

## Εργασία 2

Κωσταντίνος Σαΐτας - Ζαρκιάς - 2406  
Οδυσσεύς Κρυσταλάκος - 2362

1 Μαΐου 2016

### Θέμα 1

(vi)

Υπάρχουν 4 τύποι επιθέσεων στις ψηφιακές υπογραφές:

- Existential forgery: Ο επιτηθέμενος μπορεί να παράξει υπογραφεί για κάποιο μήνυμα  $m$  στο οποίο δεν έχει καμία επιρροή. Αυτό σημαίνει ότι ο επιτηθέμενος δεν διαλέγει το  $m$  και το μήνυμα δεν είναι απαραίτητο να έχει κάποιο νόημα.
- Selective forgery: Ο επιτηθέμενος επιλέγει ένα μήνυμα  $m$  και στην συνέχεια μπορεί να παράξει υπογραφή για αυτό το συγκεκριμένο  $m$ .
- Universal forgery: Ο επιτηθέμενος μπορεί να παράξει ψηφιακή υπογραφή για οποιοδήποτε μήνυμα  $m$
- Total break: Ο επιτηθέμενος αποκτά πρόσβαση στο ιδιωτικό κλειδί.

(vii)

Με  $p$  και  $q$  γνωστά μπορούμε να υπολογίσουμε το  $N$  και  $\phi(N)$ .

$$N = p \cdot q = 463 \cdot 547 = 253261$$

$$\phi(N) = (p - 1) \cdot (q - 1) = 462 \cdot 546 = 252252$$

επομένως το  $d$  υπολογίζεται:

$$ed \equiv 1(\text{mod} \phi(N)) \Leftrightarrow d = 27473$$

Τελικά για την αποκρυπτογράφηση του  $c$  αρκεί να υπολογισθεί

$$c^d(\text{mod} N) = 12584$$

(vii)

Ο λόγος που χρησιμοποιείται μία συνάρτηση κατακερματισμού πριν την υπογραφή του μηνύματος είναι η αποφυγή existential forgeries. Για παραδειγμα, έστω το δημόσιο κλειδί  $(y, N)$ . Κάποιος θα μπορούσε να παράξει μία τυχαία υπογραφή, έστω  $s$ . Αυτή η υπογραφή αντιστοιχεί στο μήνυμα  $m = s^y$  και περνά τον έλεγχο. Επομένως ο επιτηθέμενος κατάφερε να υπογράψει ένα τυχαίο μήνυμα  $m$  δηλαδή κατάφερε existential forgery. Για να αποφευχθεί αυτό το πρόβλημα, το μήνυμα περνούν από μία hash  $H$ . Έτσι είναι δύσκολο να επιλεγεί  $s$  ώστε  $H(m) = s^y$ .

(ix)

Έστω ότι έχουμε σύστημα ψηφιακής υπογραφής με τα εξής στοιχεία:

$H$ : Συνάρτηση κατακερματισμού

$p$ : Μεγάλος πρώτος ακέραιος

$g$ : Τυχαίος generator στην κυκλική ομάδα  $Z_p^*$

$x$ : Μυστικό κλειδί  $< p$

$y$ : Δημόσιο κλειδί με  $y = g^x \bmod p$

Έστω πώς η Alice θέλει να υπογράψει ένα μήνυμα  $m$  και να το στείλει στον Bob. Κατά τη διαδικασία της υπογραφής, επιλέγεται ένα τυχαίο  $k$  έτσι ώστε  $1 < k < p - 1$ . Επίσης υπολογίζονται:

$$r \equiv g^k \pmod{p}$$

$$s \equiv k^{-1}(H(m) - xr) \pmod{p - 1}$$

Έτσι στον Bob αποστέλονται τα  $(m, r, s)$ . Φυσικά αυτά μπορεί να τα λάβει και οποιοσδήποτε άλλος παρακολουθεί το κανάλι επικοινωνίας.

Έστω ότι η Alice χρησιμοποιεί δύο φορές το ίδιο  $k$ . Τότε για δύο διαφορετικά μηνύματα  $m_1$  και  $m_2$  ισχύει:

$$s_1 \equiv k^{-1}(H(m_1) - xr) \pmod{p - 1}$$

$$s_2 \equiv k^{-1}(H(m_2) - xr) \pmod{p - 1}$$

εκ των οποίων προκύπτει:

$$k(s_2 - s_1) = H(m_2) - H(m_1)$$

Από αυτή την εξίσωση μπορούν να βρεθούν μία σειρά από  $k$  τα οποία αν αντικατασθούν στην σχέση:

$$r \equiv g^k \pmod{p}$$

μπορεί να βρεθεί η μοναδική σωστή τιμή του  $k$ . Με αντικατάσταση στις παραπάνω σχέσεις, μπορεί να βρεθεί το ιδιωτικό κλειδί.

