Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ζωή Παρασκευοπούλου
Νίκος Γιανναράκης

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

19 Νοεμβρίου 2012 (v2)

1 Υπολογιστική Πολυπλοκότητα του RSA-breaking

$$RSA{-}breaking \leq^p \phi(n){-}computation \equiv^p FACTORING \equiv^{rp} exponent{-}computation$$

Πρόταση 1.1. *Αν βρούμε μία μη τετριμμένη ρίζα της ισοτιμίας* $x^2 \equiv 1 \pmod N$ *τότε μπορούμε εύκολα να παραγοντοποιήσουμε το* N.

Απόδειξη. Η ισοτιμία $x^2 \equiv 1 \pmod p$, p prime έχει δύο λύσεις modulo p, τις $\pm 1 \pmod p$.

$$\left.\begin{array}{l} x^2 \equiv 1 \pmod p \\ x^2 \equiv 1 \pmod q \end{array}\right\} \Leftrightarrow x^2 \equiv 1 \pmod N \tag{1}$$

Από την (1) προκύπτει οτι υπάρχουν τέσσερις τετραγωνικές ρίζες modulo N. Δύο από αυτές θα είναι οι τετριμμένες ρίζες $x \equiv \pm 1 \pmod N$ και οι άλλες δύο μη τετριμμένες έστω $x \equiv \pm u \pmod N$.

$$\begin{aligned} & u^2 \equiv 1 \pmod N \\ \Rightarrow\ & u^2 - 1 \equiv 0 \pmod N \\ \Rightarrow\ & (u-1)\cdot(u+1) \equiv 0 \pmod N \\ \Rightarrow\ & N \mid (u-1)\cdot(u+1) \end{aligned} \tag{2}$$

Αλλά επειδή οι $\pm u$ είναι μη τετριμμένες ρίζες θα ισχύει:

$$\begin{aligned} & u \not\equiv \pm 1 \pmod N \\ \Rightarrow\ & N \not| (u+1) \wedge N \not| (u-1) \\ \stackrel{(2),(3)}{\Longrightarrow}\ & gcd(u+1, N) = p \vee gcd(u+1, N) = q \end{aligned} \tag{3}$$

□

Θεώρημα 1. *Ένας αλγόριθμος για τον υπολογισμό του εκθέτη αποκρυπτογράφησης d σε ένα κρυπτοσύστημα RSA μπορεί να μετατραπεί σε πιθανοτικό αλγόριθμο για την παραγοντοποίηση του N.*

Απόδειξη. Ο πιθανοτικός αλγόριθμος παραγοντοποιήσης διαλέγει αριθμούς $w \in \mathbb{Z}_N^*$. Προφανώς αφού $N = p{\cdot}q$ αν για μία τυχαία επιλογή του w ισχύει $gcd(w, N) > 1$ η παραγοντοποίηση του N είναι τετριμμένη. Συνεπώς υποθέτουμε οτι $gcd(w, N) = 1$.

Διαλέγουμε ένα τυχαίο $w < N$ και υποθέτουμε ότι $gcd(w, N) = 1$. Δοθέντος του αλγορίθμου υπολογισμού του εκθέτη αποκρυπτογράφησης d και δεδομένου ότι $e \cdot d \equiv 1 \pmod{\phi(N)}$, μπορούμε να γράψουμε:

$$\begin{aligned} & e \cdot d - 1 = 2^s \cdot r, s \geq 1 \wedge rodd \\ \Rightarrow & w^{2^s \cdot r} \equiv 1 \pmod{N} \end{aligned}$$

Έστω s' ο μικρότερος αριθμός για τον οποίο

$$w^{2^{s'} \cdot r} \equiv 1 \pmod{N} \wedge 0 \leq s' < N$$

Αν

$$s' > 0 \wedge w^{2^{s'-1} \cdot r} \not\equiv -1 \pmod{N} \tag{4}$$

τότε το $u \equiv w^{2^{s'-1} \cdot r} \pmod{N}$ είναι μία μη τετριμμένη τετραγωνική ρίζα του $1 \pmod{N}$ και άρα το N παραγοντοποιείται με τον τρόπο που δείξαμε στην πρόταση 1.1.
Θα δείξουμε τώρα ότι ο αλγόριθμος επιτυγχάνει με πιθανότητα $\geq \frac{1}{2}$.

