Κρυπτογραφία

9ο Εξάμηνο 2023 – 2024

Assignment 2 – Solutions

Ζαρίφης Στέλιος – el20435
Email: el20435@mail.ntua.gr

Contents

Άσκηση 1

a

Άσκηση 2

Θεωρούμε την παραλλαγή του DES-X, με 2 κλειδιά $k1$, $k2$, όπου η κρυπτογράφηση ενός απλού κειμένου M γίνεται ως εξής:

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

όπου E η συνάρτηση κρυπτογράφησης του DES. Θεωρούμε ακόμα ότι ο αντίπαλος έχει δυνατότητα KPA.
Έστω ο αντίπαλος γνωρίζει τα 2 ζεύγη message-ciphertext $(m_1, c_1), (m_2, c_2)$ και ότι $D_{k_1}(c_1), D_{k_1}(c_2)$ οι αποκρυπτογραφήσεις με το κλασσικό DES, άρα θα έχουμε:

$$D_{k_1}(c_1) \oplus D_{k_1}(c_2) = (m_1 \oplus k_2) \oplus (m_2 \oplus k_2) = m_1 \oplus m_2$$

Συνεπώς, ο αντίπαλος μπορεί να ακολουθήσει τα εξής βήματα:

Algorithm: Attack

```
forall possible keys k_1 do
    calculate D_{k_1}(c_1) ;                          // Given c_1, k_1
    calculate D_{k_1}(c_2) ;                          // Given c_2, k_1
    if D_{k_1}(c_1) ⊕ D_{k_1}(c_2) == m_1 ⊕ m_2 then
        k_2 ← m_1 ⊕ D_{k_1}(c_1);
        return k_1, k_2;
```

Έτσι, ο αντίπαλος θα ανακαλύψει τα κλειδιά k_1, k_2 σε 2^{56} το πολύ επαναλήψεις (αφού το μήκος κλειδιού είναι 56 bits) που σημαίνουν 2×2^{56} αποκρυπτογραφήσεις. Σχετικά, λοιπόν, με το κλασσικό DES (2^{56} αποκρυπτογραφήσεις με brute force), το DES-X δεν προσφέρει μεγαλύτερη ασφάλεια, αφού ασυμπτωτικά απαιτεί ίδιας τάξης πλήθος αποκρυπτογραφήσεων.

Άσκηση 3

Ερώτημα 1

Θεωρούμε το DES 2 γύρων και το δίκτυο $Feistel_{f_1,f_2}$ που χρησιμοποιηεί στους 2 γύρους τις $f_1 = F(k_1, R), f_2 = F(k_2, R)$.

Θα αποδείξουμε το εξής $Feistel_{f_1,f_2}(L_0, R_0) = (L_2, R_2) \Rightarrow (R_0, L_0)$:

- Για το $Feistel_{f_1,f_2}(L_0, R_0)$ έχουμε:

$$\begin{aligned} L_1 &= R_0 \\ R_1 &= L_0 \oplus f_1(R_0) \\ L_2 &= R_1 = L_0 \oplus f_1(R_0) \\ R_2 &= L_1 \oplus f_2(R_1) = R_0 \oplus f_2(L_2) \end{aligned}$$

- Για το $Feistel_{f_2,f_1}(R_2, L_2), L'_0 = R_2, R'_0 = L_2$ έχουμε:

$$\begin{aligned} L'_1 &= R'_0 \\ R'_1 &= L'_0 \oplus f_2(R'_0) \\ L'_2 &= R'_1 = L'_0 \oplus f_2(R'_0) \\ R'_2 &= L'_1 \oplus f_1(R'_1) = R'_0 \oplus f_1(L'_2) \end{aligned}$$

Αντικαθιστούμε $L'_0 = R_2, R'_0 = L_2$:

$$\begin{aligned} L'_2 &= R_2 \oplus f_2(L_2) \\ R'_2 &= L_2 \oplus f_1(L'_2) \end{aligned}$$

Επίσης είδαμε πως:

$$R_2 = R_0 \oplus f_2(L_2) \Rightarrow R_0 = R_2 \oplus f_2(L_2) \Rightarrow R_0 = R_2 \oplus L'_2 \oplus R_2 = L'_2$$

