Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία

Κρυπτογραφία Δημοσίου Κλειδιού

Άρης Παγουρτζής – Στάθης Ζάχος

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Κρυπτοσύστημα RSA (Rivest, Shamir, Adlemann, 1977)

Ορισμός RSA

- Παραγωγή κλειδιών
  1. Εύρεση πρώτων p, q μεγάλου μήκους (> 1000 ψηφία) – χρήση *ελέγχου πρώτων αριθμών* (π.χ. Miller-Rabin).
  2. Υπολογισμός $n = p \cdot q$ και $\varphi(n) = (p-1) \cdot (q-1)$.
  3. Επιλογή $e \in U(\mathbb{Z}_n) : \gcd(e, \varphi(n)) = 1$.
  4. Υπολογισμός $d : e \cdot d \equiv 1 \pmod{\varphi(n)}$ – χρήση *Επεκταμένου Ευκλείδειου αλγόριθμου*.

  Δημόσιο κλειδί: e, n.
  Ιδιωτικό κλειδί: d.
- Κρυπτογράφηση
  $enc(m) = m^e \bmod n \quad (m \in \mathbb{Z}_n)$.
- Αποκρυπτογράφηση
  $dec(c) = c^d \bmod n$.

Ιδιότητες του RSA

- Ορθότητα

$$dec(m^e \bmod n) \equiv (m^e)^d \equiv m^{k \cdot \varphi(n)+1} \equiv m \pmod{n}$$

  Αποδεικνύεται εύκολα για $m \in U(\mathbb{Z}_n)$, αλλά ισχύει και για κάθε $m \in \mathbb{Z}_n \setminus U(\mathbb{Z}_n)$ (**άσκηση**).
- Και οι τρεις διαδικασίες (παραγωγή κλειδιών, κρυπτογράφηση, αποκρυπτογράφηση) υλοποιούνται αποδοτικά.

RSA και παραγοντοποίηση

Αν κάποιος μπορει να βρει τα p και q μπορεί εύκολα να υπολογίσει το $\varphi(n)$ και επομένως και το d:

$$\text{RSA-decrypt}(c, e, n) \leq^p \text{FindSecrExp}(e, n) \leq^p$$

$$\varphi(n) - \text{Computation} \leq^p \text{Factoring}(n)$$

Η εύρεση του $\varphi(n)$ οδηγεί σε παραγοντοποίηση (άρα είναι παρόμοιας δυσκολίας) λύνοντας ως προς p, q:

$$n = p \cdot q$$
$$\varphi(n) = (p-1) \cdot (q-1)$$

Επομένως:

$$\text{RSA-decrypt}(c, e, n) \leq^p \text{FindSecrExp}(e, n) \leq^p$$

$$\varphi(n) - \text{Computation} \equiv^p \text{Factoring}(n)$$

Εύρεση μυστικού εκθέτη $d \Rightarrow$ παραγοντοποίηση του n

Πρόταση

Η εύρεση του ιδιωτικού κλειδιού d (εκθέτη αποκρυπτογράφησης) του RSA, οδηγεί στην παραγοντοποίηση του n με πολύ μεγάλη πιθανότητα.

Απόδειξη.

Αν γνωρίζουμε το d μπορούμε να σχεδιάσουμε τον παρακάτω πιθανοτικό αλγόριθμο:

- Υπολογίζουμε $u = ed - 1$. Ισχύει
  $\varphi(n) \mid ed - 1 \Rightarrow \forall a \in U(\mathbb{Z}_n) : a^u \equiv 1 \pmod{n}$.
- Χρησιμοποιούμε την ίδια ιδέα που είδαμε στην απόδειξη του Miller-Rabin:
  Γράφουμε $u = t \cdot 2^s$ και παίρνουμε sequences
  $\langle b^t, b^{2t}, \ldots, b^{2^i t}, \ldots b^{2^s t} \rangle \pmod{n}$,
  για διάφορες τυχαία επιλεγμένες τιμές του b.