Έστω ότι η σχέση (4) δεν ικανοποιείται, δηλαδή:

$$w^r \equiv 1 \pmod{N} \vee w^{2^t \cdot r} \equiv -1 \pmod{N}, 0 \leq t < s \tag{5}$$

Θα προσδιορίσουμε ένα άνω όριο για τα w που δεν ικανοποιούν την (4) και άρα προφανώς ικανοποιούν την (5). Τα w αυτά θα είναι αριθμοί που έχουν προκύψει από μία σειρά $w^r, w^{2 \cdot r}, w^{2^2 \cdot r}, \cdots, w^{2^i \cdot r}, w^{2^{s'} \cdot r}$ της μορφής:

$$\left.\begin{aligned} <\neq \pm 1, \neq \pm 1, \cdots, -1, 1, \cdots, 1 > \\ < 1, 1, 1 \cdots, 1, 1 > \end{aligned}\right\} \textbf{Non Factoring Sequences}$$

Έχουμε ότι:

$$p - 1 = 2^i \cdot a \wedge q - 1 = 2^j \cdot b \wedge a, b\ odds$$

Και επιπλέον υποθέτουμε ότι $i \leq j$ χωρίς βλάβη της γενικότητας. Συνεπώς:

$$\begin{aligned} & e \cdot d \equiv 1 \pmod{\phi(n)} \\ \Rightarrow & 2^s \cdot r \equiv 0 \pmod{\phi(N)} \\ \Rightarrow & 2^s \cdot r \equiv 0 \pmod{(p-1) \cdot (q-1)} \\ \Rightarrow & 2^s \cdot r = k \cdot 2^{i+j} \cdot a \cdot b, k \in \mathbb{N} \\ \Rightarrow & a \cdot b | r \end{aligned}$$

Το παραπάνω ισχύει επειδή τα r, a, b είναι περιττοί. Με βάση το παραπάνω, έστω ότι $t \geq i$ τότε το $2^t \cdot r$ είναι πολλαπλάσιο του $p-1 = 2^i \cdot a$ και άρα μπορούμε να γράψουμε

$$\begin{aligned} 2^t \cdot r &\equiv 0 \pmod{p-1} \\ \Rightarrow w^{2^t \cdot r} &\equiv 1 \pmod{p} \\ \Rightarrow w^{2^t \cdot r} &\not\equiv 1 \pmod{p} \\ \Rightarrow w^{2^t \cdot r} &\not\equiv 1 \pmod{N} \end{aligned}$$

Άρα με βάση την υπόθεση μας ότι $t \geq i$ οι συνθήκες της (5) δεν ικανοποιούνται ποτέ άρα αφού $i < s$ μπορούμε να γράψουμε την (5) στη μορφή :

$$w^r \equiv 1 \pmod{N} \vee w^{2^t \cdot r} \equiv -1 \pmod{N}, 0 \leq t < i \tag{6}$$

Θα κάνουμε τώρα μία εκτίμηση για τον αριθμό των w που ικανοποιούν την (6). Έστω g ένας γεννήτορας του $\mathbb{Z}_p^*$ και έστω επίσης $w \equiv g^u \pmod{p}$. Τότε έχουμε:

$$w^r \equiv 1 \pmod{p} \Leftrightarrow u \cdot r \equiv 0 \pmod{p-1}$$

Οι δύο παραπάνω ισοτιμίες είναι ισοδύναμες και άρα έχουν το ίδιο πλήθος λύσεων ως προς τα u, w. Το πλήθος των λύσεων της τελευταίας ισοτιμίας είναι ίσο με $gcd(r, p-1) = a$. Με ανάλογο τρόπο προκύπτει και ο αριθμός των λύσεων της ισοτιμίας $w^r \equiv 1 \pmod{q}$ ο οποίος είναι b. Συνεπώς η ισοτιμία $w^r \equiv 1 \pmod{}$ έχει $a \cdot b$ λύσεις.
Το πλήθος των λύσεων της ισοτιμίας $w^{2^t \cdot r} \equiv -1 \pmod{N}$ μπορεί να βρεθεί με βάση την εξής παρατήρηση:

$$w^{2^{t+1} \cdot r} \equiv 1 \pmod{p}$$

Η παραπάνω ισοτιμία για $t+1 \leq i$ έχει $gcd(2^{t+1} \cdot r, p-1) = 2^{t+1} \cdot a$ λύσεις. Αντίστοιχα παρατηρούμε ότι:

$$w^{2^t \cdot r} \equiv 1 \pmod{p}$$

Η παραπάνω ισοτιμία έχει $gcd(2^t \cdot r, p-1) = 2^t \cdot a$ λύσεις. Με βάση τα παραπάνω και τη σχέση (1) της πρότασης 1.1 συμπεραίνουμε ότι το πλήθος των λύσεων της ισοτιμίας

