Το κρυπτοσύστημα RSA

Παναγιώτης Γροντάς - Άρης Παγουρτζής

ΕΜΠ - Κρυπτογραφία (2017-2018)

14/11/2017

Περιεχόμενα

Εισαγωγή I

Συμμετρικά Κρυπτοσυστήματα - Το Μειονέκτημα

Διανομή Κλειδιών

Διανομή Κλειδιών σε Συμμετρικά Κρυπτοσυστήματα - Μειονεκτήματα

- Πρέπει να 'συναντηθούν' για να ανταλλάξουν κλειδιά
- Σε περιβάλλοντα πολλών χρηστών: Ανταλλαγή κλειδιών ανά ζεύγος
- Για n χρήστες χρειάζονται $\frac{n(n-1)}{2}$ κλειδιά
- Εύκολο σε ελεγχομένα περιβάλλοντα, δύσκολο σε ανοικτά
- Δυσκολίες διαχείρισης (πχ. έκδοση νέων), αποθήκευσης

Εισαγωγή II

Η λύση μετά από *2500* χρόνια κρυπτογραφίας:

Whitfield Diffie, Martin Hellman
New Directions in Cryptography - *(1976)*

- Ralph Merkle
- ίσως και νωρίτερα (GCHQ - James H. Ellis, Clifford Cocks, Malcolm J. Williamson)

Βασική ιδέα

Ασυμμετρία κρυπτογράφησης - αποκρυπτογράφησης

Παράδειγμα - Λουκέτα
Κλειδώνουν εύκολα
Ανοίγουν δύσκολα (χωρίς το κλειδί)

New Directions in Cryptography

Ανταλλαγή Κλειδιού Diffie - Hellman

Δημιουργία κοινού κλειδιού πάνω από δημόσιο - μη ασφαλές κανάλι (online)

Κρυπτογραφία Δημοσίου Κλειδιού

Το κλειδί κρυπτογράφησης μπορεί να είναι δημόσιο
Το κλειδί αποκρυπτογράφησης πρέπει να είναι μυστικό
n χρήστες, n ζεύγη κλειδιών
Εύκολη διανομή

Ψηφιακή Υπογραφή

Ασύμμετρα MACs
Επαλήθευση με δημόσιο κλειδί - Δημιουργία με ιδιωτικό
Αυθεντικότητα, Μη Αποκήρυξη

Trapdoor Functions

Συναρτήσεις μονής κατεύθυνσης

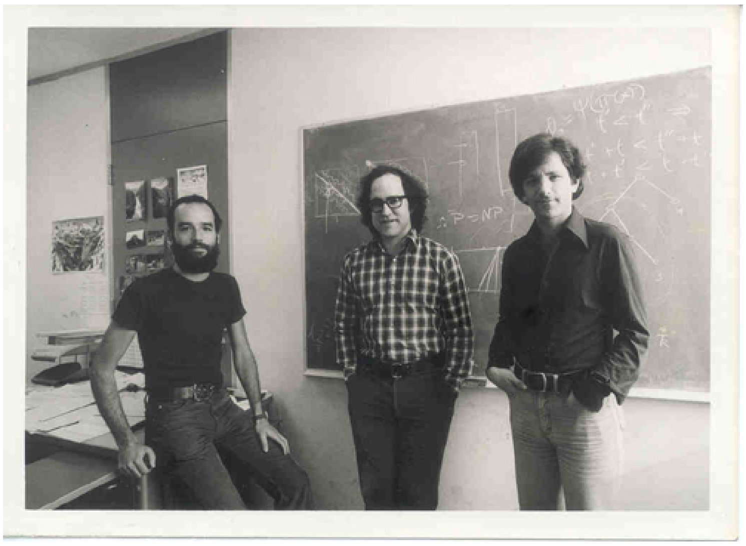
Μία συνάρτηση f λέγεται μονής κατεύθυνσης εάν είναι εύκολο να υπολογιστεί το $f(x)$ δεδομένου του x, ενώ ο αντίστροφος υπολογισμός του x δεδομένου του $f(x)$ είναι απρόσιτος.

Trapdoor Functions - Ορισμός

Μια συνάρτηση μονής κατεύθυνσης f για την οποία ο υπολογισμός της f^{-1} είναι *εύκολος* όταν δίνεται μια μυστική πληροφορία (secret trapdoor) k

RSA (1978)

- Η πρώτη *κατασκευή* κρυπτοσυστήματος δημοσίου κλειδιού
- Ron Rivest, Adi Shamir, Leonard Adleman
- Πατέντα μέχρι το 2000



Το κρυπτοσύστημα

Δημιουργία Κλειδιών:

- $KeyGen(1^\lambda) = ((e, n), d)$
- $n = p \cdot q$,
  p, q πρώτοι αριθμοί $\frac{\lambda}{2}$ bits
- Επιλογή e με $1 < e < \phi(n)$ και $gcd(e, \phi(n)) = 1$
- $d = e^{-1} \pmod{\phi(n)}$ με EGCD