Όπως και στο Miller-Rabin, αποδεικνύεται ότι τουλάχιστον τα μισά $b \in U(\mathbb{Z}_n)$ δίνουν factoring sequences. □

Η σχέση των προβλημάτων ως τώρα

$$\text{RSA-decrypt}(c, e, n) \leq^p \textit{FindSecrExp}(e, n) \leq^p$$

$$\varphi(n) - \text{Computation} \equiv^p \text{Factoring}(n) \leq^{rp} \text{FindSecrExp}(e, n)$$

Επίθεση Κοινού Γινομένου

Σενάριο: μια *Έμπιστη Αρχή (Trusted Third Party)* διανέμει το ίδιο γινόμενο n και διαφορετικά ζεύγη (e_1, d_1) και (e_2, d_2) σε δύο χρήστες. Οι πρώτοι αριθμοί p, q είναι γνωστοί μόνο στην Έμπιστη Αρχή. Τι πρόβλημα υπάρχει;

(i) Ο χρήστης 1 μπορεί να υπολογίσει $(e_1 \cdot d_1 - 1)$ και να παραγοντοποιήσει το n με τον πιθανοτικό αλγόριθμο.

(ii) Μπορεί επίσης να υπολογίσει έναν εκθέτη αποκρυπτογράφησης χωρίς παραγοντοποίηση του n ως εξής:

- Γνωρίζει ότι $g_0 = e_1 \cdot d_1 - 1 = k \cdot \varphi(n)$, για κάποιο $k \in \mathbb{N}$.
- Από κατασκευή ισχύει $\gcd(e_2, \varphi(n)) = 1$.
- Επομένως, διαιρώντας διαδοχικά το g_0 με τους κοινούς παράγοντές του με το e_2 βρίσκουμε $a = g_i = k' \cdot \varphi(n),\ \gcd(e_2, a) = 1$.
- Το $d_2' = (e_2)^{-1} \pmod{a}$ μπορεί να χρησιμοποιηθεί ως εκθέτης αποκρυπτογράφησης (*γιατί;*).

Μερική ανάκτηση πληροφοριών στο RSA

Σχετική έννοια: Semantic Security, το υπολογιστικό ανάλογο της Perfect Secrecy.

Ενδιαφέρει η ποσότητα πληροφορίας που μπορεί να διαρρεύσει σε εφικτό υπολογιστικό χρόνο.

Διαρροή της τιμής του συμβόλου Jacobi

Έστω $c = m^e \bmod n$. Τότε:
$(\frac{c}{n}) = (\frac{m^e}{p}) \cdot (\frac{m^e}{q}) = (\frac{m}{p})^e \cdot (\frac{m}{q})^e = (\frac{m}{p}) \cdot (\frac{m}{q}) = (\frac{m}{n})$

Αυτή η διαρροή δεν θεωρείται απειλητική για την ασφάλεια του RSA.

Μερική ανάκτηση πληροφοριών στο RSA

Έστω $c = m^e \bmod n$.

Μπορούμε από τα (c, e, n) να μάθουμε το τελευταίο bit του m;

Ή το 'bit' που μας λέει αν $m > \frac{n}{2}$;

Θα δούμε ότι κάθε μία από τις δύο αυτές πληροφορίες είναι ισοδύναμη με το σπάσιμο του κρυπτοσυστήματος.

$$parity_{n,e}(c) = \begin{cases} 0, & \text{αν } m \text{ είναι άρτιος} \\ 1, & \text{αν } m \text{ είναι περιττός} \end{cases}$$

$$loc_{n,e}(c) = \begin{cases} 0, & \text{αν } m \leq \frac{n}{2} \\ 1, & \text{αν } m > \frac{n}{2} \end{cases}$$

όπου m το μοναδικό $m \in \mathbb{Z}_n :\ m^e \bmod n = c$

Μερική ανάκτηση πληροφοριών στο RSA

Πρόταση

Αν μπορούμε να υπολογίσουμε οποιαδήποτε από τις συναρτήσεις loc ή parity (για όλες τις εισόδους) τότε μπορούμε να βρούμε το απλό κείμενο (σπάσιμο του RSA.)

