

ΜΗΥΠ 416 – ΚΡΥΠΤΟΓΡΑΦΙΑ

Χρήστος Κακλαμάνης
Καθηγητής

Πάυλος Σπυράκης
Καθηγητής

Ιούλιος 2003

Ασκήσεις

1. Σε ένα σύστημα RSA υποκλέπουμε το κρυπτόγραμμα $C = 5347$ που στέλνεται σε παραλήπτη με δημόσιο κλειδί $(e, n) = (5, 16781)$. Ποιος είναι ο ακέραιος M που μεταδίδεται; (Δίνεται ότι $16781 = 97 \cdot 173$)
2. Θεωρήστε την μέθοδο $RSA \pmod N$. Ένας ακέραιος αριθμός $M, 1 \leq M \leq N - 1$, είναι σταθερό σημείο, αν η κρυπτογράφηση του δίνει τον εαυτό του. Αποδείξτε ότι αν το M είναι σταθερό σημείο, τότε και το $N - M$ είναι σταθερό σημείο.
3. Αν το $2^n + 1$ είναι περιττός πρώτος για κάποιον ακέραιο, δείξτε ότι το n είναι δύναμη του 2.
4. Δείξτε ότι ο αριθμός των θετικών ακεραίων μικρότερων του n , των οποίων οι πρώτοι παράγοντες ανήκουν σε ένα δοσμένο σύνολο πρώτων $\{p_1, p_2, \dots, p_m\}$ είναι τουλάχιστον $m^r / r!$ με $r = \lfloor \frac{\log n}{\log p_m} \rfloor$ και $p_1 < p_2 < \dots < p_m$.
5. Υποθέστε ότι οι χρήστες Alice, Bob και Carol έχουν τα δημόσια κλειδιά $(n_A, 3)$, $(n_B, 3)$ και $(n_C, 3)$ αντίστοιχα. Υποθέστε πως στέλνουμε χρησιμοποιώντας το RSA το ίδιο μήνυμα M και στους 3. Δείξτε πώς μπορεί κάποιος που 'ακούει' τα τρία μηνύματα, να βρει ποιο ήταν το μήνυμα M . Προτείνετε μια απλή τροποποίηση που εμποδίζει την υποκλοπή.
6. Έστω (n, e) το δημόσιο κλειδί στο RSA και $RSA_{n,e}(x) = x^e \pmod n$. Υποθέστε ότι υπάρχει αλγόριθμος \mathcal{A} που μπορεί να αντιστρέψει 1% των εισόδων της μορφής $y = x^e \pmod n$.
 - (α') Αποδείξτε ότι για κάθε $a, b \in Z_n^*$ ισχύει ότι $RSA_{n,e}(a) \cdot RSA_{n,e}(b) = RSA_{n,e}(ab)$.
 - (β') Αποδείξτε ότι χρησιμοποιώντας τον αλγόριθμο \mathcal{A} , μπορούμε να αντιστρέψουμε οποιαδήποτε είσοδο με μεγάλη πιθανότητα.
7. Υποθέτουμε πως βλέπουμε την κρυπτογράφηση RSA των μηνυμάτων $m, m + 1, m + 2$, με $e = 3$. Πώς μπορούμε να βρούμε το m σε πολυωνυμικό χρόνο;
8. Έστω $n = p \cdot q$, όπου p, q περιττοί πρώτοι αριθμοί, διαφορετικοί μεταξύ τους. Έστω $\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}$. Υποθέτουμε πως τροποποιούμε το πρωτόκολλο RSA έτσι ώστε $ed = 1 \pmod{\lambda(n)}$.
 - Δείξτε ότι η κρυπτογράφηση και η αποκρυπτογράφηση είναι αντίστροφες συναρτήσεις στο τροποποιημένο πρωτόκολλο.
 - Αν $p = 37, q = 79$ και $d = 7$, υπολογίστε το e του τροποποιημένου πρωτοκόλλου, καθώς και του κανονικού πρωτοκόλλου RSA.

Παράδοση : Τρίτη 8/7, ώρα 15 : 00

Άσκηση 1

Για να βρούμε το αρχικό μήνυμα M από το κρυπτογράφημα C πρέπει να γνωρίζουμε το secret key d .

