Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ανδρεας Μαντης

Διδάσκοντες:
Σταθης Ζαχος
Αρης Παγουρτζης

12 Δεκεμβρίου 2011

1 RSA και παραγοντοποίηση

Θεώρημα. *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. Μια μέθοδος παραγοντοποίησης για $n = pq$ επιτυγχάνεται βρίσκοντας τις λύσεις x, y όταν $x^2 \equiv y^2 \pmod{n}$ και $x \not\equiv \pm y \pmod{n}$. Από την πρώτη ισοτιμία συμπεραίνουμε ότι $n|(x-y)(x+y)$. Έτσι, εφόσον ισχύει και $x \not\equiv \pm y \pmod{n}$, ξέρουμε πως ένα από τα $gcd(n, x-y), gcd(n, x+y)$ είναι το p και το άλλο το q.

Ειδική περίπτωση αυτού είναι να θεωρήσουμε πως το $y = 1$ και έτσι οι παραπάνω ισοτιμίες γίνονται $x^2 \equiv 1 \pmod{n}$ και $x \not\equiv \pm 1 \pmod{n}$. Το x σε αυτήν την περίπτωση λέγεται μη τετριμμένη ρίζα της μονάδας και η εύρεση αυτής οδηγεί στην παραγοντοποίηση του n όπως πιο πάνω.

Το ζήτημα γενικά είναι να μπορούμε να βρούμε με πιθανοτικό αλγόριθμο τέτοιες ισοτιμίες $\pmod{n}$ έχοντας βρει ήδη με κάποιο τρόπο το d.

Από τον ορισμό του RSA έχουμε $ed \equiv 1 \pmod{\phi(n)} \Rightarrow ed - 1 = k\phi(n)$. Έτσι, από τις σημειώσεις [Zac07, σελ.156 Πόρισμα 6.43] μπορούμε να συμπεράνουμε ότι $a^{ed-1} \equiv 1 \pmod{n}$ για κάθε $a \in Z_n^*$. Αν $a \notin Z_n^*$ τότε $a|n$ και έχουμε αμέσως την παραγοντοποίηση. Χωρίς βλάβη της γενικότητας λοιπόν υποθέτουμε πως $a \in Z_n^*$.

Αφού $\phi(n) = (p-1)(q-1)$ τότε $2|ed-1$ και $4|ed-1$. Έτσι, διαιρώντας το $ed-1$ συνεχώς με το 2, αν βρούμε πιθανές μη τετριμένες ρίζες της μονάδας της μορφής $a^{\frac{ed-1}{2^i}}$ θα παραγοντοποιήσουμε το n όπως πιο πάνω.

Ένας πιο αποδοτικός τρόπος να υλοποιηθεί αυτός ο έλεγχος, και ταυτόχρονα να αποδειχθεί η ορθότητά του, είναι μέσω των a-sequences. Γράφοντας το $ed - 1 = 2^s r$, όπου r περιττός, υπολογίζουμε την ακολουθία a-sequence $< a^r, a^{2r}, ..., a^{2^i r}, ..., a^{2^s r} \equiv 1 \pmod{n} >$, όπου όλες οι τιμές είναι $\pmod{n}$. Μια a-sequence είναι factoring sequence -δηλαδή οδηγεί σε παραγοντοποίηση- έαν $\exists i < s, a^{2^i r} \not\equiv \pm 1 \pmod{n}, a^{2^{i+1} r} \equiv 1 \pmod{n}$.

Για κάθε a δημιουργούμε μία a-sequence. Θα δείξουμε τώρα πως μία a-sequence έχει περισσότερο από 0.5 πιθανότητα να είναι factoring sequence και έτσι μπορούμε να έχουμε πιθανοτικό αλγόριθμο για την παραγοντοποίηση του n. Αρκεί να δείξουμε πως το σύνολο των a που οδήγουν σε non factoring sequences -ή ακόμα καλύτερα ένα γενικότερο σύνολο B- έχει λιγότερα από τα μισά στοιχεία του Z_n^*.

Μία non factoring sequence έχει μία εκ των δύο ακόλουθων μορφών:

$< 1, 1, 1, ..., 1 >$

$<\not\equiv \pm 1, \not\equiv \pm 1, \not\equiv \pm 1, ..., -1, 1, 1, ..., 1 >$.

Έστω a_0 τέτοιο ώστε $a_0^{2^j r} \equiv -1 \pmod{n}$, j max, και για κάθε $a \not\equiv a_0 \pmod{n}$ τέτοιο ώστε α-sequence είναι non factoring και ισχύει $a^{2^{j+1}r} \equiv 1 \pmod{n}$

Σταθεροποιώντας το j ορίζουμε το B ως το σύνολο που έχει στη θέση j 1 ή -1. Το B είναι υπερσύνολο των non factoring sequences γιατί υπάρχουν και factoring sequences που έχουν στη θέση j 1 ή -1. Δηλαδή:

$B = \{a \in Z_n^* | a^{2^j r} \equiv \pm 1 \pmod{n}\} \supseteq \{a \in Z_n^* | \text{α-sequence not factoring}\}$

Παρατηρήσεις

1. Το B είναι κλειστό ως προς τον πολλαπλασιασμό modulo. Πράγματι $(a \cdot a')^{2^j r} \equiv \pm 1 \cdot \pm 1 \equiv \pm 1 \pmod{n}$

2. Υπάρχει $a_* \in Z_n^* \setminus B$ Πράγματι, από CRT υπάρχει $a_* \in Z_n^*$ που είναι λύση του συστήματος

$$(a_*)^{2^j r} \equiv 1 \pmod{p} \Leftarrow a_* \equiv 1 \pmod{p}$$

$$(a_*)^{2^j r} \equiv -1 \pmod{q} \Leftarrow a_* \equiv a_0 \pmod{q}$$

Επομένως $(a_*)^{2^j r} \not\equiv \pm 1 \pmod{n}$, γιατί διαφορετικά θα έπρεπε να έχει την ίδια ισοτιμία (1 ή -1) και modulo p και modulo q και έτσι $a_* \notin B$ που υποδεικνύει ότι $a_* \in Z_n^* \setminus B$.

