Υπολογιστική Κρυπτογραφία
3η Σειρά Ασκήσεων

Μαραβίτσας Παναγιώτης
Α.Μ: 03116206

15 Δεκεμβρίου 2020

Περιεχόμενα

Άσκηση 1

Έστω ότι ο επιτιθέμενος πραγματοποιεί Known Plaintext Attack (KPA), οπότε διαθέτει αρκετά ζευγάρια plaintext-ciphertext. Η επίθεση πραγματοποιείται ως εξής: Αρχικά επιλέγουμε ένα από αυτά τα ζευγάρια, έστω (M,C). Για το ζευγάρι αυτό έχουμε:

$$C = Enc_{k_1,k_2}(M) = E_{k_1}(M \oplus k_2)$$

$$M = Dec_{k_1,k_2}(C) = E_{k_1}^{-1}(C) \oplus k_2 \implies k_2 = M \oplus E_{k_1}^{-1}(C)$$

Συνεπώς μπορούμε με εξαντλητική αναζήτηση να δοκιμάσουμε όλα τα πιθανά κλειδιά k_1 και να πάρουμε 2^{56} ζευγάρια (k_1, k_2). Για κάθε ζευγάρι plaintext-ciphertext που διαθέτουμε μπορούμε να ελέγξούμε αν το ζευγάρι (k_1, k_2) ικανοποιεί την πρώτη σχέση. Με αυτό τον τρόπο μπορούν να ανακτηθούν και τα 2 κλειδιά του κρυπτοσυστήματος.

Τελικά η πολυπλοκότητα για να σπάσει αυτή η παραλλαγή με KPA είναι ίδια με την πολυπλοκότητα μιας brute force επίθεσης στον απλό DES.

Άσκηση 2

Έστω ότι η κρυπτογράφηση πραγματοποιείται με ένα ασφαλές κρυπτοσύστημα τμήματος με κλειδί k και τρόπο λειτουργίας CBC. Αν m_i είναι το i-οστό block του plaintext και c_i το i-οστό block του ciphertext τότε ισχύει ότι:

$$m_i = Dec_k(c_i) \oplus c_{i-1}$$

Επομένως κατά την αποκρυπτογράφηση, η ανάκτηση ενός block plaintext εξαρτάται από ακριβώς 2 block ciphertext. Συνεπώς εφόσον δεν αλλάξουμε κάποιο από τα τελευταία 2 blocks ciphertext, μπορούμε να τροποποιήσουμε το μήνυμα με το block μηδενικών να παραμένει αμετάβλητο. Μάλιστα αν γνωρίζουμε το περιεχόμενο κάποιου συγκεκριμένου block μπορούμε να αλλάξουμε το περιεχόμενό του σε οτιδήποτε. Έστω λοιπόν ότι γνωρίζουμε το περιεχόμενο του block m_j και θέλουμε να το τροποποιήσουμε σε m_k. Τότε υπάρχει block m_l τέτοιο ώστε $m_j \oplus m_l = m_k$. Αρκεί να τροποποιήσουμε το block c_{j-1} ως εξής:

$$c_{j-1} := c_{j-1} \oplus m_l = c'_{j-1}$$

Τότε λοιπόν έχουμε κατά την αποκρυπτογράφηση:

$$m'_j = Dec_k(c_j) \oplus c'_{j-1} = Dec_k(c_j) \oplus c_{j-1} \oplus m_l = m_j \oplus m_l = m_k$$

Συνεπώς η μέθοδος αυτή δεν εξασφαλίζει ακεραιότητα και απαιτείται κάποια άλλη μέθοδος, για παράδειγμα η χρήση MAC.

Άσκηση 3

1.

Μπορούμε να βρούμε μία σύγκρουση για την h_1 ως εξής:

1. Επιλέγουμε τυχαία x_1, x_2, x_3, x_4 με $x_3 \neq x_4$.
2. Υπολογίζουμε τα $x'_3 = h(x_3||x_3), x'_4 = h(x_4||x_4)$.
3. Τότε έχουμε σύγκρουση μεταξύ των $x_1||x_2||x_3||x'_4$ και $x_1||x_2||x_4||x'_3$

Συγκεκριμένα:

$$\begin{aligned} h_1(x_1||x_2||x_3||x'_4) &= h((x_1 \oplus h(x_2||x_2))||(h(x_3||x_3) \oplus x'_4)) \\ &= h((x_1 \oplus h(x_2||x_2))||(h(x_3||x_3) \oplus h(x_4||x_4))) \end{aligned}$$

$$\begin{aligned} h_1(x_1||x_2||x_4||x'_3) &= h((x_1 \oplus h(x_2||x_2))||(h(x_4||x_4) \oplus x'_3)) \\ &= h((x_1 \oplus h(x_2||x_2))||(h(x_3||x_3) \oplus h(x_4||x_4))) \end{aligned}$$

Επομένως η h_1 δεν είναι collision free.