Κρυπτογράφηση

- $\texttt{Encrypt} : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$
- $\texttt{Encrypt}((e, N), m) = m^e \bmod n$

Αποκρυπτογράφηση

- $\texttt{Decrypt} : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$
- $\texttt{Decrypt}(d, c) = c^d \bmod n$

Ορθότητα

Πρέπει: $\texttt{Decrypt}(d, \texttt{Encrypt}((e,n),m)) = m, \forall m$

$$\begin{aligned} \texttt{Decrypt}(d, \texttt{Encrypt}((e,n),m)) &= \\ (m^e)^d \bmod n &= \\ m^{ed} \bmod n &= \\ m^{k\phi(n)+1} \bmod n &= \\ m^{\phi(n)k} \cdot m \bmod n &= \\ m \bmod n & \end{aligned}$$

λόγω Θ.Euler και αφού $m \in \mathbb{Z}_n^*$

Κωδικοποίηση Μηνύματος I

Δεν απαιτείται $m \in \mathbb{Z}_n^*$ για ορθότητα. Ισχύει για κάθε $m \in \mathbb{Z}_n$

Κωδικοποίηση Μηνύματος II

Απόδειξη

$m \in \mathbb{Z}_n \Rightarrow gcd(m, n) \neq 1 \implies gcd(m, n) \in \{p, q\}$
Πρέπει νδο
$m^{ed} = m \pmod{p}$ και
$m^{ed} = m \pmod{q}$
Από CRT θα έχουμε:
$m^{ed} = m \bmod pq$

Κωδικοποίηση Μηνύματος III

$gcd(m, n) = p$

$$\begin{aligned} m^{ed} &= m \pmod{p} \\ (kp)^{ed} &= kp = 0 \pmod{p} \end{aligned}$$

OK

$$\begin{aligned} m^{ed} = m \cdot m^{ed-1} = m \cdot m^{k\phi(n)} &= m \cdot m^{k(p-1)(q-1)} \\ m \cdot m^{\phi(q)k(p-1)} &= m \cdot 1 \pmod{q} \end{aligned}$$

λόγω του Θ. Fermat που ισχύει στο $\mathbb{Z}_q$ OK

Ομοίως και για $gcd(m, n) = q$

Παράμετρος Ασφάλειας

Παραγοντοποίηση Modulus 768bit

RSA-768 = 1 230 186 684 530 117 755 130 494 958 384 962 720 772 853 569 595 334 792 197 322 452 151 726 400 507 263 657 518 745 202 199 786 469 389 956 474 942 774 063 845 925 192 557 326 303 453 731 548 268 507 917 026 122 142 913 461 670 429 214 311 602 221 240 479 274 737 794 080 665 351 419 597 459 856 902 143 413= 33 478 071 698 956 898 786 044 169 848 212 690 817 704 794 983 713 768 568 912 431 388 982 883 793 878 002 287 614 711 652 531 743 087 737 814 467 999 489 × 36 746 043 666 799 590 428 244 633 799 627 952 632 279 158 164 343 087 642 676 032 283 815 739 666 511 279 233 373 417 143 396 810 270 092 798 736 308 917

Παραγοντοποιήθηκε το 2009 μετά από 2 ημερολογιακά χρόνια (Factorization of a 768-bit RSA modulus)
2000 χρόνια σε single core system (2.2 GHz AMD Opteron)
Χρήση modulus

- 1024bits: βραχυχρόνια ασφάλεια (80 bit AES key)
- 2048bits, 3072bits: μακροχρόνια ασφάλεια (128 bit AES key)

Επιλογή πρώτων

- Τυχαία επιλογή ακέραιου $\frac{\lambda}{2}$ bits
- Primality test (Miller Rabin) επαναληπτικά
- p, q ίδιου μήκους
- p, q safe primes δηλ. $p-1, q-1$ έχουν μεγάλους πρώτους παράγοντες
- $p+1, q+1$ έχουν μεγάλους πρώτους παράγοντες

Επιλογή εκθέτη κρυπτογράφησης

Θέλουμε ταχύτατη κρυπτογράφηση

- Εύκολος Υπολογισμός Δύναμης Με Square και Multiply
  - Αναπαράσταση e στο δυαδικό
  - Για κάθε 0 ύψωση στο τετράγωνο
  - Για κάθε 1 ύψωση στο τετράγωνο και πολλαπλασιασμός
- Ελαχιστοποίηση Πολλαπλασιασμών: Low Hamming Weight
- Παράδειγμα: $e \in \{3, 17, 65537 = 2^{16} + 1 (RFC4871)\}$
- Μπορεί e να είναι πρώτος
- Ανεξάρτητη επιλογή από p, q

Βελτίωση αποκρυπτογράφησης

Το κλειδί αποκρυπτογράφησης δεν μπορεί να είναι μικρό

- Επιθέσεις brute force
- Εξειδικευμένες επιθέσεις
- $|d| > \frac{\lambda}{3}$

Επιτάχυνση

- Υπολογισμός $c_p = c \bmod p, c_q = c \bmod q$
- Υπολογισμός $d_p = d \bmod (p-1),\ d_q = d \bmod (q-1),$
- Υπολογισμός $m_p = c_p^{d_p} \bmod p, m_q = c_q^{d_q} \bmod q$
- Συνδυασμός με CRT για m