Γράφουμε το n ως γινόμενο πρώτων αριθμών δηλαδή σε μορφή $n = p \cdot q$ όπου p, q είναι πρώτοι. Γνωρίζουμε ότι ένας εκ των δύο θα είναι μικρότερο του \sqrt{n} εκτός και αν $p = q = \sqrt{n}$

Εδώ $n = 16781 = 97 \cdot 173$ άρα $\sqrt{n} = 129,8884$. Συνεπώς $p = 97, q = 173$

Ισχύει ότι: $\phi(n) = \phi(p) \cdot \phi(q) = (p-1)(q-1) = 16512$

ως γνωστόν $e \cdot d \equiv 1 \pmod{\phi(n)} \Rightarrow e \cdot d = 1 \pmod{16512}$

Το d μπορούμε να το βρούμε είτε με τον αλγόριθμο του Ευκλείδη είτε με διαδοχικές δοκιμές. Εδώ μας συμφέρει ο δεύτερος τρόπος με τις διαδοχικές δοκιμές.

Έτσι $e \cdot d \equiv 1 \pmod{\phi(n)} \Rightarrow 16512 | e \cdot d - 1 \Rightarrow$
 $\Rightarrow ed - 1 = \lambda \cdot 16512, \lambda \in \mathbb{Z}$

Άρα $d = \frac{16512\lambda + 1}{e} \Rightarrow d = \frac{16512\lambda + 1}{5}$

Δοκιμάζουμε διάφορες τιμές του λ και βρίσκουμε αντίστοιχες τιμές για το d .

για $\lambda = 0 \rightarrow d = \frac{1}{5}$ απορρίπτεται

για $\lambda = 1 \rightarrow d = 3302,6$ απορρίπτεται

για $\lambda = 2 \rightarrow d = 6605$ δεκτό

Άρα το μήνυμα είναι: $M = C^d \pmod{n} \Rightarrow M = 5347^{6605} \pmod{16781} = 16657$

Επαλήθευση: το κρυπτογράμμα C του $M=16657$ είναι

$$C = M^e \pmod{n} = 16657^5 \pmod{16791} = 5347$$

Άρα η λύση είναι $M=16657$

Άσκηση 2

Αφού το M είναι σταθερό σημείο έχουμε ότι $M^e = M \pmod{N}$ ①

Για την υφολογρήφηση του $(N-M)^e$ έχουμε $C = (N-M)^e \pmod{N}$

Απο το διανυφματικό ανάπτυγμα έχουμε:

$$(N-M)^e = N^e - \binom{e}{1} N^{e-1} M + \binom{e}{2} N^{e-2} M^2 - \dots + (-1)^{e-1} N M^{e-1} - M^e$$

Αφού δουλεύουμε με modulo N όλοι οι όροι του πιο πάνω ανάπτυγματος που περιέχουν το N εφοφονίζονται και συνεπώς έχουμε

$$C = (N-M)^e \pmod{N} \equiv -M^e \pmod{N}$$

Απο την ① έχουμε $-M^e \equiv -M \pmod{N}$

$$\text{ήρα τελικά} \quad C \equiv -M \pmod{N}$$

Βλέπουμε πως $-M \equiv N-M \pmod{N}$ καθώς ο όρος N είναι μηδέν αφού είναι modulo N ($N \pmod{N} = 0$)

ήρα $C \equiv -M \equiv N-M \pmod{N}$ δηλαδή βλέπουμε ότι:

$$C = (N-M)^e \equiv N-M \pmod{N}$$

Συνεπώς η υφολογρήφηση του $N-M$ είναι το ίδιο το $N-M$ και με άλλα λόγια το $N-M$ είναι επίσης σταθερό σημείο

Άσκηση 3

Γνωρίζουμε ότι αν $0 < k$ είναι περιττός τότε:

$$x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + x^{k-3} - \dots + 1)$$

Διαυρύνουμε τις εφής περιπτώσεις για το n :

- Έστω n περιττός:

Τότε το $x^n + 1$ έχει παράγοντα το $(x+1)$ οπότε το $2^n + 1$ έχει παράγοντα το $(2+1) = 3$. Άρα το $2^n + 1$ διαιρείται (με το 3 πραγματικό διότι $2^n + 1$ είναι πρώτος (από την εκφώνηση)). Άρα το n είναι άρτιος.

- Έστω n άρτιος αλλά όχι δύναμη του 2:

Τότε $n = 2^a \cdot b$ όπου b : περιττός και $a \in \mathbb{N}^*$

Άρα $2^n + 1 = 2^{2^a \cdot b} + 1 = (2^{2^a})^b + 1$ αφού $b =$ περιττός τότε το $(2^{2^a})^b + 1$

αναλύεται σε γινόμενο και έχει ως παράγοντα το $(2^{2^a} + 1)$

Οπότε το $2^n + 1$ διαιρείται με το $2^{2^a} + 1$. Άρα είναι άσολο όμοια διότι το $2^n + 1$ είναι πρώτος (από την εκφώνηση). Άρα ο n είναι δύναμη του 2.