2.

Έστω ότι η h_2 δεν είναι collision free. Τότε μπορούμε σε πολυωνυμικό χρόνο να βρούμε x, y με $x \neq y$ τέτοια ώστε $h_2(x) = h_2(y)$. Έστω ότι $x = x_1||x_2||x_3||x_4$ και $y = y_1||y_2||y_3||y_4$. Έστω η συνάρτηση $f(x_1||x_2||x_3||x_4) = h(x_1||x_2)||h(x_3||x_4)$. Διακρίνουμε τις παρακάτω περιπτώσεις:

1η Περίπτωση: $f(x) \neq f(y)$
Αφού τα x, y αποτελούν collision για την h_2 τότε τα $f(x), f(y)$ αποτελούν collision για την h.

2η Περίπτωση: $f(x) = f(y)$
Έχουμε ότι $h(x_1||x_2) = h(y_1||y_2)$ και $h(x_3||x_4) = h(y_3||y_4)$. Όμως έχουμε υποθέσει ότι τα x, y αποτελούν collision για την h_2, συνεπάγεται λοιπόν πως υπάρχει κάποιο $i \in \{1, 2, 3, 4\}$ τέτοιο ώστε $x_i = y_i$. Έτσι τουλάχιστον ένα ζευγάρι από τα $x_1||x_2, y_1||y_2$ και $x_3||x_4, y_3||y_4$ αποτελεί collision για την h.

Έτσι καταλήγουμε σε άτοπο αφού για κάθε collision της h_2 μπορούμε να βρούμε γρήγορα κάποιο collision για την h και η h είναι collision free. Τελικά η h_2 είναι collision free.

3.

Μπορούμε να βρούμε μία σύγκρουση για την h_3 ως εξής:

1. Επιλέγουμε τυχαία x_1, x_2 με $x_1 \neq x_2$.
2. Τότε έχουμε σύγκρουση μεταξύ των $x_1||x_1||x_2||x_2$ και $x_2|x_2|x_1||x_1$

Συγκεκριμένα:

$$h_3(x_1||x_1||x_2||x_2) = h(x_1||x_1) \oplus h(x_2||x_2) = h(x_2||x_2) \oplus h(x_1||x_1) = h_3(x_2||x_2||x_1||x_1)$$

Επομένως η h_3 δεν είναι collision free.

4.

Έστω ότι η h_4 δεν είναι collision free. Τότε μπορούμε σε πολυωνυμικό χρόνο να βρούμε x, y με $x \neq y$ τέτοια ώστε $h_4(x) = h_4(y)$. Έστω ότι $x = x_1||x_2||x_3||x_4$ και $y = y_1||y_2||y_3||y_4$. Ορίζουμε τις εξής συναρτήσεις:

- $f_1(x_1||x_2||x_3||x_4) = h(h(x_1||x_2)||x_3)||x_4$
- $f_2(x_1||x_2||x_3||x_4) = h(x_1||x_2)||x_3$

Διακρίνουμε τις περιπτώσεις:

Περίπτωση 1: $f_1(x) \neq f_1(y)$
Αφού τα x,y αποτελούν collision για την h_4, τα $f_1(x), f_1(y)$ αποτελούν collision για την h.

Περίπτωση 2: $f_1(x) = f_1(y)$
Έχουμε ότι $x_4 = y_4$ και $h(h(x_1||x_2)||x_3) = h(h(y_1||y_2)||y_3)$. Διακρίνουμε τις εξής υποπεριπτώσεις:

Περίπτωση 2.1: $f_2(x) \neq f_2(y)$
Τα $f_2(x), f_2(y)$ αποτελούν collision για την h.

Περίπτωση 2.2: $f_2(x) = f_2(y)$
Έχουμε ότι $x_3 = y_3$ και $h_(x_1||x_2) = h(y_1||y_2)$. Όμως για να είναι τα x,y collisions πρέπει $x_1 \neq y_1$ ή $x_2 \neq y_2$, άρα τα $x_1||x_2$, $y_1||y_2$ είναι collisions για την h.