Βελτίωση:4 φορές

Σχετιζόμενα (Δύσκολα) Προβλήματα

Το πρόβλημα RSA (e-οστές ρίζες)

Δίνονται $n = pq$, e με $gcd(e, \phi(n)) = 1$ και $c \in \mathbb{Z}_n^*$.
Να βρεθεί η τιμή $c^{\frac{1}{e}}(=d)$

Το πρόβλημα RSA-KINV

Δίνονται $n = pq$, e με $gcd(e, \phi(n)) = 1$.
Να βρεθεί η τιμή $e^{-1} \pmod{\phi(n)}(= d)$

Το πρόβλημα FACTORING

Δίνεται $n = pq$ με p, q πρώτοι. Να βρεθούν τα p, q

Το πρόβλημα COMPUTE-$\phi(n)$

Δίνεται $n, \phi(n)$ με $n = pq$ όπου p, q πρώτοι.
Να βρεθούν τα p, q

Σχέσεις Προβλημάτων I

RSAP $\leq$ RSA-KINV

Αν βρεθεί $d = e^{-1}$ υπολογίζεται εύκολα $c^d \bmod n$

RSA-KINV $\leq$ FACTORING

Έστω ότι μπορούν να βρεθούν p, q για $n = pq$ (λύση FACTORING)
Υπολογισμός $(p-1) \cdot (q-1)$
Χρήση EGCD για εύρεση $\frac{1}{e}$

Σχέσεις Προβλημάτων II

COMPUTE-$\phi(n)$ $\equiv$ FACTORING

$n = pq$ και $\phi(n) = (p-1)(q-1)$
Προκύπτει η εξίσωση
$p^2 - (n - \phi(n) + 1)p + n = 0$

FACTORING $\leq^r$ RSA-KINV (RSA,1977)

Αν γνωρίζουμε τον $d = e^{-1}$ μπορούμε να κατασκευάσουμε πιθανοτικό αλγόριθμο παραγοντοποίησης του n με βάση τον Miller Rabin

Σχέσεις Προβλημάτων III

Πώς;

- Υπολογίζουμε $s = ed - 1 (= k\phi(n))$
- $\phi(n), s$ είναι ζυγοί, άρα $s = 2^t r$ με $t \geq 1$ και r μονό
- Επιλέγουμε τυχαίο $a \in \{1, \cdots n-1\}$
- Δύο περιπτώσεις:
  - $gcd(a, n) > 1$: Βρέθηκε - Τερματισμός
  - $gcd(a, n) = 1$: Από Θ. Euler $a^s = a^{k\phi(n)} = 1 \pmod n$
- Δηλαδή: $(a^{\frac{s}{2}}) \in$\{ 1,-1,+x,-x \}$\bmod n$ (τετραγωνικές ρίζες)
- Αν $(a^{\frac{s}{2}}) = x \pmod n$ ή τότε $p = gcd(x-1, n)$
- Αν όχι - επανάληψη με $(a^{\frac{s}{4}}), \cdots, a^{\frac{s}{2^{O(logn)}}}$
- μέχρι να βρεθεί μη τετριμμένη ρίζα

Σχέσεις Προβλημάτων

Συνολική Εικόνα

RSAP $\leq$ RSA-KINV $\leq$ COMPUTE-$\phi(N)$ $\equiv$ FACTORING $\leq^r$ RSA-KINV

Αργότερα (May, 2004) FACTORING $\leq$ RSA-KINV

Συνολική Εικόνα - Νέα

RSAP $\leq$ RSA-KINV $\equiv$ COMPUTE-$\phi(N)$ $\equiv$ FACTORING

Το RSAP λοιπόν δεν είναι δυσκολότερο από το FACTORING
Μάλλον είναι ευκολότερο αλλά δεν γνωρίζουμε ακριβώς πόσο.
Υπόθεση RSA: Το RSAP είναι υπολογιστικά απρόσιτο.

Επίθεση μικρού δημόσιου εκθέτη

Κακή ιδέα

Χρήση $e = 3$ για να μειωθεί το κόστος κρυπτογράφησης

- Τρία δημόσια κλειδιά $k_1 = (3, n_1), k_2 = (3, n_2), k_3 = (3, n_3)$
- Ο $\mathcal{A}$ γνωρίζει 3 κρυπτογραφήσεις του ίδιου μηνύματος m
  - $c_1 = \texttt{Encrypt}(k_1, m) = m^3 \bmod n_1$
  - $c_2 = \texttt{Encrypt}(k_2, m) = m^3 \bmod n_2$
  - $c_3 = \texttt{Encrypt}(k_3, m) = m^3 \bmod n_3$
- Χρήση CRT για υπολογισμό του $c = m^3 \bmod n_1 n_2 n_3$
- Αλλά $m^3 < n_1 n_2 n_3$ αφού $m < n_1$ και $m < n_2$ και $m < n_3$
- Εύρεση μηνύματος ως $m = \sqrt[3]{c}$