$$w^{2^t \cdot r} \equiv -1 \pmod{p}$$

είναι το πολύ $2^{t+1} \cdot a - 2^t \cdot a = 2^t \cdot a$. Με ανάλογο τρόπο προκύπτει ότι το πλήθος των λύσεων της ισοτιμίας

$$w^{2^t \cdot r} \equiv -1 \pmod{q}$$

είναι το πολύ $2^t \cdot b$. Συνεπώς το πλήθος των λύσεων για την ισοτιμία

$$w^{2^t \cdot r} \equiv -1 \pmod{N}$$

είναι το πολύ $2^t \cdot a \cdot 2^t \cdot b = 2^{2 \cdot t} \cdot a \cdot b$ πάλι από τη σχέση (1) της πρότασης 1.1. Συνεπώς το άνω όριο για το πλήθος των w που δε ικανοποιούν τη σχέση (5) (και άρα και την (6)), δηλαδή το άνω όριο για το πλήθος των w που δε μπορούμε να χρησιμοποιήσουμε για να παραγοντοποιήσουμε το N μπορεί να βρεθεί ως άθροισμα για όλες τις πιθανές τιμές του πλήθους των λύσεων των δύο ισοτιμιών της συνθήκης (5).

$$a \cdot b + a \cdot b \cdot \sum_{t=0}^{i-1} 2^{2t}$$

Το παραπάνω άθροισμα προκύπτει ίσο με $\frac{\phi(N)}{2}$. Το πλήθος των w είναι $\phi(N)$ αφού $gcd(w, N) = 1$ άρα το πολύ τα μισά απο όλα τα δυνατά w δε μπορούν να χρησιμοποιηθούν για να παραγοντοποιήσουμε το N. Άρα μέτα k τυχαίες επιλογές υπάρχει πιθανότητα $\frac{1}{2^k}$ να μη βρούμε κατάλληλο w. □

2 Primality Testing

2.1 Fermat Test

Το *Fermat test* στηρίζεται στο μικρό θεώρημα του Fermat.

Θεώρημα. Μικρό Θεώρημα Fermat

$$\forall a \in \mathbb{Z},\ \forall\ prime\ p \not| a :\ a^{p-1} \equiv 1 \pmod{p}$$

Απόδειξη. Zac12 σελ. 151, Θεώρημα 6.41 □

Θα θέλαμε εξετάζοντας τη συνθήκη για διάφορες τιμές του a να αποφανθούμε με κάποια πιθανότητα για το αν ο n είναι πρώτος. Αυτό ωστόσο είναι αδύνατο καθώς ανακαλύφθηκαν οι αριθμοί Carmichael. Οι αριθμοί Carmichael είναι σύνθετοι αριθμοί n που ικανοποιούν την ισοτιμία για όλα τα a για τα οποία ισχύει $gcd(a, n) = 1$ οπότε το παραπάνω test θα ισχυρίζεται ότι κάποιος τέτοιος αριθμός είναι πρώτος ενώ είναι σύνθετος.

2.2 Euler Test

Το *Euler test* είναι πιο ισχυρό από το *Fermat test* υπό την έννοια ότι μπορεί να βρεί κάποιους σύνθετους αριθμούς τους οποιούς το *Fermat test* αποτυγχάνει να βρεί.

Πρόταση 2.1. *Αν για κάποιο a ισχύει ότι $a \not\equiv 0 \pmod{n} \ \wedge\ a^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$ τότε ο n είναι σύνθετος.*

Μία τέτοια ισοτιμία έχει τουλάχιστον 4 ρίζες modulo n. Οι 2 ρίζες θα είναι οι τετριμμένες $\pm 1 \pmod{n}$ και έστω δύο άλλες ρίζες $u \neq \pm 1$. Έτσι θα ισχύει η

ισοτιμία $a^{n-1} \equiv 1 \pmod{n}$ αλλά θα πρόκειται για σύνθετο αριθμό. Σε αυτή την περίπτωση το *Fermat Test* θα αποτύχει ενώ το *Euler Test* θα πετύχει.