Σύμφωνα με τις πιο πάνω παρατηρήσεις και το θεώρημα του Langrange, [Zac07 σελ.151 Θεώρημα 6.30], ισχύει ότι το $|B|$ διαιρεί το $|Z_n^*| = \phi(n) \Rightarrow |B| \leq \frac{\phi(n)}{2}$

$$Prob_{a \in Z_n^*}[a \; gives \; factoring \; sequence] \geq \frac{1}{2}$$

Οπότε, με κ επαναλήψεις του αλγορίθμου μπορούμε να επιτύχουμε ακόμα καλύτερη πιθανότητα επιτυχίας

$$Prob_{a \in Z_n^*}[a \; gives \; factoring \; sequence] \geq 1 - \frac{1}{2^k}$$

□

2 Primality Test

Fermat Test

Το τεστ του Fermat βασίζεται στο μικρό Θεώρημα του Fermat [Zac07 σελ.155 Θεώρημα 6.41] που αν n πρώτος ξέρουμε ότι ισχύει

$$\forall a \in Z_n : a^{n-1} \equiv 1 \pmod{n}$$

Αντίστροφα αν $a^{n-1} \not\equiv 1 \pmod{n}$, τότε n είναι σύνθετος.

Algorithm 1 Fermat Test Algorithm

```
1: for i=1 to k do
2:    Choose a ∈ Z_n uniformly at random
3:    if a^{n-1} mod n ≠ 1 then
4:       return COMPOSITE
5:    end if
6: end for
7: return PRIME
```

Για να έχουμε πιθανοτικό αλγόριθμο θα πρέπει για κάθε a που δοκιμάζουμε να έχουμε πιθανότητα μεγαλύτερη από το μισό να πετύχουμε σωστή απάντηση. Παρόλα αυτά οι αριθμοί Carmichael είναι αριθμοί που είναι σύνθετοι και θεωρούνται πρώτοι από το τεστ του Fermat. Έτσι, δε μπορούμε χρησιμοποιήσουμε τον πιο πάνω αλγόριθμο ως πιθανοτικό αλγόριθμο για primality test.

Miller-Rabin Test

Το Miller-Rabin test είναι μία βελτίωση του Fermat test που αντιμετωπίζει ικανοποιητικά τους αριθμούς carmichael. Η διαφορά είναι πως τώρα ελέγχουμε και αν ο τυχαίως επιλεγμένος αριθμός οδηγεί σε factoring sequence και κατ΄ επέκταση στο συμπέρασμα ότι το n είναι σύνθετος. Η απόδειξη ορθότητας του αλγορίθμου χρησιμοποιεί α-sequences όπως πριν με τη διαφορά ότι

$$(a_*)^{2^j r} \equiv 1 \pmod{n_1} \Leftarrow a_* \equiv 1 \pmod{n_1}$$

$$(a_*)^{2^j r} \equiv -1 \pmod{n_2} \Leftarrow a_* \equiv a_0 \pmod{n_2}$$

όπου n_1, n_2 πρώτοι μεταξύ τους, ώστε να μπορούμε να εφαρμόσουμε CRT.

Algorithm 2 Miller-Rabin Test Algorithm

1: Choose $a \in Z_n$ *uniformly at random*
2: **if** $gcd(a, n) \geq 1$ **then**
3: **return** COMPOSITE
4: **end if**
5: $(b_{k-1}, b_k, ..., b_1, b_0) \leftarrow$ *binary representation of* $n - 1$
6: $t \leftarrow 1$
7: $i \leftarrow k - 1$
8: **while** $i \geq 0$ **do**
9: $m \leftarrow t$
10: $t \leftarrow t^2 \ \underline{mod}\ n$
11: **if** $t = 1$ *and* $m \neq \pm 1$ **then**
12: **return** COMPOSITE
13: **end if**
14: **if** $b_i = 1$ **then**
15: $t \leftarrow at \ \underline{mod}\ n$ $\{t = a^{b_{k-1} \cdots b_i} \ \underline{mod}\ n\}$
16: **end if**
17: $i \leftarrow i - 1$
18: **end while**
19: **if** $t \neq 1$ **then**
20: **return** COMPOSITE
21: **else**
22: **return** PRIME {with prob ≥ 0.5}
23: **end if**

Παράδειγμα 1

$n = 15 \Rightarrow n - 1 = 14 = (1110)_2$ και έστω $a = 7$

i	b_i	a	m	t
3	1	7	1	$1, 7$
2	1		7	$4, 13$
1	1		13	$4, 13$
0	0		13	$\underline{4}$

Έτσι, ο αριθμός είναι composite.

Παράδειγμα 2

$n = 57 \Rightarrow n - 1 = 56 = (111000)_2$ και έστω $a = 11$

i	b_i	a	m	t
5	1	11	1	$1, 11$
4	1		11	$7, 20$
3	1		20	$\underline{1}$

Έτσι, ο αριθμός είναι composite.

Βιβλιογραφία

1. [Zac07]: Σημειώσεις Ζάχου, ΕΜΠ, 2007.