Επίθεση μικρού ιδιωτικού εκθέτη - Θεωρία

Αναπαράσταση Με Συνεχή Κλάσματα

Έστω $x \in \mathbb{R}$. Τότε $\exists a_0, a_1, a_2, a_3, \cdots : x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\cdots}}}}$

Αν $x \in \mathbb{Q}$ τότε η αναπαράσταση είναι πεπερασμένη

Θεώρημα

Έστω $x \in \mathbb{R}$. Αν $|x - \frac{a}{b}| < \frac{1}{2b^2}$ τότε το κλάσμα $\frac{a}{b}$ εμφανίζεται στην προσέγγιση με συνεχή κλάσματα του x.

Βασική ιδέα

Για μεγάλες τιμές του e (μικρές τιμές του d - $d < \frac{1}{3}n^{\frac{1}{4}}$) μπορούμε να βρούμε το d μέσω της αναπαράστασης με συνεχή κλάσματα.

Επίθεση μικρού ιδιωτικού εκθέτη - Προσαρμογή I

$$n - \phi(n) = pq - (p-1)(q-1) = p + q - 1 < 3\sqrt{n} \quad (1)$$

Ο $\mathcal{A}$ γνωρίζει το e και ότι $\exists k : ed = 1 + k\phi(n)$
Επίσης ισχύει

$$e < \phi(n) \Rightarrow ke < k\phi(n) < 1 + k\phi(n) = ed \Rightarrow k < d \quad (2)$$

Επίσης:

$$|\frac{e}{n} - \frac{k}{d}| = |\frac{ed - kn}{dn}| = |\frac{1 + k\phi(n) - kn}{dn}| = |\frac{1 - k(n - \phi(n))}{dn}| \leq \frac{1 + k(n - \phi(n))}{dn}$$

Επίθεση μικρού ιδιωτικού εκθέτη - Προσαρμογή ΙΙ

Από την σχέση (1):

$$|\frac{e}{n} - \frac{k}{d}| < \frac{3k\sqrt{n}}{dn} = \frac{3k}{d\sqrt{n}}$$

Από την σχέση (2):

$$|\frac{e}{n} - \frac{k}{d}| < \frac{3}{\sqrt{n}}$$

Από την υπόθεση για το μέγεθος του d έχουμε:

$$d < \frac{\sqrt[4]{n}}{3} \Rightarrow d^2 < \frac{\sqrt{n}}{9} \Rightarrow 2d^2 < \frac{2\sqrt{n}}{9} < \frac{\sqrt{n}}{3} \Rightarrow \frac{3}{\sqrt{n}} < \frac{1}{2d^2}$$

Επίθεση μικρού ιδιωτικού εκθέτη - Προσαρμογή ΙΙΙ

Τελικά:

$$|\frac{e}{n} - \frac{k}{d}| < \frac{1}{2d^2}$$

Επειδή $gcd(k, d) = 1$ το κλάσμα k/d είναι απλοποιημένο, και κατά συνέπεια θα εμφανίζεται στην προσέγγιση του e/n με συνεχή κλάσματα.

Επίθεση μικρού ιδιωτικού εκθέτη

Διαδικασία

- Κρυπτογράφηση μηνύματος m (επιλογής του $\mathcal{A}$)
- Κατασκευή αναπαράστασης του e/n με συνεχή κλάσματα
- Ύψωση c σε κάθε έναν από τους παρονομαστές της
- Επιλογή παρονομαστή που επιτυγχάνει σωστή αποκρυπτογράφηση

Επίθεση μικρού ιδιωτικού εκθέτη - Παράδειγμα

$(e, n) = (207031, 242537)$

Προσεγγίσεις-δοκιμές για $m = 8$ και $8^{207031} \bmod 242537 = 46578$

$$\frac{207031}{242537} = \mathbf{0} + \frac{1}{\frac{242537}{207031}} =$$

$$\mathbf{0} + \frac{1}{\mathbf{1} + \frac{35006}{207031}} =$$

$$0 + \frac{1}{\mathbf{1} + \frac{1}{\frac{207031}{35006}}} =$$

$$\mathbf{0} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{5} + \frac{32280}{35006}}} =$$

$$\mathbf{0} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{5} + \frac{1}{1 + \frac{35006}{32280}}}} = \cdots$$

$$[0; 1] = 0 + \frac{1}{1} = 1 \quad \text{και}$$

$$46578^1 \bmod 242537 = 46578$$

$$[0; 1; 5] = 0 + \frac{1}{1 + \frac{1}{5}} = \frac{5}{6} \quad \text{και}$$

$$46578^6 \bmod 242537 = 175938$$

$$[0; 1; 5; 1] = 0 + \frac{1}{1 + \frac{1}{5+1}} = \frac{6}{7} \quad \text{και}$$

$$46578^7 \bmod 242537 = 8$$

Επίθεση κοινού γινομένου I

Πολύ Κακή ιδέα

Χρήση κοινού n για να μειωθεί το κόστος πράξεων modulo

Σενάριο

TTP διαθέτει $n = pq$ και μοιράζει στους χρήστες A, B τα κλειδιά (e_A, d_A) και (e_B, d_B).