και από τις πιο πάνω σχέσεις, έχουμε:

$$R'_2 = L_2 \oplus f_1(R_0) = R_0$$

Άρα είναι:

$$\begin{aligned} R'_2 &= L_0 \\ L'_2 &= R_0 \\ Feistel_{f_2,f_1}(R_2, L_2) &= (R_0, L_0) \end{aligned}$$

Έστω το DES_{f_1,f_2} που χρησιμοποιεί το $Feistel_{f_2,f_1}$ και ύστερα αντιμεταθέτει τα L, R: $\text{DES}_{f_1,f_2} = (R_2, L_2)$
Αυτό, με είσοδο το $(L'_0, R'_0) = (R_2, L_2)$ μας δίνει:

$$\text{DES}_{f_2,f_1}(L'_0, R'_0) = DES_{f_2,f_1}(R_2, L_2) = \text{Swap}\left(\text{Feistel}_{f_2,f_1}(R_2, L_2)\right) = \text{Swap}(R_0, L_0) = (L_0, R_0)$$

Όπου $\text{Swap}(x = x[0 : mid] \| x[mid + 1, n]) = x[mid + 1, n] \| x[0 : mid]$

Επαγωγικά λοιπόν, μπορούμε να δούμε ότι

$$\text{DES}_{f_{16},\ldots,f_1}(\text{DES}_{f_1,\ldots,f_{16}}(L_0, R_0)) = \text{DES}_{f_{16},\ldots,f_1}(R_2, L_2) = (L_0, R_0)$$

Όταν τα κλειδιά είναι ίδια για όλους τους γύρους, κάθε γύρος θα έχει τη συνάρτηση $f_i = f$, άρα $\text{DES}_{f,\ldots,f}(\text{DES}_{f,\ldots,f}(L_0, R_0)) = (L_0, R_0)$
Ασθενές είναι ένα κλειδί όταν σε κάθε γύρο προκύπτουν τα ίδια υποκλειδιά. Τα κλειδιά παράγονται ως εξής:

$$k_{i+1} = \text{transposition}(k_i[0 : mid]) \| \text{transposition}'(k_i[mid + 1 : n])$$

Όπου transposition & $\text{transposition}'$ (κάποιες) μεταθέσεις. Παρατηρούμε ότι αν το κλειδί k_i έχει μια από τις εξής ειδικές μορφές:

$$k_i = 0^{56} \text{ ή } k_i = 0^{28} \| 1^{28} \text{ ή } k_i = 1^{28} \| 0^{28} \text{ ή } k_i = 1^{56}$$

Το επόμενο κλειδί θα είναι $k_{i+1} = \text{transposition}(k_i[0 : mid]) \| \text{transposition}'(k_i[mid + 1 : n]) = k_i$. Έτσι προκύπτουν τα 4 ασθενή κλειδιά.

Ερώτημα 2

Στο γύρο i, το DES έχει κλειδί K_i, για το οποίο είναι:

$$K_i = \text{transposition}'(K_L \ll n_i, K_R \ll n_i), \text{ όπου } K_L \| K_R = \text{transposition}(K)$$

Με transposition, transposition$'$ συμβολίζουμε 2 διαφορετικές μεταθέσεις (σταθερές κάθε φορά) και ο τελεστής $\ll n_i$ σημαίνει bit rotation, όπου το πλήθος θέσεων n_i κάθε φορά είναι Semi-weak keys είναι τα κλειδιά των οποίων τα μέρη K_L, K_R επαναλαμβάνονται

$n_0 = 1$	$n_1 = 2$	$n_2 = 4$	$n_3 = 6$
$n_4 = 8$	$n_5 = 10$	$n_6 = 12$	$n_7 = 14$
$n_8 = 15$	$n_9 = 17$	$n_{10} = 19$	$n_{11} = 21$
$n_{12} = 23$	$n_{13} = 25$	$n_{14} = 27$	$n_{15} = 28$

με περίοδο 2, δηλαδή παραθέσεις $K = K_L \| K_R$ όπου τα K_L, K_R επιλέγονται από

- $0000 \ldots 00$
- $0101 \ldots 01$
- $1010 \ldots 10$
- $1111 \ldots 11$

Άσκηση 4

Ερώτημα 1

Έστω το CBC με τη συνάρτηση $e_k : 1 - 1$. Οι σχέσεις που συνδέουν τα blocks $i-1, i$ και $j-1, j$ είναι οι εξής:

$$y_i = e_k(y_{i-1} \oplus x_i), y_j = e_k(y_{j-1} \oplus x_j)$$

Άρα, δεδομένης σύγκρουσης $y_i = y_j$, έχουμε $e_k(y_{i-1} \oplus x_i) = e_k(y_{j-1} \oplus x_i) \Rightarrow y_{i-1} \oplus x_i = y_{j-1} \oplus x_j \Rightarrow x_i \oplus x_j = y_{i-1} \oplus y_{j-1}$
Άρα μπορούμε να εξάγουμε πληροφορία για το plaintext.