Έτσι καταλήγουμε σε άτοπο αφού για κάθε collision της h_4 μπορούμε να βρούμε γρήγορα κάποιο collision για την h και η h είναι collision free. Τελικά η h_4 είναι collision free.

Άσκηση 4

1.

Έστω ότι η H_3 δεν είναι collision free. Τότε μπορούμε σε πολυωνυμικό χρόνο να βρούμε x, y με $x \neq y$ τέτοια ώστε:

$$H_3(x) = H_3(y) \implies H_1(x)||H_2(x) = H_1(y)||H_2(y) \implies H_1(x) = H_1(y) \wedge H_2(x) = H_2(y)$$

Καταλήγουμε λοιπόν σε άτοπο αφού για κάθε collision της H_3 μπορούμε να κατασκευάσουμε collision για τις H_1, H_2. Άρα σε κάθε περίπτωση η H_3 είναι collision free.

2.

Διακρίνουμε τις εξής περιπτώσεις:

Περίπτωση 1: Μόνο η H_1 είναι collision free
Σε αυτή την περίπτωση η H_4 δεν είναι collision free.
Απόδειξη:
Η H_2 δεν είναι collision free άρα μπορούμε σε πολυωνυμικό χρόνο να βρούμε x, y με $x \neq y$ τέτοια ώστε $H_2(x) = H_2(y)$. Όμως τα x, y αποτελούν collision για την H_4 αφού:

$$H_2(x) = H_2(y) \implies H_1(H_2(x)) = H_1(H_2(y)) \implies H_4(x) = H_4(y)$$

Περίπτωση 2: Μόνο η H_2 είναι collision free
Σε αυτή την περίπτωση δεν μπορούμε να αποφανθούμε για την H_4 χωρίς να γνωρίζουμε την H_1. Για παράδειγμα αν η H_1 είναι σταθερή συνάρτηση τότε η H_4 δεν μπορεί να είναι collision free. Ένα άλλο παράδειγμα είναι η H_1 να έχει επαρκώς μεγάλο πεδίο τιμών και τα outputs να είναι ομοιόμορφα κατανεμημένα σε αυτό. Έστω ότι μπορούμε εύκολα να βρούμε x, y τέτοια ώστε $H_1(x) = H_1(y)$. Επειδή η H_2 είναι collision free είναι υπολογιστικά δύσκολο να βρούμε x', y' τέτοια ώστε $H_2(x') = x$ και $H_2(y') = y$. Επίσης αφού το πεδίο τιμών της H_1 είναι επαρκώς μεγάλο η πιθανότητα να βρεθεί collision με τυχαία επιλογή των x', y' είναι αμελητέα.

Περίπτωση 3: Τόσο η H_1 όσο και η H_2 είναι collision free
Σε αυτή την περίπτωση η H_4 είναι collision free.
Απόδειξη:
Έστω ότι η H_4 δεν είναι collision free. Τότε μπορούμε σε πολυωνυμικό χρόνο να βρούμε x, y τέτοια ώστε $H_4(x) = H_4(y)$. Διακρίνουμε τις περιπτώσεις:

Περίπτωση 1: $H_2(x) = H_2(y)$
Καταλήγουμε σε άτοπο αφού η τα x, y αποτελούν collision για την H_2 η οποία είναι collision free.

Περίπτωση 2: $H_2(x) \neq H_2(y)$
Και σε αυτή την περίπτωση καταλήγουμε σε άτοπο αφού οι $H_2(x), H_2(y)$ αποτελούν collision για την H_1 η οποία είναι collision free.

Τελικά η H_4 είναι collision free αφού για κάθε collision της H_4 μπορούμε να κατασκευάσουμε collision είτε για την H_1, είτε για την H_2.

Άσκηση 5

α.

Αρχικά θα δείξουμε ότι αν ο p είναι πρώτος με $p \equiv 3 \pmod 4$ και $a \in QR(p)$, τότε οι τετραγωνικές ρίζες του α είναι οι αριθμοί $\pm a^{\frac{p+1}{4}}$. Θέτουμε $x = a^{\frac{p+1}{4}}$. Τότε:

$$x^2 \equiv (a^{\frac{p+1}{4}})^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} a \equiv J(\frac{a}{p})a \equiv a \pmod{\text{p}}$$

άρα η υπόθεση ισχύει.