Εσωτερική Επίθεση (από γνώστη του d_A)

- Ο A αφού γνωρίζει το d_A μπορεί να παραγοντοποιήσει το n (αναγωγή FACTORING $\leq^r$ RSA-KINV)
- Υπολογισμός $\phi(N)$
- Ευρεση $d_B = e_B^{-1} \pmod{\phi(n)}$ με EGCD
- Διάβασμα όλων των μηνυμάτων του B

Επίθεση κοινού γινομένου II

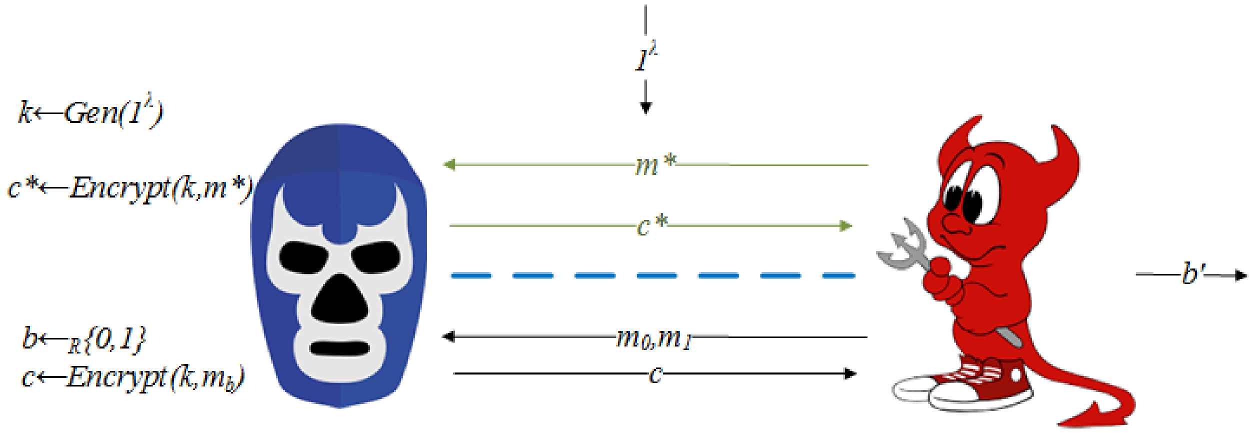
Εξωτερική Επίθεση

- Ο $\mathcal{A}$ γνωρίζει $(n, e_1), (n, e_2)$
- Μπορεί να αποκρυπτογραφήσει οποιοδήποτε κοινό μήνυμα m
  - $c_1 = m^{e_1} \bmod n$
  - $c_2 = m^{e_2} \bmod n$
- Αν $gcd(e_1, e_2) = 1$ τότε με τον EGCD μπορούν να βρεθούν αποδοτικά t_1, t_2:

$$e_1 t_1 + e_2 t_2 = 1$$

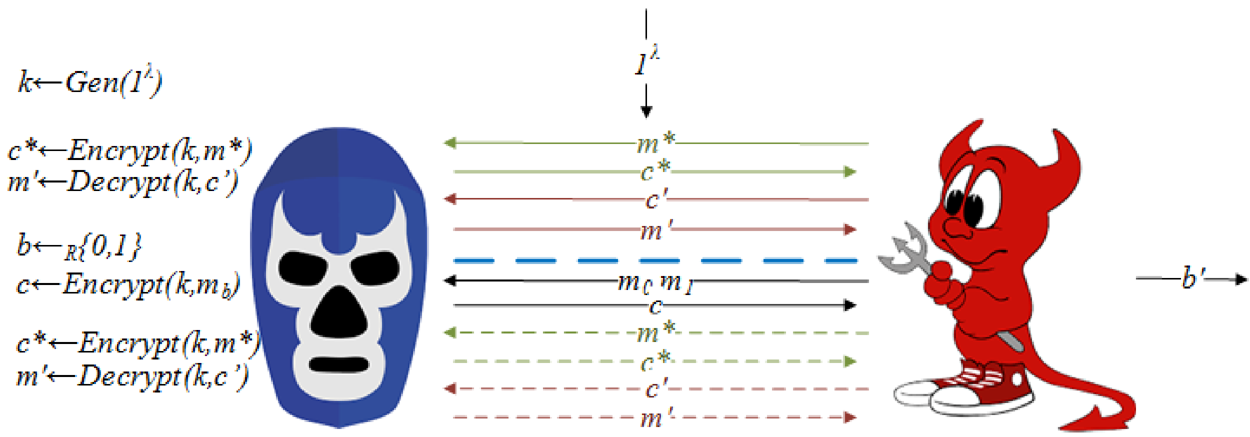
- $c_1^{t_1} c_2^{t_2} = m^{e_1 t_1} m^{e_2 t_2} = m^1 = m$