Ερώτημα 2

Η πιθανότητα να μην υπάρχει σύγκρουση με hash size x δεδομένου ότι παράγουμε

- $k = 2$ κλειδιά: $\Pr[No\_Collision \mid k = 2] = \dfrac{x-1}{x}$
- $k = 3$ κλειδιά: $\Pr[No\_Collision \mid k = 3] = \Pr[No\_Collision \mid k = 2] \cdot \dfrac{x-2}{x} = \dfrac{(x-1)(x-2)}{x^2}$
- $k = n$ κλειδιά: $\Pr[No\_Collision \mid k = n] = \dfrac{(x-1)(x-2)\dots(x-n+1)}{x^n} \leq \prod_{i=1}^{n-1} e^{-i/x} = \exp\left(\frac{\sum_{i=1}^{n-1} i}{n}\right) = e^{-\frac{n(n-1)}{2x}}$

Άρα η πιθανότητα να έχουμε σύγκρουση, για το συγκεκριμένο hash size ($x = 2^{64}$) είναι

$$\Pr[Collision \mid k = n] \geq 1 - e^{-\frac{n(n-1)}{2 \cdot 2^{64}}} = 1 - e^{-\frac{n(n-1)}{2^{65}}}$$

Ερώτημα 3

Παρατηρούμε ότι για την πιθανότητα $\Pr[Collision \mid k = n] \geq 1 - e^{-\frac{n(n-1)}{2x}}$, μπορούμε να επιλέξουμε το n να είναι της τάξης του $\sqrt{x}$, δηλαδή $n = \lambda\sqrt{x}$ ή ισοδύναμα και τότε έχουμε:

$$\Pr[Collision \mid k = n] \approx 1 - e^{-\frac{n^2}{2x}} = 1 - e^{-\frac{\lambda^2}{2}}$$

Επομένως, για πιθανότητα σύγκρουσης p, είναι $p \approx 1 - e^{-\frac{\lambda^2}{2}} \Rightarrow \lambda \approx \sqrt{-2\ln(1-p)}$.
Αν, για παράδειγμα, όπως στο παράδοξο των γενεθλίων επιθυμούμε πιθανότητα σύγκρουσης τουλάχιστον 50% (δηλαδή τότε θεωρούμε χρήσιμη επίθεση), επιλέγουμε $\lambda \approx \sqrt{-2\ln(1-0.5)} \Rightarrow \lambda \approx 1.1774$, άρα το n πρέπει να είναι τουλάχιστον $1.1774\sqrt{x} = 1.1774\sqrt{2^{64}} \approx 5056894494.3104$

Άσκηση 5

Ερώτημα 1

Ο αλγόριθμος έχει ως εξής:

- Ξεκινάμε με μήνυμα m μήκους 0 και μετράμε το μήκος της εξόδου $c = \text{AES}_k(m\|s)$.
- Αυξάνουμε το μήκος της εισόδου σε κάθε βήμα κατά 1 και παρατηρούμε το νέο μήκος της εξόδου.
- Τη στιγμή που θα παρατηρήσουμε διαφορετικό μήκος εξόδου, επιστρέφουμε τη διαφορά των μηκών και αυτή είναι το μέγεθος του block.

Ο αλγόριθμος λειτουργεί επειδή το AES προσθέτει 1 block κάθε φορά που γεμίζει το προηγούμενο. Οπότε τη στιγμή της προσθήκης νέου block, μπορούμε να μετρήσουμε το block size.