Έστω λοιπόν ότι έχουμε τη γεννήτρια BBS με $n = pq$, και $p \equiv q \equiv 3 \pmod 4$. Επιλέγουμε τυχαία κάποιο $x_0 \in QR(n)$. Αν $BBS_n^i(x) = x^{2^i} \bmod \text{n}$ τότε είναι προφανές πως:

$$\forall i > 0 : BBS_n^i(x_0) \in QR(n)$$

επομένως η ακολουθία $\{BBS_n^0(x_0), BBS_n^1(x_0), \dots\}$ έχει κύκλο. Η ακολουθία αυτή μπορεί να έχει μία από τις παρακάτω μορφές:

1. $\{x_0, x_1, x_2, \dots, x_0, x_1, x_2, \dots\}$
2. $\{x_0, x_1, x_2, \dots, x_{k-1}, x_k, x_{k+1}, \dots x_l, x_k, \dots\}$, με $x_l \neq x_k$

Θα δείξουμε ότι μπορούν να υπάρχουν ακολουθίες μόνο της 1ης μορφής.

Έστω $x \in QR(n)$. Τότε

$$\sqrt{x} = \pm x^{\frac{p+1}{4}} \pmod{\text{p}}$$

όπως δείξαμε παραπάνω. Θα υπολογίσουμε το σύμβολο Jacobi για τις 2 αυτές ρίζες:

$$J(\frac{x^{\frac{p+1}{4}}}{p}) = (J(\frac{x}{p}))^{\frac{p+1}{4}} = 1$$

$$J(\frac{-x^{\frac{p+1}{4}}}{p}) = J(\frac{-1}{p})(J(\frac{x}{p}))^{\frac{p+1}{4}} = J(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = -1$$

όπου η τελευταία ισότητα προκύπτει από το γεγονός πως $p \equiv 3 \pmod 4$. Συνεπώς μόνο η ρίζα $x^{\frac{p+1}{4}} \bmod \text{p}$ είναι τετραγωνικό υπόλοιπο στο $\mathbb{Z}_p^*$. Ομοίως προκύπτει πως μόνο η ρίζα $x^{\frac{q+1}{4}} \bmod \text{q}$ είναι τετραγωνικό υπόλοιπο στο $\mathbb{Z}_q^*$. Συνεπώς το x έχει μοναδική τετραγωνική ρίζα mod n, η οποία ισούται με την απεικόνιση του $(x^{\frac{p+1}{4}} \bmod \text{p}, x^{\frac{q+1}{4}} \bmod \text{q})$ στο $\mathbb{Z}_n^*$ μέσω του CRT. Τελικα υπάρχουν ακολουθίες μόνο της πρώτης μορφής αφού τόσο το x_{k-1} όσο και το x_l είναι τετραγωνικά υπόλοιπα του x_k mod n, κάτι που δεν μπορεί να συμβαίνει όπως δείξαμε παραπάνω.

Γνωρίζοντας πλέον τη μορφή της ακολουθίας και διατηρώντας fixed τα p, q, x_0 μπορούμε να ορίσουμε την περίοδο π ως τον ελάχιστο θετικό ακέραιο τέτοιο ώστε $BBS_n^0(x_0) = BBS_n^\pi(x_0)$. Συμβολίζουμε με $ord_n x$ την τάξη του x στην ομάδα $\mathbb{Z}_n^*$. Για την περίοδο έχουμε λοιπόν ότι:

$$x_0 \equiv x_0^{2^\pi} \text{ (mod n)} \implies 2^\pi \equiv 1 \text{ (mod } ord_n x_0) \implies \pi = ord_{ord_n x_0} 2$$

Η παραπάνω σχέση ικανοποιείται μόνο για τα x_0 τέτοια ώστε $gcd(ord_n x_0, 2) = 1$. Θα δείξουμε ότι ο περιορισμός ικανοποιείται από όλα τα $x \in QR(n)$. Έστω x_i το i-οστό στοιχείο της ακολουθίας. Έχουμε ότι για κάθε $i \geq 0$: $x_{i+1} = x_i^2$ (mod n) Επομένως έχουμε πως:

$$\forall i \geq 0 : x_{i+1} \in < x_i > \implies ord_n x_{i+1} | ord_n x_i$$

όπου η τελευταία συνεπαγωγή προκύπτει από το θεώρημα Lagrange. Επίσης δείξαμε ότι η ακολουθία $\{x_0, x_1, x_2, \dots\}$ είναι περιοδική. Από τα παραπάνω συμπεραίνουμε πως:

$$\forall i \geq 0 : ord_n x_{i+1} = ord_n x_i$$

Έστω ότι $2 | ord_n x_i$. Τότε για την τάξη του x_{i+1} έχουμε:

$$ord_n x_{i+1} = \frac{ord_n x_i}{gcd(2, ord_n x_i)} = \frac{ord_n x_i}{2}$$

Καταλήγουμε σε άτοπο αφού $ord_n x_i = ord_n x_{i+1}$, άρα συμπεραίνουμε πως:

$$\forall i \geq 0 : gcd(2, ord_n x_i) = 1$$

και η σχέση για την περίοδο ισχύει για κάθε $x_0 \in QR(n)$.