Το RSA δεν διαθέτει IND-CPA



- Γιατί είναι ντετερμινιστικό
- Ο $\mathcal{A}$ μπορεί να ξεχωρίσει κρυπτογραφήσεις μηνυμάτων του
- τις οποίες μπορεί να παράγει μόνος του (δημόσιο κλειδί)

Το RSA δεν διαθέτει IND-CCA(2) I



Αφού δεν διαθέτει IND-CPA (δεν χρειάζεται το decryption oracle)

Το RSA δεν διαθέτει IND-CCA(2) II

...αλλά και λόγω Malleability

- Στόχος: Αποκρυπτογράφηση του $c = m_b^e \bmod n$
- Μπορεί να αποκρυπτογραφήσει το $c' = c_b x^e \bmod n$ όπου το x είναι δικής του επιλογής
- Ανακτά το $m_b = \frac{m'}{x}$
- Αν $m_b = m_0$ επιστρέφει $b^* = 0$ αλλιώς επιστρέφει $b^* = 1$

Ομομορφικές ιδιότητες

$\texttt{Encrypt}((e, n), m_1) \cdot \texttt{Encrypt}((e, n), m_2) = m_1^e \cdot m_2^e \bmod n = (m_1 \cdot m_2) \bmod n = \texttt{Encrypt}((e, n), m_1 \cdot m_2)$

Διαρροή Πληροφοριών I

Τι διαρρέει (χωρίς συνέπειες)

Jacobi symbol $(\frac{c}{n}) = (\frac{m^e}{n}) = (\frac{m^e}{p})(\frac{m^e}{q}) = (\frac{m}{p})(\frac{m}{q}) = (\frac{m}{n})$

Τι δεν διαρρέει

Έστω $c = m^e \bmod n$

$parity((e, n), c) = (m \bmod n) \bmod 2$ - τελευταίο bit του plaintext

$loc((e, n), c) = (m \bmod n) > \frac{n}{2}$ - κάτω μισό / πάνω μισό

Διαρροή Πληροφοριών II

Θεώρημα (Goldwasser, Micali, Tong)

Για κάθε στιγμιότυπο του RSA (e,n), τα παρακάτω είναι ισοδύναμα:

1. Υπάρχει ένας αποδοτικός αλγόριθμος $\mathcal{A}$ τέτοιος ώστε $\mathcal{A}(c) = m, \forall m \in \mathbb{Z}_n$
2. Υπάρχει ένας αποδοτικός αλγόριθμος που υπολογίζει την συνάρτηση *parity*
3. Υπάρχει ένας αποδοτικός αλγόριθμος που υπολογίζει την συνάρτηση *loc*

Διαρροή Πληροφοριών III

$parity \to loc$

$loc(c) = parity(c \cdot \mathtt{Encrypt}(2))$ γιατί:

Διαρροή Πληροφοριών IV

$loc \rightarrow parity$

$loc(c) = parity(c \cdot \texttt{Encrypt}(2))$ γιατί:

$parity(c \cdot \texttt{Encrypt}(2)) = parity(\texttt{Encrypt}(2 \cdot m)) =$
$(2m \bmod n) \bmod 2$

$loc(c) = 1 \Rightarrow m > \frac{n}{2} \Rightarrow 2m > n$ δηλ. $(2m \bmod n) \bmod 2 = 1$
αφού n μονός
και $2m \bmod n = 2m - n$ αφού $n < 2m < 2n$

$loc(c) = 0 \Rightarrow m \leq \frac{n}{2}$ τότε $2m \leq n$ δηλ. $(2m \bmod n) \bmod 2 = 0$

Διαρροή Πληροφοριών V

$parity \rightarrow loc$

$parity(c) = loc(c \cdot \texttt{Encrypt}(2^{-1}))$

Παρατηρώ:

$loc(c \cdot \texttt{Encrypt}(2^{-1})) = loc(\texttt{Encrypt}(m \cdot 2^{-1})) =$
$loc(\texttt{Encrypt}(m \cdot \frac{n+1}{2}))$

$parity(c) = 0 \Rightarrow m \bmod 2 = 0$ τότε: $\frac{m}{2} < \frac{n}{2}$ αφού $m < n$

$parity(c) = 1 \Rightarrow m \bmod 2 = 1$ τότε:
$(m\frac{n+1}{2}) \bmod n = ((2k+1)\frac{n+1}{2}) \bmod n = k(n+1) + \frac{n+1}{2} \bmod n =$
$k + \frac{n+1}{2} > \frac{n}{2}$