Algorithm: Block Size Determination for AES Encryption

Data: AES key k
Result: Block size of AES encryption

$message \leftarrow$ empty;
$initial\_output\_length \leftarrow$ length(AES_encrypt($message\|\text{s}, k$));
for $i \leftarrow 1$ **to** ∞ **do**
    $message \leftarrow message +' A'$; `// Increase the length of the input message by 1`
    $new\_output\_length \leftarrow$ length(AES_encrypt($message\|\text{s}, k$));
    if $new\_output\_length \neq initial\_output\_length$ **then**
        $block\_size \leftarrow new\_output\_length - initial\_output\_length$;
        return $block\_size$;

Ερώτημα 2

Από το προηγούμενο ερώτημα γνωρίζουμε το block size. Δίνουμε είσοδο το μήνυμα $m = m_1\|m_1, length(m_1) = block\ _size$, δηλαδή την παράθεση 2 ίδιων μηνυμάτων μήκους όσο το block size. Αν το Oracle χρησιμοποιεί ECB, τότε η έξοδος θα είναι $c = \text{AES}(m) = c_1\|c_1, c_1 = \text{AES}(m_1)$. Αλλιώς (αν δε χρησιμοποιεί ECB), με μικρή πιθανότητα αν το Oracle χρησιμοποιεί CBC και υπάρξει collision μπορεί το m_1 να έδινε ίδια κρυπτογράφηση c_1.

Algorithm: ECB Detection

Data: Block size b, Oracle function AES(m)
Result: Detection of ECB mode

`// Construct the input message` $m = m_1\|m_1$, `where` $|m_1| = b$
$m \leftarrow m_1\|m_1$;
`// Encrypt the message using the Oracle`
$c \leftarrow \text{AES}(m)$;
`// Extract the blocks of the ciphertext`
$c_1 \leftarrow c[0 : mid - 1]$;
$c_2 \leftarrow c[mid : b - 1]$;
`// Check for ECB mode`
if $c_1 = c_2$ **then**
    return *ECB mode detected*;
return *Not ECB mode*;

Ερώτημα 3

Άσκηση 6

Έστω η γεννήτρια ψευδοτυχαιότητας RC4. Θα δείξουμε ότι το δεύτερο byte εξόδου είναι ίσο με 0 με πιθανότητα περίπου ίση με 2^{-7}.

Algorithm: PRGA - First Iteration

1 $i \leftarrow 0, j \leftarrow 0$;
2 $i \leftarrow 1, j \leftarrow P[1] = 0 + P[1]$; // $P[1] \neq 2$
3 swap$(P[1], P[a])$;
4 $P[1] \leftarrow P[a] = P[P[1]]$;
5 $P[a] \leftarrow a$;
6 $K_0 \leftarrow P[P[1] + P[a] \pmod{256}] = P[1] + a \pmod{256}$

Algorithm: PRGA - Second Iteration

1 $i \leftarrow 2, j \leftarrow a + P[1] = a$;
2 swap$(P[2], P[a])$;
3 $P[2] \leftarrow P[a] = a$;
4 $P[a] \leftarrow P[2] = 0$;
5 $K_1 \leftarrow P[P[2] + P[a] \pmod{256}] = P[a] = 0$

Οπότε μετά τη φάση δημιουργίας κλειδιών (KSA) έχουμε $\Pr[_1 = 0] = 1$ αν $P[2] = 0$ και $P[1] \neq 2$.
Έστω το ενδεχόμενο όπου $P[2] = 0$ και $P[1] \neq 2$. Τότε η πιθανότητα το δεύτερο byte να είναι μηδέν είναι:

$$\begin{aligned}\Pr[K_1 = 0] &= \sum_A \Pr[K_1 = 0, A] = \sum_A \Pr[K_1 = 0 \mid A] \Pr[A] = \\ &= \Pr[K_1 = 0 \mid A = True] \Pr[A = True] + \Pr[K_1 = 0 \mid A = False] \Pr[A = False] = \\ &= 1 \cdot \Pr[A = True] + \frac{1}{256} \cdot (1 - \Pr[A = True])\end{aligned}$$

Αν θεωρήσουμε ότι η μετάθεση $P[\cdot]$ ακολουθεί ομοιόμορφη κατανομή, τότε:

$$\Pr[A = True] = \Pr[P[2] = 0] \cdot \Pr[P[1] \neq 2] = \frac{1}{256} \cdot (1 - \Pr[P[1] = 2]) = \frac{1}{256}\left(1 - \frac{1}{255}\right) \simeq \frac{1}{256}$$

Και τελικά για τη ζητούμενη πιθανότητα έχουμε:

$$\Pr[K_1 = 0] = \frac{1}{256} + \frac{1}{256}\left(1 - \frac{1}{256}\right) \simeq \frac{1}{256} + \frac{1}{256} = \frac{2}{256} = 2^{-7}$$