Άσκηση 4

Έστω λ θετικός ακέραιος τέτοιος ώστε:

$$\lambda = p_1^{q_1} \cdot p_2^{q_2} \cdot \dots \cdot p_m^{q_m} \quad \text{όπου } p_i \text{ οι πρώτοι παράγοντες του δοσμένου ευαίστου } \{p_1, p_2, \dots, p_m\}$$

Σκοπός μας να βρούμε το σύνολο των διαφορετικών τιμών του λ .

Έστω ότι $q_1 + q_2 + \dots + q_m = k$

Τότε το λ μπορεί να πάρει m^k διαφορετικές τιμές καθώς η επανάληψη των p_i είναι εαίρετη. Αντάδι κάθε ένας από τους k παράγοντες του λ μπορεί να πάρει m τιμές.

Όμως η σειρά εμφάνισης των k παραγόντων δεν μας ενδιαφέρει οπότε το πλήθος των τιμών που μπορεί να έχει το λ είναι

$$\lambda = \frac{m^k}{k!}$$

Άρα τώρα να φράσουμε τον αριθμό λ ώστε $\lambda < n$. Αυτό γίνεται

Άρα να φράσουμε το μέγιστο λ δηλαδή $\lambda_{\max} < n$

Όμως $\lambda_{\max} = p_m^k$ (δίου $p_1 < p_2 < \dots < p_m$)

Άρα πρέπει $\lambda_{\max} = p_m^k < n \Rightarrow k \log p_m < \log n \Rightarrow$

$$\Rightarrow k < \frac{\log n}{\log p_m}$$

Η μέγιστη τιμή του k είναι ο ακέραιος $\left\lfloor \frac{\log n}{\log p_m} \right\rfloor = r$ άρα το

α παίρνει τιμές μικρότερες ή ίσες του r .

Παρατηρούμε ότι το $\frac{m^k}{k!}$ παίρνει την ελάχιστη τιμή του για μέγιστο k δηλαδή $\frac{m^r}{r!}$

Άρα τελικά ο αριθμός των θετικών ακεραίων μικρότερων του n των οποίων οι πρώτοι παράγοντες ανήκουν στο $\{p_1, p_2, \dots, p_m\}$ είναι $\geq \frac{m^r}{r!}$. Άρα είναι τουλάχιστον $m^r/r!$.

Άσκηση 5

Υποθέτουμε ότι $M < n_A, n_B, n_C$ ώστε να μην χρειάζεται να επιβουβεί το M σε υποβάθια. Το μήνυμα προς τους τρεις αφίερα μπορεί να γραφτεί σαν:

$$M_A = M^3 \pmod{n_A} = M^3 - k_A n_A$$

$$M_B = M^3 \pmod{n_B} = M^3 - k_B n_B$$

$$M_C = M^3 \pmod{n_C} = M^3 - k_C n_C$$

Με τη κριση των δημόσιων κλειδιών και του ΕΥΚΛΕΙΔΕΟΥ Δευρήματος υπολογίζουμε τα εξής:

$$e_A = (n_B n_C)^{-1} \pmod{n_A}$$

$$e_B = (n_A n_C)^{-1} \pmod{n_B}$$

$$e_C = (n_A n_B)^{-1} \pmod{n_C}$$

Τώρα υπολογίζουμε το M' ώστε να μας προσύψει μόνο ο M^3 σαν άγνωστη παράμετρος και συνεπώς έχουμε:

$$M' = M_A e_A n_B n_C + M_B e_B n_A n_C + M_C e_C n_B n_A \Rightarrow$$

$$\Rightarrow M' = M^3 (e_A n_B n_C + e_B n_A n_C + e_C n_A n_B) \pmod{n_A n_B n_C}$$

Τα n_A, n_B, n_C είναι όλα πρώτα από τα δημόσια κλειδιά. Το e_A, e_B, e_C μπορούν εύκολα να υπολογιστούν και συνεπώς υπολογίζεται εύκολα και το $M^3 \pmod{n_A}$. Επίσης εύκολα υπολογίζεται και η αντίστροφη ρίζα του M^3 (αφού $M^3 < n_A$) που είναι το μήνυμα M .