Τελικά, ο Bob ή οποιοσδήποτε άλλος παρακολουθεί το κανάλι μπορεί να υπογράψει με την υπογραφή της Alice.

(x)

Ισχύει

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = pq - (p+q) + 1$$

και επειδή  $N = pq$

$$\phi(n) = N - (p+q) + 1$$

## Θέμα 2

(i)

Υλοποιώντας και χρησιμοποιώντας τον εκτεταμένο αλγόριθμο του Ευκλείδη για την εύρεση του GCD, βρέθηκε:

$$GCD(126048, 5050) = 202$$

$$-1 \cdot 126048 + 25 \cdot 5050 = 202$$

(ii)

Για τον υπολογισμό του αντίστροφου, υπολογίστηκαν όλα τα γινόμενα  $809 * i$  όπου  $i$  παίρνει τιμές από 1 έως 1000. Βρέθηκε πως ο αντίστροφος είναι το 464.

(iii)

Καθώς το  $2^{100}$  είναι δύσκολο να αποθηκευτεί και να χρησιμοποιηθεί σε πράξεις με ακρίβεια, χρησιμοποιήθηκε μία διαφορετική τεχνική. Υπολογίστηκε το 2 modulo 101 και το αποτέλεσμα πολλαπλασιάστηκε(modulo 101) με το 2. Αυτό έγινε επαναληπτικά 100 φορές και το αποτέλεσμα είναι 464.

(iv)

Ο αλγόριθμος υλοποιήθηκε στο αρχείο fast.py. Τα αποτελέσματα είναι:

$$2^{1234567} \bmod 12345 = 8648$$

$$130^{7654321} \bmod 567 = 319$$

### Θέμα 3

Θέμα 4

Θέμα 5

## Θέμα 6

(i)

$$\begin{aligned}
 \frac{123454}{546542} &= 0 + \frac{1}{4 + \frac{52726}{123454}} \\
 &= 0 + \frac{1}{4 + \frac{1}{2 + \frac{18002}{52726}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{16722}{18002}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1280}{16722}}}}} \\
 &= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{82}{1280}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{50}{82}}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{32}{50}}}}}}}} \\
 &= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{18}{32}}}}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{14}{18}}}}}}}}} \\
 &= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{4}{14}}}}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{2}{3 + \frac{2}{4}}}}}}}}}}} \\
 &= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{2}{0}}}}}}}}}}}
 \end{aligned}$$

Θέμα 7

Θέμα 8



## Θέμα 9

(α)

Εφαρμόστηκε το τεστ του Fermat με τις συνθήκες που αναφέρονται στην εκφώνηση. Αυτό που παρατηρείται είναι ότι, κατά προσέγγιση, οι μισοί αριθμοί που παράγονται από την  $f(x)$  είναι πρώτοι ενώ οι υπόλοιποι μισοί όχι.

(β)

Τα μόνα πολυώνυμα του  $Z$  που, για κάθε ακέραια τιμή, δίνουν πρώτο αριθμό είναι τα σταθερά πολυώνυμα με τιμή κάποιον πρώτο αριθμό.

$$P(x) = p$$

όπου  $p$  πρώτος αριθμός

Αντιθέτως, δεν υπάρχει μη σταθερό πολυώνυμο για το οποίο να ισχύει η παραπάνω συνθήκη.

Απόδειξη

Έστω ένα μη σταθερό πολυώνυμο  $P(x)$  που μας δίνει πρώτο αριθμό για κάθε τιμή του  $x \in Z$

Τότε ισχύει

$$P(1) = p$$

όπου  $p$  πρώτος αριθμός.

Επομένως ισχύει και

$$P(1 + np) \equiv 0(\text{mod } p), n \in Z$$

γιατί η παραπάνω τιμή του  $P$  διαιρείται με το  $p$ . Επομένως, αφού η τιμή του  $P(1 + np)$  διαιρείται με το  $p$ , δεν είναι πρώτος αριθμός. Άτοπο, άρα η αρχική υπόθεση είναι εσφαλμένη και δεν υπάρχει τέτοιο μη σταθερό πολυώνυμο.