Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Κωνσταντινα Μελλου

Διδάσκοντες:
Σταθης Ζαχος
Αρης Παγουρτζης

16 Δεκεμβρίου 2011

Hard-core predicates (for one-way functions)

Έστω η συνάρτηση $f : \mathcal{M} \to \mathcal{C}$. Τότε η συνάρτηση $B : \mathcal{M} \to \{0,1\}$ λέγεται *hard-core predicate* για την f εάν είναι 'δύσκολο' έχοντας το $f(x)$ να υπολογίσουμε το $B(x)$.

($\forall$ PPT algorithm A, $Pr[A(f(x), r)] \leq \frac{1}{2} + \varepsilon, r$: random string)

Άσκηση

- $parity_N(x) = (x \, mod \, N) \, mod \, 2$
- $$upperhalf_N(x) = \begin{cases} 1 & \text{if } x \, mod \, N > \frac{N}{2}, \\ 0 & \text{otherwise.} \end{cases}$$

Δείξτε ότι για το RSA οι συναρτήσεις αυτές είναι *hard-core predicates*.

Πιο απλά: Δείξτε ότι αν μπορούμε με γνωστό $y = x^e \, mod \, N$ να υπολογίσουμε την $parity_N(x)$ ή την $upperhalf_N(x)$ τότε μπορούμε να βρούμε το x/να σπάσουμε το RSA.

Έστω $N = 35$.

Δοκιμές για διάφορες τιμές του x:

x	9	24	25	6	31
$parity$	1	0	1	0	1
$upperhalf$	0	1	1	0	1

Έστω ότι θέλω να βρω το x, το οποίο έχει την τιμή 27.

Ισχύει $parity(x) = 1 \Rightarrow x =$ ____1

Υποδιπλασιάζω: $parity(13) = 1 \Rightarrow x =$ ___11

Υποδιπλασιάζω: $parity(6) = 0 \Rightarrow x =$ __011 κ.ο.κ.

Αυτή η διαδικασία θα δούλευε καλά στους φυσικούς αριθμούς.

Έχοντας $y = x^e \, mod \, N$ θέλω $y' = (\frac{x}{2})^e \, mod \, N$.
Όμως αν x περιττός το παραπάνω δεν ορίζεται καλά άρα παίρνω: $y' = (2^{-1}x)^e \, mod \, N$.

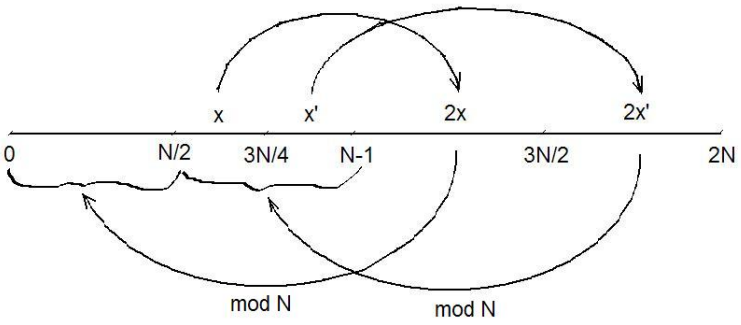
$$y' = (2^{-1}x)^e \, mod \, N = (2^{-1})^e x^e \, mod \, N = (2^{-1})^e y \, mod \, N.$$

Ο προηγούμενος πίνακας ολοκληρωμένος:

x	9	24	25	6	31
$parity$	1	0	1	0	1
$upperhalf$	0	1	1	0	1
$2^{-1}x$	22	12	30	3	33
$2x$	18	13	15	12	27

π.χ.: $25 = (11001)_2$. Παίρνω από $parity(25)$ τον τελευταίο άσο αλλά πως βρίσκω τα άλλα;

Με την $upperhalf : u(x^2 \, mod \, N) = upperhalf_N(x)$ βρίσκουμε σε ποιο τέταρτο ανήκει ο αριθμός.