Το $gcd(p-1, q-1)$ πρέπει να είναι μικρό αφού έτσι προκύπτει μεγαλύτερη μέγιστη τάξη στην ομάδα $\mathbb{Z}_n^*$. Αυτό είναι προφανές αφού:

$$\lambda(n) = lcm(p-1, q-1) = \frac{(p-1)(q-1)}{gcd(p-1, q-1)}$$

β.

Όπως δείξαμε παραπάνω η περίοδος είναι ο ελάχιστος θετικός ακέραιος π τέτοιος ώστε:

$$2^\pi \equiv 1 \text{ (mod } ord_n x_0)$$

Επιπλέον ισχύει ότι:

$$2^{\lambda(ord_n x_0)} \equiv 1 (\text{mod } ord_n x_0)$$

Συμπεραίνουμε λοιπόν πως:

$$\pi | \lambda(ord_n x_0)$$

Όμως από τον ορισμό της συνάρτησης Carmichael έχουμε:

$$ord_n x_0 | \lambda(n) \implies \lambda(ord_n x_0) | \lambda(\lambda(n))$$

και σε συνδυασμό με την προηγούμενη σχέση προκύπτει:

$$\pi | \lambda(\lambda(n)) \implies \pi \leq \lambda(\lambda(n))$$

Έτσι βρήκαμε ένα άνω φράγμα για την περίοδο δεδομένων p,q. Έστω ότι p,q είναι SafeSafe primes. Τότε $p = 2p' + 1$ και $p' = 2p'' + 1$, όπου p', p'' πρώτοι. Ομοίως $q = 2q' + 1$ και $q' = 2q'' + 1$. Επιπλέον αν $p'' \equiv q'' \equiv 1 \pmod 4$ τότε για τους p, q ισχύει $p \equiv q \equiv 3 \pmod 4$ και επομένως ο $n = pq$ είναι Blum integer. Για αυτές τις επιλογές έχουμε:

$$\lambda(n) = \lambda(pq) = lcm(p-1, q-1) = lcm(2p', 2q') = 2p'q'$$

Επίσης:

$$\lambda(\lambda(n)) = \lambda(2p'q') = lcm(p'-1, q'-1) = lcm(2p'', 2q'') = 2p''q'' \implies \pi \leq 2p''q''$$

Θα δείξουμε ότι αν $ord_n x_0 = \frac{\lambda(n)}{2}$ και το 2 ανήκει το πολύ σε ένα εκ των $QR(p'), QR(q')$ τότε επιτυγχάνουμε τη μέγιστη δυνατή περίοδο. Παρατηρούμε από τους παραπάνω υπολογισμούς ότι

$$\lambda(\frac{\lambda(n)}{2}) = \lambda(\lambda(n)) \implies ord_{\frac{\lambda(n)}{2}} 2 | \lambda(\lambda(n)) \implies ord_{\frac{\lambda(n)}{2}} 2 | 2p''q''$$

Έστω ότι $ord_{\frac{\lambda(n)}{2}} 2 \neq 2p''q''$. Διακρίνουμε τις περιπτώσεις:

Περίπτωση 1: $ord_{\frac{\lambda(n)}{2}} 2 = p''q''$

Σε αυτή την περίπτωση έχουμε ότι:

$$2^{p''q''} \equiv 1 \pmod{\text{p'q'}}$$

Από το CRT παίρνουμε:

$$2^{p''q''} \equiv 1 \pmod{\text{p'}} \implies 2^{p''} \not\equiv -1 \pmod{\text{p'}}$$

όπου η τελευταία συνεπαγωγή προκύπτει από το γεγονός ότι ο q'' είναι περιττός πρώτος. Όμως από τον τρόπο που ορίσαμε τα p, q έχουμε ότι:

$$2^{\frac{p'-1}{2}} \not\equiv -1 \pmod{\text{p'}} \implies 2^{\frac{p'-1}{2}} \equiv 1 \pmod{\text{p'}} \implies 2 \in QR(p')$$

Ομοίως μπορούμε να δείξουμε ότι $2 \in QR(q')$ οπότε καταλήγουμε σε άτοπο αφού υποθέσαμε ότι το 2 ανήκει το πολύ σε ένα εκ των $QR(p'), QR(q')$.