Απόδειξη.

Στηρίζεται στην *πολλαπλασιαστική ιδιότητα* της κρυπτογράφησης RSA:
$enc_{n,e}(m_1) \cdot enc_{n,e}(m_2) = enc_{n,e}(m_1 \cdot m_2)$
Παρατηρήστε ότι:

- $loc_{n,e}(c) = parity_{n,e}(enc_{n,e}(2 \cdot m)) = parity_{n,e}(c \cdot enc_{n,e}(2))$
- $parity_{n,e}(c) = loc_{n,e}(enc_{n,e}(m \cdot 2^{-1} \pmod{n})) = loc_{n,e}(c \cdot enc_{n,e}(\frac{n+1}{2}))$

Επομένως οι δύο συναρτήσεις είναι ισοδύναμες υπολογιστικά (ως προς πολυωνυμικό χρόνο). □

Απόδειξη (συν.)

Μένει να εφαρμόσουμε δυαδική αναζήτηση, χρησιμοποιώντας την *loc*, για να βρούμε το m:

$loc_{n,e}(enc(m)) = 0 \iff x \in [0, \frac{n}{2})$

$loc_{n,e}(enc(2m)) = 0 \iff x \in [0, \frac{n}{2}) \cup [\frac{n}{2}, \frac{3n}{4})$

...

κ.ο.κ. για $\log n$ βήματα.

Επομένως, αποδοτικός υπολογισμός της *loc* (ή της *parity*) οδηγεί σε αποκρυπτογράφηση. Συμπέρασμα;

Επίθεση μικρού εκθέτη

Έστω τα δημόσια κλειδιά των Bob, Charlie και Diane $p_B = (n_1, 3)$, $p_C = (n_2, 3)$, $p_D = (n_3, 3)$, έχουν δηλαδή τον ίδιο μικρό εκθέτη. Η Alice στέλνει σε όλους το ίδιο μήνυμα m.

Η Eve σχηματίζει το σύστημα
$c_1 = m^3 \pmod{n_1}$
$c_2 = m^3 \pmod{n_2}$
$c_3 = m^3 \pmod{n_3}$

Ερώτηση: τι δίνει το σύστημα αυτό με χρήση CRT;

Απάντηση: την τιμή του m^3 στο $\mathbb{Z}n_1n_2n_3$, δηλαδή το m^3 (γιατί;).

Συνιστώμενες παράμετροι του RSA

- $|n| \geq 2048$ (μέχρι το 2030 περίπου, μετά $|n| \geq 3072$).
- p, q περίπου ίδιου μήκους.
- $p - q > 2^{\frac{|n|}{2}-100}$.
- $p-1, q-1$ έχουν και 'μεγάλους' πρώτους παράγοντες (αποφυγή κυκλικών επιθέσεων).
- $66537 < e \leq 2^{256}$. Επιλέγεται *πριν* από τα p, q.
- $ed \equiv 1 \pmod{\lambda(n) = \text{lcm}(p-1, q-1)}$.
- $2^{\frac{|n|}{2}} < d < \text{lcm}(p-1, q-1)$.
- Περισσότερα: NIST.

Το κρυπτοσύστημα Rabin

Ορισμός

Δημόσιο κλειδί: $n = pq, b < n$. Ιδιωτικό κλειδί: p, q.

$$enc(x) = (x \cdot (x + b)) \bmod n$$

$$dec(y) = x' - \tfrac{b}{2} \bmod n, \; x'^2 \equiv y + \tfrac{b^2}{4} \pmod{n}$$

Η αποκρυπτογράφηση συνίσταται ουσιαστικά στην *εύρεση τετραγωνικών ριζών* $\pmod n$ του $y' = y + \frac{b^2}{4}$:

$\pm y'^{(p+1)/4} \pmod p$, $\pm y'^{(q+1)/4} \pmod q$, αν γνωρίζουμε p, q και $p \equiv q \equiv 3 \pmod 4$.

Σημαντικό: η αποκρυπτογράφηση χωρίς γνώση των p, q είναι ισοδύναμη με παραγοντοποίηση του n.

