

ΜΗΥΠ 416 – ΚΡΥΠΤΟΓΡΑΦΙΑ

Χρήστος Κακλαμάνης
Καθηγητής

Πάυλος Σπυράκης
Καθηγητής

Ιούνιος 2006

Ασκήσεις

Στις παρακάτω ασκήσεις, το $\alpha\mu_x$ αναφέρεται στο υπόλοιπο της διαίρεσης του αριθμού μητρώου σας με τον αριθμό x .

- (10%) Σε ένα σύστημα RSA υποκλέπουμε το κρυπτογραφημένο μήνυμα $C = (3 + \alpha\mu_{10})$ που στέλνεται σε παραλήπτη με δημόσιο κλειδί $(e, n) = (3 + 2\alpha\mu_5, 7897)$. Ποιος είναι ο ακέραιος M που μεταδίδεται; Παρουσιάστε αναλυτικά τον τρόπο με τον οποίο καταλήγετε στο αποτέλεσμα. Δίνεται ότι $7897 = 53 \cdot 149$.
- (20%) Θεωρήστε ότι χρησιμοποιούμε το πρωτόκολλο RSA και έστω ότι το δημόσιο κλειδί χρησιμοποιεί τον σύνθετο αριθμό 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.
- (15%) 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 3% των εισόδων της μορφής $y = x^e \pmod{n}$.
 - Αποδείξτε ότι για κάθε $a, b \in \mathbb{Z}_n^*$ ισχύει ότι $RSA_{n,e}(a) \cdot RSA_{n,e}(b) = RSA_{n,e}(ab)$.
 - Αποδείξτε ότι χρησιμοποιώντας τον αλγόριθμο \mathcal{A} , μπορούμε να αντιστρέψουμε οποιαδήποτε είσοδο με μεγάλη πιθανότητα.
- (10%) 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 $p = 37, q = 53$ και $d = 7 + 4\alpha\mu_5$, υπολογίστε το e του τροποποιημένου πρωτοκόλλου, καθώς και του κανονικού πρωτοκόλλου RSA.
- (15%) Έστω ότι δουλεύουμε σε RSA και η Alice έχει δημόσιο κλειδί $(n, e) = (851, 7)$. Έστω $m_1 = 80 + \alpha\mu_{10}, m_2 = 155 + \alpha\mu_{15}$, και υποθέτουμε ότι έχουμε την υπογραφή της Alice στο μήνυμα m_1 την συμβολίζουμε με $\text{sig}(m_1)$. Θέλουμε να βρούμε την υπογραφή της στο μήνυμα m_2 (την $\text{sig}(m_2)$ δηλαδή). Έχουμε δικαίωμα να της δώσουμε

ένα μήνυμα x , $x \neq m_2$ και να μας το υπογράψει. Δεν μπορούμε να χρησιμοποιήσουμε την παραγοντοποίηση του 851, ούτε από το $e = 7$ να βρούμε το d . Ποιο μήνυμα θα πρέπει να της δώσουμε;

6. (20%) Έστω ότι χρησιμοποιούμε το πρωτόκολλο του Rabin και έχουμε επιλέξει $p = 23$, $q = 47$ και $B = 10 + 10\alpha_{m_{10}}$. Αν θέλουμε να μεταδώσουμε το μήνυμα $M = 100$, ποιο θα είναι το κρυπτογραφημένο μήνυμα C ; Επίσης, ποια είναι τα μηνύματα στα οποία θα καταλήξει ο παραλήπτης αποκρυπτογραφώντας το C ;
7. (10%) Δύο χρήστες A και B χρησιμοποιούν το πρωτόκολλο RSA και διαλέγουν δημόσια κλειδιά $P_A = (n, e_1)$ και $P_B = (n, e_2)$, όπου $\text{gcd}(e_1, e_2) = 1$. Ο χρήστης C στέλνει το ίδιο μήνυμα x στους A , B , οπότε ένας τέταρτος χρήστης, ο D , υποκλέπτει τα μεταδιδόμενα μηνύματα $y = x^{e_1} \pmod n$ και $z = x^{e_2} \pmod n$. Ακολούθως, ο D υπολογίζει τα $c_1 = e_1^{-1} \pmod e_2$ και $c_2 = (c_1 e_1 - 1)/e_2$ και τελικά υπολογίζει το $y^{c_1} (z^{c_2})^{-1} \pmod n$. Ποιο είναι το τελικό μήνυμα που υπολόγισε ο D ;

Παράδοση : Τετάρτη, 27/06/2007 ώρα 20:00