Περίπτωση 2: $ord_{\frac{\lambda(n)}{2}} 2 | 2p''$

Σε αυτή την περίπτωση έχουμε:

$$2^{2p''} \equiv 1 \text{ (mod p'q')}$$

Από το CRT έχουμε:

$$2^{2p''} \equiv 1 \text{ (mod q')}$$

Επιπλέον:

$$2^{2q''} \equiv 2^{2q'' \bmod \lambda(q')} \equiv 2^{2q'' \bmod 2q''} \equiv 1 \text{ (mod q')}$$

Από τις 2 προηγούμενες σχέσεις έχουμε:

$$ord_{q'} 2 | 2p'' \wedge ord_{q'} 2 | 2q'' \implies ord_{q'} 2 = 2 \implies 2^2 \equiv 1 \text{ (mod q')}$$

Καταλήγουμε σε άτοπο αφού $q'' \geq 3 \implies q' \geq 7$.

Περίπτωση 3: $ord_{\frac{\lambda(n)}{2}} 2 | 2q''$

Ομοίως με την προηγούμενη περίπτωση.

Άρα η περίοδος με τις παραπάνω συνθήκες είναι:

$$\pi = ord_{ord_n x_0} 2 = ord_{\frac{\lambda(n)}{2}} 2 = \lambda(\lambda(n) = 2p''q''$$

που είναι μέγιστη.

Άσκηση 6

α.

Οι συνθήκες που πρέπει να ικανοποιούν τα p, q, x_0 έχουν ήδη αναφερθεί παραπάνω. Ο αλγόριθμος επιλογής του x_0 είναι ο εξής:

Αρχικά επιλέγουμε το x_0 να είναι κάποιο τυχαίο τετραγωνικό υπόλοιπο του $\mathbb{Z}_n^*$. Αυτό γίνεται εύκολα επιλέγοντας κάποιο τυχαίο $x \in \mathbb{Z}_n^*$ και υπολογίζοντας το $x_0 = x^2$ mod n. Στη συνέχεια ελέγχουμε αν $ord_n x_0 = \frac{\lambda(n)}{2}$. Γνωρίζουμε ότι $\frac{\lambda(n)}{2} = p'q'$. Αρκεί λοιπόν να ελέγξουμε ότι $x_0^{p'} \not\equiv 1$ mod n, $x_0^{q'} \not\equiv 1$ mod n και $x_0^{p'q'} \equiv 1$ mod n. Αν οι συνθήκες αυτές ικανοποιούνται τότε το x_0 είναι κατάλληλο αλλιώς επαναλαμβάνουμε από την αρχή της διαδικασία.

Ο κώδικας επισυνάπτεται.

β.

Το πρόγραμμα υπολογίζει κατάλληλα p, q ώστε να είναι SafeSafe primes και με βάση αυτά βρίσκει κάποιο κατάλληλο seed x_0. Έχουμε αποδείξει ήδη ότι ο κύκλος ξεκινάει από το x_0 άρα για να υπολογίσουμε πειραματικά την περίοδο αρκεί να βρούμε το ελάχιστο i τέτοιο ώστε:

$$x_0^{2^i} \equiv x_0 \text{ (mod n)}$$

Για το πείραμα χρησιμοποιήθηκαν: $p = 539159$, $q = 555287$ και $x_0 = 14665304776$. Η περίοδος προέκυψε $\pi = 37423087538 = \lambda(\lambda(pq))$ οπότε ταυτίζεται με τη θεωρητική.

Ο κώδικας επισυνάπτεται.

γ.

Έστω ότι το πείραμα αποτελείται από N δοκιμές. Τότε περιγράφεται από το σύνολο τυχαίων μεταβλητών $\{X_i | 1 \leq i \leq N\}$ οι οποίες ορίζονται ως εξής:

$$X_i = \begin{cases} 1, \text{ αν το i-οστό σημείο βρίσκεται εντός του κύκλου} \\ 0, \text{ αλλιώς} \end{cases}$$