Διακριτός Λογάριθμος

Ορισμός

Έστω G μία πεπερασμένη κυκλική ομάδα τάξης n, α ένας γεννήτορας της G και $\beta \in G$.

Ο διακριτός λογάριθμος (discrete logarithm) του β στη βάση α, που συμβολίζεται $log_\alpha \beta$, είναι ο μοναδικός ακέραιος $x \in \mathbb{Z}_n$ τέτοιος ώστε $\beta = \alpha^x$.

Παράδειγμα. Για $p = 97$, η $\mathbb{Z}_{97}^*$ είναι κυκλική ομάδα τάξης $n = 96$.

Ένας γεννήτορας της $\mathbb{Z}_{97}^*$ είναι ο $\alpha = 5$.

Αφού $5^{32} \equiv 35 \pmod{97}$, έχουμε ότι $\log_5 35 = 32$ στο $\mathbb{Z}_{97}^*$.

Το πρόβλημα του Διακριτού Λογαρίθμου στο $\mathbb{Z}_p^*$

Discrete Logarithm Problem (DLP)

Δίνονται: ένας πρώτος αριθμός p, ένας γεννήτορας α του $\mathbb{Z}_p^*$ και ένα στοιχείο $\beta \in \mathbb{Z}_p^*$.

Ζητείται: Να βρεθεί ακέραιος x, $0 \leq x \leq p-2$, τέτοιος ώστε

$$\alpha^x \equiv \beta \pmod p \tag{1}$$

Το πρόβλημα DLP (στο $\mathbb{Z}_p^*$) θεωρείται υπολογιστικά δύσκολο (υπό κάποιες προϋποθέσεις). Δεν γνωρίζουμε πολυωνυμικό αλγόριθμο που να το επιλύει.

Δυσκολία του DLP: ανεξάρτητη του γεννήτορα

Πρόταση

Η δυσκολία του DLP είναι ανεξάρτητη από την επιλογή του γεννήτορα α του $\mathbb{Z}_p^*$.

Απόδειξη.

Έστω α και γ δύο γεννήτορες του $\mathbb{Z}_p^*$, και $\beta \in \mathbb{Z}_p^*$.

Έστω $x = \log_\alpha \beta, y = \log_\gamma \beta$ και $z = \log_\alpha \gamma$.

Τότε $\alpha^x \equiv \beta \equiv \gamma^y \equiv (\alpha^z)^y \pmod p$, δηλαδή $x \equiv zy \pmod{p-1}$.

Αλλά τότε $y \equiv xz^{-1} \pmod{p-1}$, δηλαδή:

$$\log_\gamma \beta \equiv (\log_\alpha \beta)(\log_\alpha \gamma)^{-1} \pmod{p-1}$$

□

Επομένως αν μπορούμε να υπολογίσουμε τον διακριτό λογάριθμο σε μία βάση α τότε μπορούμε να τον υπολογίσουμε σε οποιαδήποτε βάση γ, όπου α,γ γεννήτορες του $\mathbb{Z}_p^*$.

Αλγόριθμοι για το DLP

Προφανής αλγόριθμος: $\widetilde{O}(p)$.

Αλγόριθμος με προεπεξεργασία: υπολογίζουμε όλα τα ζεύγη (x, α^x) και ταξινομούμε ως προς δεύτερη συντεταγμένη. Χρόνος και χώρος προεπεξεργασίας $\widetilde{O}(p)$, χρόνος απάντησης ερωτήματος $\widetilde{O}(1)$.

Βελτιωμένη ιδέα: αλγόριθμος Shanks.

Αλγόριθμος Shanks

Είσοδος: πρώτος p, α γεννήτορας του $\mathbb{Z}_p^*$, $\beta \in \mathbb{Z}_p^*$.
Έξοδος: $x \in \mathbb{Z}_p^* : \alpha^x \equiv \beta \pmod p$.