Διαρροή Πληροφοριών VI

Απόδειξη $(1) \Leftrightarrow (2) \Leftrightarrow (3)$
Προφανώς $(1) \Rightarrow (2)$ (αν μπορώ να αποκρυπτογραφήσω ξέρω parity) και $(2) \Leftrightarrow (3)$ (από προηγούμενα)
Για το $(3) \Rightarrow (1)$
Δυαδική αναζήτηση, για το m, χρησιμοποιώντας την loc:
$loc(\texttt{Encrypt}(m)) = 0 \iff m \in [0, \frac{n}{2})$ και
$loc(\texttt{Encrypt}(2m)) = 0 \iff m \in [0, \frac{n}{4}) \cup (\frac{n}{2}, \frac{3n}{4})$
$loc(\texttt{Encrypt}(4m)) = 0 \iff m \in [0, \frac{n}{8}) \cup (\frac{n}{2}, \frac{5n}{8})$
Άρα αν $loc(\texttt{Encrypt}(m)) = 0$ και $loc(\texttt{Encrypt}(2m)) = 0$ και $loc(\texttt{Encrypt}(4m)) = 0$ τότε $m \in [0, \frac{n}{8})$
... κ.ο.κ. για $\log n$ βήματα.

padded-RSA I

Βασική ιδέα

- Προσθήκη ψηφίων τυχαιοποίησης r στο μήνυμα.
- Κρυπτογράφηση $f(m, r)$
- Αποκρυπτογράφηση
- Αντιστροφή f (πρέπει να γίνεται εύκολα)

PKCS1 v1.5 $f(m, r) = r || m$

padded-RSA II

Έστω $|m| = l$.

- Πριν την κρυπτογράφηση δημιουργείται το μήνυμα: $\bar{m} = r||m$, όπου r είναι μια τυχαία συμβολοσειρά από $\lambda - l$ bits.
- Μετατροπή του $\bar{m}$ σε ακέραιο
- Η κρυπτογράφηση γίνεται (κανονικά) ως: $\bar{c} = \bar{m}^e \bmod n$
- Η αποκρυπτογράφηση γίνεται (κανονικά) ως $\bar{c}^d \bmod n = \bar{m}$
- Από το $\bar{m}$ κράταμε μόνο τα l bits χαμηλότερης τάξης.

Αποδεικνύεται ότι διαθέτει ασφάλεια IND-CPA, όχι όμως IND-CCA (μπορούμε να εκμεταλλευτούμε την δομή του μηνύματος)

Η επίθεση του Bleichenbacher (Million Message Attack) I

Βασική Ιδέα:Padding Oracle

Χρήση ενός συστήματος το οποίο μπορεί να αποφανθεί αν ένα κρυπτοκείμενο έχει προκύψει με σωστό padding

- Ακριβής Μορφή padded μηνύματος στο PKCS1: $PKCS(r, m) =$ 0x 00||02||$\mathtt{r}$||00||$\mathtt{m}$
- Αποκρυπτογράφηση:
  - Έλεγχος πρώτου byte για την τιμή 0
  - Έλεγχος δεύτερου byte για την τιμή 2
  - Αναζήτηση του 0
  - Ανάκτηση του m

Η επίθεση του Bleichenbacher (Million Message Attack) II

- Το oracle στην πράξη:
  - Ύπαρξη μηνύματος λάθους για μη αποδεκτό padding ή
  - ανάκτηση της πληροφορίας μέσω side channel (πχ. χρόνος απάντησης)

Fact

Μια τυχαία συμβολοσειρά από bytes θα έχει την σωστή μορφή δηλ.

0x 00||02||non-zero||00||non-zero

με πιθανότητα από 2^{-17} εώς 2^{-15}.

Η επίθεση του Bleichenbacher (Million Message Attack) III

Η επίθεση:

- Στόχος: Αποκρυπτογράφηση ενός c
- Ο $\mathcal{A}$ ξέρει ότι $c = PKCS(r, m)^e \bmod n$
- Διαλέγει *πολλά* τυχαία s
- Στέλνει στο padding oracle μηνύματα της μορφής $c' = cs^e \bmod n$
- Λόγω ιδιοτήτων RSA: $c' = (sPKCS(r, m))^e \bmod n$
- Στα περισσότερα η αποκρυπτογράφηση δίνει λάθος padding

Η επίθεση του Bleichenbacher (Million Message Attack) IV

- Αν *δεν* δώσει:
  - Ξέρουμε ότι το padded plaintext έχει σωστή μορφή
  - Δηλαδή το $sPKCS(r, m)$ βρίσκεται σε ένα συγκεκριμένο εύρος τιμών (ξεκινούν με 0002)
  - Τροποποίηση του s ώστε να περιορίζεται το εύρος της αναζήτησης
  - Επανάληψη
- Με 300.000 εως 2.000.000 c' μπορεί να αποκρυπτογραφηθεί το c

Λύσεις

- Αφαίρεση μηνύματος λάθους για padding
- Τροποποίηση ώστε να υπάρχει ασφάλεια IND-CCA2

Ιδέες;

RSA-OAEP (PKCS1 v2.0) I

Βασική Ιδέα

Τα τυχαία bits πρέπει να 'διαχυθούν' σε όλο το κρυπτοκείμενο (Δίκτυα Feistel)
Πρέπει να υπάρχει κάποιου είδους δέσμευση στο αρχικό μήνυμα ενσωματωμένη στο κρυπτοκείμενο
(Συνάρτηση Σύνοψης)