Επιπλέον ισχύει ότι $Pr[X_i = 1] = E[X_i] = \frac{\pi}{4}$. Ορίζουμε την τυχαία μεταβλητή X έτσι ώστε:

$$X = \sum_{i=1}^{N} X_i$$

για την οποία προφανώς ισχύει $E[X] = \frac{N\pi}{4}$. Τέλος ορίζουμε την τυχαία μεταβλητή Y να είναι:

$$Y = \frac{4}{N}X$$

Επομένως με αυτό το πείραμα μπορούμε να προσεγγίσουμε την τιμή του π μέσω της Y. Χρησιμοποιώντας το Chernoff bound παίρνουμε:

$$Pr[|Y - \pi| \geq \epsilon\pi] = Pr[|X - \frac{N\pi}{4}| \geq \frac{\epsilon N\pi}{4}] = Pr[|X - E[X]| \geq \epsilon E[X]] \leq 2e^{-\frac{N\pi\epsilon^2}{12}}$$

Έστω ότι θέλω η συνθήκη να μην ικανοποιείται το πολύ με πιθανότητα δ:

$$Pr[|Y - \pi| \geq \epsilon\pi] \leq \delta \implies \delta \geq 2e^{-\frac{N\pi\epsilon^2}{12}} \implies N \geq \frac{12ln(\frac{2}{\delta})}{\pi\epsilon^2}$$

Για να έχω ακρίβεια k δεκαδικών ψηφίων πρέπει να ισχύει προσεγγιστικά:

$$\epsilon\pi = 10^{-k} \implies \epsilon = \frac{10^{-k}}{\pi}$$

Άρα η παραπάνω σχέση γίνεται:

$$N \geq \frac{12ln(\frac{2}{\delta})}{\pi(\frac{10^{-k}}{\pi})^2} \implies N \geq \frac{12\pi ln(\frac{2}{\delta})}{10^{-2k}}$$

Οι τιμές που παίρνουμε για διάφορες τιμές του k με πιθανότητα επιτυχίας 0,95 (δ=0,05) είναι:

- $k = 2$: $N = 1390675$
- $k = 3$: $N = 139067480$
- $k = 4$: $N = 13906747912$

δ.

Πρακτικά το πλήθος σημείων που απαιτείται διαφέρει πολύ από τη θεωρητική προσέγγιση. Η διαφορά αυτή οφείλεται καταρχάς στην ψευδοτυχαιότητα της γεννήτριας. Επίσης το Chernoff bound δεν είναι tight και εμπλέκεται το διάστημα εμπιστοσύνης που έχουμε ορίσει μέσω του δ. Επίσης παρατηρούμε τεράστιες αλλαγές στη συμπεριφορά και την ταχύτητα σύγκλισης ανάλογα με τις αρχικές παραμέτρους p, q, x_0. Τέλος το γεγονός ότι διαθέτουμε μόνο 8 bits για την αναπαράσταση του δεκαδικού μέρους των συντεταγμένων επηρεάζει την ομοιομορφία. Για ορισμένες επιλογές πετύχαμε αριθμό επαναλήψεων αρκετές τάξεις μεγέθους κάτω του θεωρητικού ενώ για άλλες παραμέτρους χρειάζονταν επαναλήψεις της τάξης των δισεκατομμυρίων. Οι τιμές που προέκυψαν φαίνονται παρακάτω:

- 2 δεκαδικά ψηφία: 245 σημεία, π=3.1418181818181816
- 3 δεκαδικά ψηφία: 1682 σημεία, π=3.141498216409037
- 4 δεκαδικά ψηφία: 8560 σημεία, π=3.141588785046729

ε.

Για τα σφάλματα ισχύει ότι αναφέρθηκε και παραπάνω. Μία διαφορά της συγκεκριμένης παραλλαγής της γεννήτριας είναι ότι τρέχει πιο αργά, βέβαια παρουσιάζει καλύτερη απόδοση σε σχέση με την προηγούμενη. Παρόλ'αυτά δεν μπορούμε να καταλήξουμε σε ασφαλή συμπεράσματα αφού τα αποτελέσματα παρουσιάζουν τεράστιες διαφορές ανάλογα με την τυχαία επιλογή των παραμέτρων.

- 2 δεκαδικά ψηφία: 354 σημεία, π=3.1412429378531073
- 3 δεκαδικά ψηφία: 904 σημεία, π=3.1415929203539825
- 4 δεκαδικά ψηφία: 2726 σημεία, π=3.141599413059428

στ.

Μετρήθηκε το ποσοστό των άσσων σε μία ολόκληρη περίοδο καθώς και το μέγιστο πλήθος των διαδοχικών άσσων και για τις 2 γεννήτριες. Το ποσοστό των άσσων στη γεννήτρια του ερωτήματος δ είναι 49.045% ενώ στη γεννήτρια του ερωτήματος ε είναι 50.562%. Επίσης η μέγιστη υπακολουθία άσων στην πρώτη γεννήτρια είναι 31 ενώ στη δεύτερη 33. Τα αποτελέσματα αυτά δεν βοηθούν στη σύγκριση των γεννητριών αφού μεταβάλλονται ανάλογα με τις αρχικές παραμέτρους και δεν αναδεικνύεται κάποια γεννήτρια ως καλύτερη.