1. $m := \lceil \sqrt{p-1} \rceil$
2. Υπολόγισε $\alpha^{mj} \mod p, 0 \leq j \leq m-1$
3. Ταξινόμησε τα m διατεταγμένα ζεύγη $(j, \alpha^{mj} \mod p)$ βάσει της δεύτερης συντεταγμένης (δηλαδή του $\alpha^{mj} \mod p$), σε μια λίστα L_1
4. Υπολόγισε $\beta\alpha^{-i} \mod p, 0 \leq i \leq m-1$
5. Ταξινόμησε τα m διατεταγμένα ζεύγη $(i, \beta\alpha^{-i} \mod p)$ βάσει της δεύτερης συντεταγμένης (δηλαδή του $\beta\alpha^{-i} \mod p$), σε μια λίστα L_2
6. Αναζήτησε ζεύγος $(j,y) \in L_1$ τέτοιο ώστε $(i,y) \in L_2$
7. Επίστρεψε $mj + i \mod (p-1)$

Ορθότητα αλγορίθμου Shanks:

$$\alpha^{mj} \equiv y \equiv \beta\alpha^{-i} \pmod p \Rightarrow \alpha^{mj+i} \equiv \beta p mod p$$

Πολυπλοκότητα: $\widetilde{O}(\sqrt{p})$ σε χρόνο και $\widetilde{O}(\sqrt{p})$ σε χώρο.

Ανταλλαγή Κλειδιού Diffie-Hellman

Πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman

1. Επιλογή κοινού πρώτου p, και γεννήτορα α του $\mathbb{Z}_p^*$.
2. Η **Αλίκη** επιλέγει έναν τυχαίο ακέραιο x που το γνωρίζει μόνο αυτή και στέλνει στον **Βασίλη** το μήνυμα: $\alpha^x \mod p$
3. Ο **Βασίλης** επιλέγει έναν τυχαίο ακέραιο y που γνωρίζει μόνο αυτός και στέλνει στην **Αλίκη** το μήνυμα: $\alpha^y \mod p$
4. **Βασίλης**: $k = (\alpha^x)^y \mod p$
   Αλίκη: $k = (\alpha^y)^x \mod p$

Η ασφάλεια του πρωτοκόλλου αυτού φαίνεται να βασίζεται στην δυσκολία του DLP. Αυτό δεν είναι απόλυτα ακριβές.

Στην πραγματικότητα, η ασφάλεια του πρωτοκόλλου Diffie-Hellman ταυτίζεται με την υπολογιστική δυσκολία του Προβλήματος Diffie-Hellman (DHP).

Το Πρόβλημα Diffie-Hellman

Diffie-Hellman Problem (DHP)

- *Δίνονται*: ένας πρώτος αριθμός p, ένας γεννήτορας α του $\mathbb{Z}_p^*$ και τα στοιχεία $\alpha^a \mod p$, $\alpha^b \mod p \in \mathbb{Z}_p^*$.
- *Ζητείται*: Να βρεθεί το $\alpha^{ab} \mod p$.

Πρόταση

Το DHP ανάγεται σε πολυωνυμικό χρόνο στο DLP: $DHP \leq^p DLP$

Πράγματι, αν $x = \alpha^a \mod p$ και $y = \alpha^b \mod p$, τότε $a = \log_\alpha x$ και $b = \log_\alpha y$. Επομένως, λύνοντας το DLP, μπορούμε να υπολογίσουμε τα a, b άρα και το $\alpha^{ab} \mod p$.

Δεν γνωρίζουμε αν ισχύει και το αντίστροφο (DLP$\leq^p$ DHP).

Το Πρόβλημα Απόφασης Diffie-Hellman

Decision Diffie-Hellman Problem (DDHP)

- *Δίνονται*: ένας πρώτος αριθμός p, ένας γεννήτορας α του $\mathbb{Z}_p^*$ και δύο τριάδες $\langle \alpha^a, \alpha^b, \alpha^c \rangle, \langle \alpha^a, \alpha^b, \alpha^{ab} \rangle \pmod p$.
- *Ζητείται*: Να βρεθεί (με πιθανότητα 'αρκετά' μεγαλύτερη από 1/2) ποιά είναι η "σωστή" τριάδα, δηλαδή η $\langle \alpha^a, \alpha^b, \alpha^{ab} \rangle$.