Υποθέσεις

- $|m| = l$
- $\mathcal{G}, \mathcal{H} : \{0,1\}^{2l} \rightarrow \{0,1\}^{2l}$ συναρτήσεις σύνοψης
- $r \in \{0,1\}^{2l}$

RSA-OAEP (PKCS1 v2.0) II

Κρυπτογράφηση

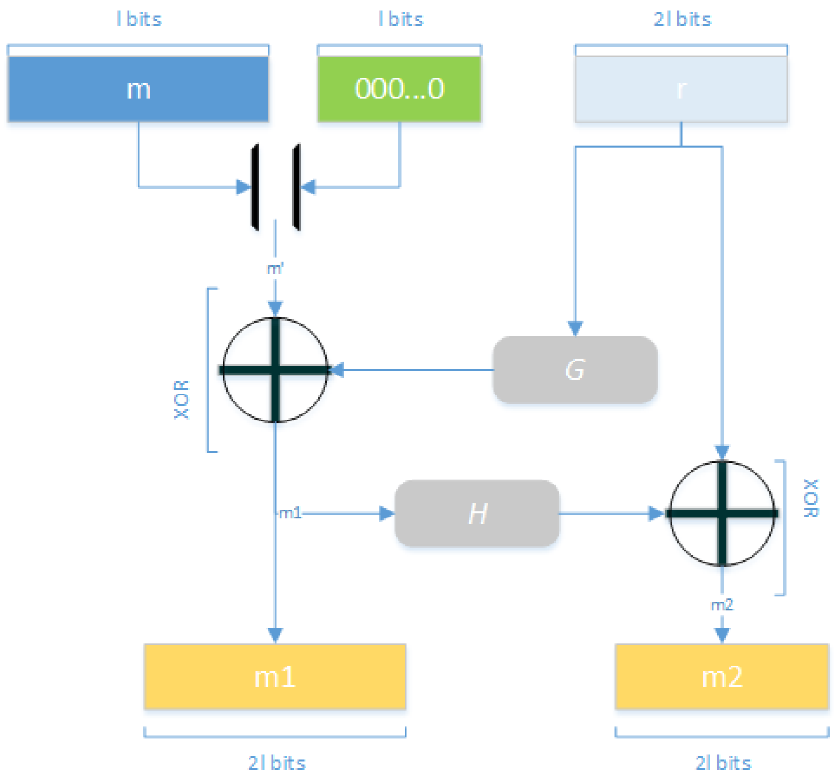
- Padding για μέγεθος $2l$: $m' = m||0^l$
- Διάχυση bits τυχαιότητας $m_1 = \mathcal{G}(r) \oplus m'$
- Δέσμευση $m_2 = r \oplus \mathcal{H}(m_1)$
- Συνδυασμός $\bar{m} = m_1||m_2$
- Κρυπτογράφηση $\bar{c} = \bar{m}^e \bmod n$

RSA-OAEP (PKCS1 v2.0) III

Αποκρυπτογράφηση

- Αποκρυπτογράφηση $\bar{c}^d \bmod n = \bar{m}$
- Θεωρούμε ότι $\bar{m} = m_1||m_2$ (χωρισμός στα δύο)
- $\mathcal{H}(m_1) \oplus m_2$
- Ανακτούμε το r (γιατί;)
- $m_1 \oplus \mathcal{G}(r)$
- Ανακτούμε το m'
- Έλεγχος l bits χαμηλότερης τάξης
- Αν είναι 0 τότε ανάκτηση μηνύματος από τα l bits υψηλότερης τάξης

RSA-OAEP (PKCS1 v2.0) IV



Βιβλιογραφία

1. St. Zachos and Aris Pagourtzis. Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία. Πανεπιστημιακές Σημειώσεις
2. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography (Chapman and Hall/Crc Cryptography and Network Security Series). Chapman and Hall/CRC, 2007
3. Nigel Smart. Introduction to cryptography
4. Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science-Business Media, 2009.
5. Dan Boneh, Introduction to cryptography, online course
6. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21:120–126, 1978
7. Alexander May. Computing the rsa secret key is deterministic polynomial time equivalent to factoring. In Advances in Cryptology–CRYPTO 2004, pages 213–219. Springer, 2004.
8. Michael J Wiener. Cryptanalysis of short rsa secret exponents. Information Theory, IEEE Transactions on, 36(3):553–558, 1990.
9. Boneh, Dan. "Twenty years of attacks on the RSA cryptosystem." Notices of the AMS 46.2 (1999): 203-213.
10. Bellare, Mihir, and Phillip Rogaway. "Optimal asymmetric encryption." Advances in Cryptology—EUROCRYPT'94. Springer Berlin Heidelberg, 1995.
11. Bleichenbacher, Daniel. "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS1" Advances in Cryptology—CRYPTO'98. Springer Berlin Heidelberg, 1998.