειδιού

- Κάθε χρήστης:
  - «διαλέγει» 2 μεγάλους πρώτους αριθμούς p και q
  - με $p \equiv q \equiv 3 \pmod{4}$
  - υπολογίζει $n=pq$
- Δημόσιο κλειδί χρήστη: n
- Ιδιωτικό κλειδί χρήστη: (p,q)

Rabin: (Απο)Κρυπτογράφηση

- Η Αλίκη θέλει να στείλει το μήνυμα m στον Μπόμπο
- Πρώτα βλέπει το δημόσιο κλειδί n_B του Μπόμπου
- Μετατρέπει το m σε ακέραιο στο διάστημα $[1,n_B-1]$
- Υπολογίζει $c=m^2 \bmod n_B$ και το στέλνει στον Μπόμπο
- Ο Μπόμπος υπολογίζει το m ως την τετραγωνική ρίζα του $c \bmod n_B$, δηλαδή $m^2 \equiv c \pmod{n_B}$
- Μετατρέπει το m σε κείμενο
  - Πρόβλημα;

Rabin: Παράδειγμα

- $p = 7$, $q = 11$, $n = 77$, $m = 10$
- Κρυπτογράφηση: $c = 100 \bmod 77 = 23$
- Αποκρυπτογράφηση: $m^2 \equiv 23 \pmod{77}$
- $r^2 \equiv 23 \equiv 2 \pmod{7}$
  - $r = 2^{(7+1)/4} \bmod 7 = 4$
- $s^2 \equiv 23 \equiv 1 \pmod{11}$
  - $s = 1^{(11+1)/4} \bmod 11 = 1$
- $7c+11d = 1 \rightarrow$ (Ευκλείδης2) $\rightarrow c=-3, d=2$
- $x = 4\cdot 2\cdot 11+1\cdot(-3)\cdot 7 \bmod 77 = 67$
- $y = 4\cdot 2\cdot 11-1\cdot(-3)\cdot 7 \bmod 77 = 32$
- *Λύσεις = (67, 10, 32, 45)*

Πρωτόκολλο Merkle - Hellman

- Ralph Merkle, Martin Hellman (1978)
- Βασίζεται στο πρόβλημα του σακιδίου
  - NP-πλήρες πρόβλημα
- Έσπασε το 1984 από τον Shamir (το S στο RSA)
- Χρήσιμο για εκπαιδευτικούς σκοπούς

Το υπολογιστικό πρόβλημα

- SUBSET SUM: Ειδική περίπτωση του KNAPSACK
- Είσοδος: Σύνολο ακεραίων $I = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ και ακέραιος T
- Έξοδος: Υποσύνολο S έτσι ώστε το άθροισμα των ακεραίων στο S να ισούται με T
- Υπολογιστικά δύσκολο πρόβλημα
- Π.χ.: I = {14, 28, 56, 82, 90, 132, 197, 284, 341, 455}
  - T = 516 (δεν υπάρχει λύση)
  - T = 515 (S = {28, 56, 90, 341})

Το υπολογιστικό πρόβλημα – Εύκολη περίπτωση

- I = {1, 2, 4, 9, 18, 35, 70}: Υπεραύξουσα ακολουθία
- T = 101
- Αν I είναι υπεραύξουσα ακολουθία τότε το πρόβλημα γίνεται έυκολο.
- Μια διατεταγμένη ακολουθία ακεραίων $(b_1, b_2, \ldots, b_n)$ ονομάζεται υπεραύξουσα αν: $b_i > \sum_{j=1}^{i-1} b_j$
- Ιδέα πρωτοκόλλου:
- Ξεκινάμε με υπεραύξουσα ακολουθία
- Τη μετασχηματίζουμε σε μια «δύσκολη» ακολουθία
- Η κρυπτογράφηση γίνεται με τη «δύσκολη»
- Η αποκρυπτογράφηση γίνεται με την υπεραύξουσα

Merkle-Hellman: Δημιουργία κλειδιού

- Κάθε χρήστης:
  - Επιλέγει μια υπεραύξουσα ακολουθία $b = (b_1, b_2, \ldots, b_n)$
  - Επιλέγει 2 μεγάλους w και N με gcd(w,N) = 1
  - b, w, N ιδιωτικό κλειδί
  - Υπολογίζει $T(b_i) = wb_i \bmod N$
  - Ταξινομεί τα $T(b_i)$ και προκύπτει η ακολουθία $a = (a_1, a_2, \ldots, a_n)$
    - Δημόσιο κλειδί = ακολουθία a
    - Γνησίως αύξουσα ακολουθία (όχι όμως υπεραύξουσα) που αντιστοιχεί σε δύσκολο πρόβλημα

Merkle – Hellman: Κρυπτογράφηση

- Η Αλίκη θέλει να στείλει το μήνυμα m στον Μπόμπο
- Πρώτα βλέπει το δημόσιο κλειδί $a=(a_1, a_2, \ldots, a_n)$ του Μπόμπου
- Σπάει το m σε block των n bit
- Για κάθε block m_j υπολογίζει το $c_j = \sum_{i=1}^{n} (mj_{,i} \cdot ai)$
  Στέλνει την ακολουθία $c_1, c_2, \ldots$

Merkle – Hellman: Αποκρυπτογράφηση

- Για κάθε block c_j υπολογίζουμε το $c'_j = w^{-1}c_j \bmod N$
- Λύνουμε το SubsetSum με $I = f((b_1, b_2, \ldots, b_n))$ και $T = c'_j$
- Γιατί η Αλίκη δεν κρυπτογράφησε με βάση τα $(T(b_1), T(b_2), \ldots, T(b_n))$ αλλά με βάση την ταξινόμησή τους;

Merkle – Hellman: Παράδειγμα

- b = (1, 2, 4, 9, 20, 38), w = 31, N = 105
  - $w^{-1}=31^{-1}$ mod 105 = 61, γιατί; Λυσαμε την $31 \cdot x \equiv 1 \pmod{105}$
- T(1) = 31, T(2) = 62, T(4) = 19, T(9) = 69, T(20) = 95, T(38) = 23
- a = (19, 23, 31, 62, 69, 95)
- M = 001100 110100 111010
- c = (93, 104, 142)→ ·61 mod 105 → (3, 44, 52)

a	19=T(4)=a_1	23	31	62	69	95
$f(b_i)$	4	38	1	2	9	20
c'=3	0	0	1	1	0	0
c'=44	1	1	0	1	0	0
c'=52	1	1	1	0	1	0