Για αποφυγή σύγχυσης, το κλασικό πρόβλημα DHP αναφέρεται συχνά και ως Computational Diffie-Hellman Problem (CDHP).

Η σχετική δυσκολία των DDHP, CDHP, DLP

Προφανώς ισχύει:

$$DDHP \leq^p CDHP \leq^p DLP$$

Cryptographic assumptions

Για κάθε πρόβλημα ορίζεται και η αντίστοιχη υπόθεση υπολογιστικής δυσκολίας του: DDH, CDH, DL.

Η σειρά ισχύος των υποθέσεων:

$$DDH \Rightarrow CDH \Rightarrow DL$$

Σημαντική παρατήρηση: υπάρχουν κυκλικές ομάδες όπου το DDHP είναι εύκολο (υπό προϋποθέσεις), ενώ το CDHP θεωρείται δύσκολο. Παράδειγμα: η ομάδα $\mathbb{Z}_p^*$ (λόγω της *δυνατότητας υπολογισμού του τελευταίου bit* του διακριτού λογαρίθμου).

Το κρυπτοσύστημα ElGamal (Taher ElGamal, Crypto'84)

Παραγωγή κλειδιών

Η Alice διαλέγει ένα πρώτο p, όπου ο $p-1$ έχει τουλάχιστον ένα μεγάλο παράγοντα, ένα γεννήτορα g της $\mathbb{Z}_p^*$, και τυχαίο $a \in \mathbb{Z}_p^*$
Δημόσιο κλειδί της Alice: $p, g, g^a \mod p$.
Ιδιωτικό κλειδί της Alice: a.

Κρυπτογράφηση

1. Ο Bob επιλέγει τυχαίο $k \in \{2, 3, \ldots, p-2\}$.
2. Ο Bob υπολογίζει $\gamma = g^k \mod p$ και $\delta = m(g^a)^k \mod p$ και στέλνει το ζευγάρι (γ, δ) στην Alice (1-to-2 message expansion).

Αποκρυπτογράφηση

1. Η Alice πρώτα υπολογίζει: $\gamma^a \equiv g^{ak} \pmod p$ και μετά αντιστρέφει σε $(g^{ak})^{-1}$.
2. Τέλος υπολογίζει:
$(g^{ak})^{-1} \cdot \delta \mod p \equiv (g^{ak})^{-1}(m(g^a)^k) \equiv (g^{ak})^{-1} \cdot m \cdot g^{ak} \equiv m \pmod p$.

Παρατηρήσεις στο ElGamal

Επειδή το k είναι τυχαίο η κρυπτογράφηση είναι πιθανοτική.

Ερώτηση: σε ποιο πρόβλημα στηρίζεται η ασφάλεια του ElGamal;

Απάντηση: στο DHP (*γιατί;*).

Και μάλιστα με ισοδυναμία!:

$$\text{CDHP} \equiv^p \text{ElGamal-decrypt}$$

Επανάληψη του $k \Rightarrow$ επίθεση KPA

Έστω m_1, m_2 δύο απλά κείμενα και $(\gamma, \delta_1), (\gamma, \delta_2)$ τα αντίστοιχα κρυπτοκείμενα (με χρήση του ίδιου k).

Η Eve γνωρίζοντας τα $\gamma, \delta_1, \delta_2$, και m_1 (KPA), υπολογίζει το m_2 ως εξής:

$$\left.\begin{aligned} \delta_1 &\equiv m_1 g^{ak} \pmod p \\ \delta_2 &\equiv m_2 g^{ak} \pmod p \end{aligned}\right\} \Rightarrow \begin{cases} \delta_1^{-1} m_1 \equiv g^{-ak} \pmod p \\ \delta_2 g^{-ak} \equiv m_2 \pmod p \end{cases}$$

Οπότε $m_2 \equiv \delta_2 \delta_1^{-1} m_1 \pmod p$.