Αν ο αριθμός $(\forall x \in \mathbb{Z}_N)$ είναι άρτιος: $parity_N(x) = 0 \Leftrightarrow upperhalf_N(2^{-1}x) = 0$.

Αν ο αριθμός $(\forall x \in \mathbb{Z}_N)$ είναι περιττός: $parity_N(x) = 1$, το μισό του είναι στην πραγματικότητα το $\frac{x+N}{2}$, δηλαδή $2^{-1}x \, mod \, N = \frac{x+N}{2}$ (με $\frac{N}{2} < \frac{x+N}{2} < N$) $\Leftrightarrow$ $upperhalf(2^{-1}x) = 1$.

Συμπέρασμα: $parity_N(x) = upperhalf_N(2^{-1}x)$
(αν έχουμε τη μία από τις δύο, υπολογίζουμε την άλλη)

Δηλαδή αν υπάρχουν αυτές οι συναρτήσεις σπάει το RSA $\Rightarrow$ είναι *hard-core predicates*.

$2^{-1} = \frac{N+1}{2}$ (αφού $2\frac{N+1}{2} \equiv 1(mod\, N)$)

$\frac{N+1}{2}x \equiv \frac{N+x}{2}(mod\, N)$

Θεώρημα του Wilson

$(p-1)! \equiv -1\,(mod\, p)$ για p πρώτο
$1 * 2 \cdots (p-2)(p-1) \equiv -1\,(mod\, p) \Leftrightarrow 2 \cdots (p-2) \equiv 1\,(mod\, p)$

Παράδειγμα:

$2 * 3 * 4 * 5 \equiv 1\,(mod\, 7)$
$2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 \equiv 1\,(mod\, 11)$

Ξέρω ότι ο αντίστροφος κάθε αριθμού είναι μοναδικός. Αρκεί να δείξω ότι είναι μέσα σε αυτούς.

$1^{-1} \equiv 1\,(mod\, p)$
$(-1)^{-1} \equiv -1\,(mod\, p)$

Άρα υποχρεωτικά είναι όλοι ζευγαρωμένοι εκεί μέσα (έχουμε $\frac{p-3}{2}$ ζευγάρια, αφού έβγαλα τα 1 και $p-1$).

Κριτήριο Euler

$\forall \alpha \in \mathbb{Z}_p^* \; \exists \beta : \alpha \equiv \beta^2\,(mod\, p) \Leftrightarrow \alpha^{\left(\frac{p-1}{2}\right)} \equiv 1\,(mod\, p)$

i) $\alpha^{\left(\frac{p-1}{2}\right)} \equiv \pm 1\,(mod\, p)$,

επειδή $\alpha^{\left(\frac{p-1}{2}\right)^2} \equiv \alpha^{p-1} \equiv 1\,(mod\, p)$

ii) Αν $\alpha \equiv \beta^2 \Leftrightarrow \alpha^{\left(\frac{p-1}{2}\right)} \equiv \beta^{p-1} \equiv 1\,(mod\, p)$.

iii) Έστω $\nexists \beta : \alpha \equiv \beta^2\,(mod\, p)$

$\forall \kappa \in \mathbb{Z}_p^* \; \exists \lambda$ τ.ω. $\kappa\lambda \equiv \alpha (mod\, p)$

$\lambda \equiv \alpha\kappa^{-1} (mod\, p)$

αν $\kappa \equiv \lambda (mod\, p) \Rightarrow \kappa^2 \equiv \alpha (mod\, p)$, άτοπο άρα $\kappa \neq \lambda (mod\, p)$

$(p-1)! \equiv \alpha^{\left(\frac{p-1}{2}\right)} (mod\, p) \Rightarrow \alpha^{\left(\frac{p-1}{2}\right)} \equiv 1\,(mod\, p)$, από *Θεώρημα Wilson*