Ο κώδικας επισυνάπτεται.

Άσκηση 7

α.

Αρχικά βρίσκουμε $\{a_0, a_1, \ldots, a_l\}$ τέτοια ώστε:

$$\frac{e}{n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$$

Στη συνέχεια υπολογίζουμε τους παρονομαστές $\{d_0, d_1, \ldots, d_l\}$ που αντιστοιχούν στα κλάσματα:

$$a_0, a_0 + \frac{1}{a_1}, a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, \ldots$$

Γνωρίζουμε ότι μπορεί να γίνει επίθεση μικρού ιδιωτικού κλειδιού, συνεπώς ισχύει ότι:

$$|\frac{e}{n} - \frac{k}{d}| < \frac{1}{2d^2}$$

όπου το k ικανοποιεί τη σχέση $ed - 1 = k\phi(n)$. Έχουμε ότι $gcd(k, d) = 1$ άρα ο όρος $\frac{k}{d}$ θα εμφανίζεται στην προσέγγιση του $\frac{e}{n}$ με συνεχή κλάσματα. Επομένως κάποιο από τα d_i θα είναι το ιδιωτικό κλειδί d. Για να βρούμε ποιο από αυτά είναι το σωστό επιλέγουμε κάποιο μήνυμα m της επιλογής μας και υπολογίζουμε το κρυπτογραφημένο μήνυμα:

$$c = m^e \bmod \mathrm{n}$$

Κάποια στιγμή βρίσκουμε κάποιο i έτσι ώστε:

$$c^{d_i} = m \bmod \mathrm{n}$$

Τότε έχουμε ότι $d = d_i$. Για την πολυπλοκότητα αρκεί να βρούμε ένα άνω φράγμα για το l. Οι παρονομαστές μπορούν να υπολογιστούν ως εξής:

$$\begin{cases} d_0 = 1 \\ d_1 = a_1 \\ d_i = a_i d_{i-1} + d_{i-2} \end{cases}$$

Παρατηρούμε ότι οι παρονομαστές αυξάνουν εκθετικά συνεπώς $l \leq log_2 n$. Άρα η πολυπλοκότητα του αλγορίθμου είναι $O(log_2 n)$. Το ιδιωτικό κλειδί που προκύπτει είναι:
67679758331409661713816401785180874988068874274990084068659989503974301456131181
Ο κώδικας επισυνάπτεται.

β.

Έχοντας υπολογίσει το ιδιωτικό κλειδί στο προηγούμενο ερώτημα μπορούμε εύκολα να παραγοντοποιήσουμε το n. Αρχικά υπολογίζουμε τους ακέραιος r,u έτσι ώστε:

$$ed - 1 = 2^r u$$

όπου ο u είναι περιττός. Προφανώς:

$$\forall x \in \mathbb{Z}_n^* : x^{2^r u} \equiv 1 \pmod{\text{n}}$$

αφού $\phi(n)|ed-1$. Στη συνέχεια επιλέγουμε τυχαία κάποιο $x \in \mathbb{Z}_n^*$ και βρίσκουμε το μέγιστο $i \in \{0, 1, \ldots, r\}$ τέτοιο ώστε $x^{2^i u} \neq 1$. Αν $x^{2^i u} = -1$ τότε διαλέγουμε ένα νέο x και επαναλαμβάνουμε τη διαδικασία, αλλιώς μπορούμε να βρούμε τους παράγοντες του n υπολογίζοντας το $gcd(x^{2^i u} \pm 1, n)$. Αποδεικνύεται εύκολα μέσω του θεωρήματος Lagrange ότι τουλάχιστον τα μισά στοιχεία του $\mathbb{Z}_n^*$ οδηγούν σε παραγοντοποίηση. Οι παράγοντες που προκύπτουν είναι:
$p = 515922504741315943566749626987403219891093291864676284839218850201391293036$
$344358376382452245353721492342154735795372962145641675651400838388064633544892732162 37$
$q = 441225636302982878179780023917144908558044211539195809764775288443859939724$
$603243003044160103093016783412390407709958156638782463818955150559850179211550929 63657$

Ο κώδικας επισυνάπτεται