2.3 Miller-Rabin Test

Με βάση τα παραπάνω αν ισχύει ότι $a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n} \ \wedge \ gcd(a, n) = 1$ τότε ο n είναι σύνθετος και διακρίνουμε τις εξής περίπτωσεις:

- $a^{n-1} \not\equiv 1 \pmod{n}$ οπότε ο n είναι σύνθετος με βάση το *Fermat Test*.
- $a^{n-1} \equiv 1 \pmod{n} \ \wedge \ a^{\frac{n-1}{2}} \equiv \pm u \pmod{n} \ \wedge \ u \neq \pm 1$ οπότε ο n είναι σύνθετος με βάση το *Euler Test*.

Το *Miller-Rabin Test* εξετάζει αν ο τυχαίος αριθμός που επιλέξαμε οδηγεί σε **FACTORING-SEQUENCE** έτσι ώστε να εντοπίσει σύνθετους αριθμούς που το *Fermat Test* θεωρεί πρώτους. Αρκεί λοιπόν να χρησιμοποιήσουμε κατάλληλα το *Euler Test* ώστε να εξετάσουμε και τις μη τετριμμένες τετραγωνικές ρίζες του 1.

Αλγόριθμος Miller-Rabin

1. Έστω ο n ένας θετικός περιττός αριθμός. Γράφουμε $n - 1 = 2^s \cdot t$, με t περιττό.

2. Επιλέγουμε τυχαίο $0 < b < n$ και υπολογίζουμε το $b^t \pmod{n}$.

3. Αν $b^t \equiv \pm 1 \pmod{n}$ τότε το n είναι πρώτος.
Αυτό συμβαίνει επειδή το $b^{n-1} \equiv (b^t)^{2^s} \equiv 1 \pmod{n}$ και άρα δεν υπάρχουν άλλες τετραγωνικές ρίζες του 1 πέρα απο τις τετριμμένες.

4. Αλλιώς υπολογίζουμε το $b^{2^i \cdot t} \pmod{n}$ για $i = 1$.

5. Αν $b^{2^i \cdot t} \equiv 1 \pmod{n}$ τότε το n είναι σύνθετος.
Αυτό συμβαίνει επειδή το $b^{2^{i-1}} \cdot t \equiv u \pmod{n} \ \wedge \ u \neq \pm 1$ είναι τετραγωνική ρίζα του $b^{2^i \cdot t} \equiv 1 \pmod{n}$ και άρα αυτή η ισοτιμία έχει παραπάνω από 2 λύσεις συνεπώς το n δεν είναι πρώτος.

6. Αν $b^{2^i \cdot t} \equiv -1 \pmod{n}$ τότε το n είναι πρώτος.
Προκύπτει όπως στο **3**.

7. Αλλιώς συνεχίζουμε απο το βήμα **5** αυξάνοντας το i κατά 1. Αν δεν έχουμε αποφανθεί μέχρι $i = s - 1$ και $b^{2^{s-1} \cdot t} \not\equiv \pm 1 \pmod{n}$ τότε ο n είναι σύνθετος.

3 Παραγοντοποίηση

Η παραγοντοποίηση αναφέρεται στην εύρεση κάποιου αριθμού p για τον οποίο ισχύει $p \mid n \ \wedge \ 1 < p < n$. Χρησιμοποιώντας τα test που δείξαμε παραπάνω μπορούμε να εξακριβώσουμε αν ένας αριθμός έχει κάποιον διαιρέτη, έστω d. Θα δείξουμε μία μέθοδο για να βρούμε το d.

3.1 Μέθοδος ρ

Πάραγουμε μία τυχαία ακολουθία $< x_0, x_1, \cdots >$ με $x_i \in \mathbb{Z}_n$. Αυτό μπορεί να γίνει με χρήση ενός πολυωνύμου βαθμού μεγαλύτερου του 1 όπως το $f(x) = x^2+1$ και μία αρχική τιμή έστω $x_0 = 1$.

Συνθήκη 3.1. $k > j \ \wedge \ x_j \not\equiv x_k \pmod{n} \ \wedge \ gcd(x_k - x_j, n) > 1$

Αναζητούμε ένα ζευγάρι j, k που να ικανοποιεί τη συνθήκη 3.1. Ισοδύναμα αν βρούμε $x_k \equiv x_j \pmod{d}$ για κάποιο $d \mid n$ τότε παίρνουμε $gcd(x_k - x_j, n) > 1$. Αποδεικνύεται οτι μπορούμε να βρούμε ένα τέτοιο ζευγάρι μετά απο $\mathcal{O}(\sqrt{p}) = \mathcal{O}(\sqrt[4]{n})$ δοκιμές.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

Sti06 : D. Stinson: Cryptography: Theory and Practice, 3rd edition, CRC Press, 2005.