Για να εμποδίσουμε την υποδοχή δηλαδή την απομωσαίωση
των μηνυμάτων θα πρέπει να μπαίνει στο μήνυμα M
ένα string διαφορετικό κάθε φορά που εξάγουμε το μήνυμα M
σε ένα παράτητο. Η προώθηση αυτή πρέπει να γίνεται πριν την α-
πομωσαίωση του μηνύματος. Έτσι τα τρία μηνύματα στην α-
πομωσαίωση τους μορφή δεν είναι ιδιόμορφοι τους και συνεπώς η αν-
ταπόσταση των M_A, M_B, M_C στην εξίσωση δεν είναι δυνατή. Οπότε το
 M^3 δεν μπορεί να βρεθεί.

Άσκηση 6

α') Ξέρουμε ότι $RSA_{n,e}(x) = x^e \pmod{n}$

$$\begin{aligned} & [RSA_{n,e}(a) \cdot RSA_{n,e}(b)] \pmod{n} = \\ & = [a^e \pmod{n}] [b^e \pmod{n}] = \\ & = a^e b^e \pmod{n} = \\ & = [ab \pmod{n}]^e \pmod{n} = \\ & = RSA_{n,e}(ab) \pmod{n} = \\ & = RSA_{n,e}(ab) \end{aligned}$$

β') Αφού ο αλγόριθμος A αντιστρέφει 1% την είσοδο της μορφής $y = x^e \pmod{n}$. Θεωρούμε ότι υπάρχει ένα υποσύνολο $S \subseteq \mathbb{Z}_n^*$ με μέγεθος $|\mathbb{Z}_n^*|/100$ που για οποιαδήποτε τιμή του $y \in S$ ο A την αντιστρέφει ενώ αν $y \notin S$ ο A αποτυγχάνει. Έτσι θέλουμε να δείξουμε ότι χρησιμοποιώντας τον A μπορούμε να αντιστρέψουμε οποιαδήποτε είσοδο με πιθανότητα $\geq 0,99$.

Μια οποιαδήποτε είσοδος ανήκει στο υποσύνολο S με πιθανότητα $p = 0,01$ αφού το μέγεθος του S είναι $|\mathbb{Z}_n^*|/100$. Άρα αν n είναι n είσοδος εκεί πιθανότητα να αντιστραφεί στο A $0,01$ και $0,99$ ο A να αποτύχει. Έτσι για οποιαδήποτε είσοδο μπορούμε μαζώνοντας τον A να την αντιστρέψουμε με πιθανότητα $0,01$. Για να πετύχουμε αντιστροφή της είσοδου με μεγάλη πιθανότητα (περίπου 1) πρέπει να δοκιμάσουμε να αντιστρέψουμε ένα $\frac{100}{0,01} = 10000$ modulo και να μαζέψουμε τον A με είσοδο του νέου $y' = y \cdot r' \pmod{n}$ όπου r' είναι ένας τυχαίος αριθμός που ανήκει στο \mathbb{Z}_n^* . Αν ο A αποτύχει με την αντιστροφή του y' τότε βρίσκουμε το αντίστροφο του y εφαρμόζοντας στο y' το αντίστροφο του r' .

Πρέπει να βρούμε πόσες διαφορετικές r πρέπει να δοθούν
 ώστε για να πετύχουμε αντίστροφο του y' και συνεχώς επιτηρη
 της εισόδου y . Αντίθετα πόσες επαναλήψεις πρέπει να κάνουμε.

Ορίζουμε την τυχαία μεταβλητή X που δίνει την πιθανότητα
 αντίστροφης της εισόδου στην i -οστή επανάληψη

$$P(X=i) = \left(\frac{99}{100}\right)^{i-1} \left(\frac{1}{100}\right)$$

Η πιθανότητα επιτυχίας μετά από i επαναλήψεις είναι:

$$P(X \leq i) = \sum_{j=1}^i P(X=j) = \sum_{j=1}^i \left(\frac{99}{100}\right)^{j-1} \left(\frac{1}{100}\right) = \left(\frac{1}{100}\right) \sum_{j=0}^{i-1} \left(\frac{99}{100}\right)^j = \frac{\left(\frac{1}{100}\right) \sum_{j=0}^{i-1} \left(\frac{99}{100}\right)^j}{1 - \frac{99}{100}} = 1 - (0,99)^i$$

Θέλουμε λοιπόν η πιθανότητα επιτυχίας να είναι:

$$\begin{aligned} P(X \leq i) &\geq 0,99 \Rightarrow 1 - (0,99)^i \geq 0,99 \Rightarrow \\ &\Rightarrow 0,01 \leq (0,99)^i \Rightarrow i \geq \lceil \log_{0,99} 0,01 \rceil \Rightarrow \\ &\Rightarrow i \geq \lceil 458,27 \rceil \end{aligned}$$

Συγκεκριμένα θέλουμε 459 επαναλήψεις για να πάρουμε με επιτυχία
 99% οπιστραβρεμένη την y' . Μετά από 459 επαναλήψεις θα έχουμε x
 y αφού εφαρμόσουμε αντίστροφο του r' στο y' .

Έτσι για συγκεκριμένη είσοδο y και μήκους συγκεκριμένου αριθμού
 επαναλήψεων μπορούμε να πάρουμε το y' με πιθανότητα 99%.

Ακολουθεί ο αλγόριθμος των πράξεων:

function success $\{$

 for ($i=0; 459$) do

$r \in \mathbb{Z}^n$ (το r είναι τυχαίο στον χώρο \mathbb{Z}^n)

$y' = y \cdot r \pmod{n}$

$x' = A(y')$

 if $x' \neq \text{failed}$

 return $x = x' \cdot r^{-1}$

 return failed $\}$

Άσκηση 7

Η υποπερίπτωση RSA των τριών προηγουμένων είναι:

$$K_0 = m^3 \pmod{n}$$

$$K_1 = (m+1)^3 \pmod{n}$$

$$K_2 = (m+2)^3 \pmod{n}$$

Αναπτύσσοντας τα τρία πάνω έχουμε:

$$K_0 = m^3 \pmod{n}$$

$$K_1 = m^3 + 3m^2 + 3m + 1 \pmod{n}$$

$$K_2 = m^3 + 6m^2 + 12m + 8 \pmod{n}$$

Θέλουμε να βρούμε ένα τρόπο υπολογισμού του m σε πολωνομικό χρόνο. Έτσι έχουμε:

$$\begin{aligned} L &= K_2 + K_0 - 2K_1 = m^3 + 6m^2 + 12m + 8 + m^3 - 2m^3 - 6m^2 - 6m - 2 = \\ &= (6m + 6) \pmod{n} = 6(m+1) \pmod{n} \end{aligned}$$

$$\text{υπάρχει για } x = m+1 \text{ έχω } L = 6x \pmod{n}$$

Άρα ο συνδυασμός $L = K_2 + K_0 - 2K_1$ που είναι γνωστή τιμή είναι ίσο με $6(m+1) \pmod{n} = 6x \pmod{n}$ για $x = m+1$ το οποίο x υπολογίζω σε πολωνομικό χρόνο και συνεπώς σε πολωνομικό χρόνο να υπολογίσουμε το m .

Άσκηση 9

Πρέπει να δείξουμε ότι $P(S(M)) = S(P(M)) \Rightarrow M^{ed} = M \pmod{n}$

Γνωρίζουμε ότι: $ed = 1 + k \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} \pmod{p}$, $k \in \mathbb{Z}$

$$M^{ed} = M (M^{(p-1)})^k \frac{q-1}{\gcd(p-1, q-1)} = M \pmod{p}$$

Όμοια $M^{ed} = M \pmod{q}$

$$\text{Άρα } M^{ed} = M \pmod{pq} = M \pmod{n}$$

$$\kappa) n = p \cdot q = 37 \cdot 79 = 2923$$

$$\lambda(n) = \frac{36 \cdot 78}{\gcd(36, 78)} = \frac{2808}{6} = 468 \quad \text{Άρα } 7 \cdot \kappa = 1 \pmod{468}$$

d	$\lambda(n)$	$\lfloor d/\lambda(n) \rfloor$	$\gcd(d, \lambda(n))$	x	y
7	468	0	1	67	-1
468	7	66	1	-1	67
7	6	1	1	1	-1
6	1	6	1	0	1
1	0	-	1	1	0

$$\text{Επιπλέον } 7 \cdot 67 - 468 \cdot 1 = 1$$

$$\gcd(67, 468) = 1$$

$$\text{Άρα } e = 67$$

e) $n = 2923$

$$\phi(n) = (p-1)(q-1) = 2808$$

Apa $f \cdot e = 1 \pmod{2808}$

d	$\phi(n)$	$\lfloor d/\phi(n) \rfloor$	$\text{gcd}(d, \phi(n))$	x	y
7	2808	0	7	-401	1
2808	7	401	1	1	-401
7	1	7	1	0	1
1	0	-	1	1	0

Final answer $(-401)7 + 2808 = 1$

Apa $e = -401 \pmod{2808} = (2808 - 401) \pmod{2808} = 2407$