Άσκηση 7

Θεωρούμε την ψευδοτυχαία συνάρτηση $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

Ερώτημα 1

Έστω η $F_1(k,x) = F(k,x)\|0$ και ένας διαχωριστής $\mathcal{D}$ που ρωτάει το oracle $\mathcal{O}$ για $x_1, x_2, ..., x_n$ και επιστρέφει 1 για είσοδο x_i όταν το $\mathcal{O}(x_i) = y_i$ λήγει σε 0. Το oracle είτε είναι ίσο με F_{1_k} (για ομοιόμορφο k) ή με f (για ομοιόμορφη f). Εξετάζουμε τις 2 περιπτώσεις:

1. Αν $\mathcal{O} = F_{1_k}$, τότε $\Pr\left[D^{F_{1_k}}(1^n) = 1\right] = 1$
2. Αν $\mathcal{O} = f$, τότε $\Pr\left[D^{f}(1^n) = 1\right] = \prod_{i=1}^{n} \frac{1}{2} = \frac{1}{2^n}$

Είναι λοιπόν:

$$\left|\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}^{F_{1_k}}(1^n) = 1\right] - \Pr_{f\leftarrow Func_n}\left[\mathcal{D}^{f}(1^n) = 1\right]\right| = \left|1 - \frac{1}{2^n}\right| > \text{negl}(n)$$

Από τον ορισμό της ψευδοτυχαίας συνάρτησης έχουμε ότι η συνάρτηση **δεν** είναι ψευδοτυχαία.

Ερώτημα 2

Έστω η $F_2(k,x) = F(k,x) \oplus x$ και έστω ότι **δεν** είναι PRF. Αυτή σημαίνει ότι για κάποιο x, δεδομένου του $F_2(k,x)$ μπορούμε με μη αμελητέα πιθανότητα να "μαντέψουμε" το x.
Εκφράζουμε την $F(k,x)$ ως $F(k,x)\oplus x\oplus x = F_2(k,x)\oplus x$. Δείξαμε ότι αν η $F_2(k,x)$ **δεν** είναι PRF, τότε για κάποιο x, δεδομένου του $F_2(k,x)$ μπορούμε με μη αμελητέα πιθανότητα να "μαντέψουμε" το x. Οπότε με μη αμελητέα πιθανότητα μπορούμε να αποκτήσουμε το ζεύγος $F_2(k,x), x$ και συνεπώς το $F_2(k,x) \oplus x = F(k,x)$. Άρα δείξαμε ότι με μη αμελητέα πιθανότητα, για κάποιο x μπορούμε με γνώση του $F(k,x)$ να βρούμε αυτό το x. Δηλαδή δείξαμε πως και η $F(k,x)$ **δεν** είναι PRF, άρα καταλήξαμε σε άτοπο!
Τελικά, η $F_2(k,x)$ είναι PRF.

Ερώτημα 3

Έστω η $F_3(k,x) = F(k, x \oplus 1^n)$. Παρατηρούμε ότι το $y = x \oplus 1^n$ είναι μια $1-1$ απεικόνιση του x στο y. Συνεπώς, $F_3 \approx F$, άρα είναι ψευδοτυχαία.

Ερώτημα 4

Έστω η $F_4(k,x) = F(k, F(k,x))$ και ένας διαχωριστής $\mathcal{D}$ που ρωτάει το oracle $\mathcal{O} : \mathcal{O}(x) = y_L\|y_R$ και επιστρέφει 1 όταν $\mathcal{O}(x) = y_L\|y_R \wedge \mathcal{O}(y_L) = y'_L\|y'_R \wedge y'_L = y_R$. Το oracle είτε είναι ίσο με F_{4_k} (για ομοιόμορφο k) ή με f (για ομοιόμορφη f). Εξετάζουμε τις 2 περιπτώσεις:

1. Αν $\mathcal{O} = F_{4_k}$, τότε

$$\mathcal{O}(x) = F_k(x)\|F_k(F_k(x))$$
$$\mathcal{O}(F_k(x)) = F_k(F_k(x))\|F_k(F_k(F_k(x)))$$
$$\text{RightPart}(\mathcal{O}(x)) = \text{LeftPart}(\mathcal{O}(F_k(x)))$$

   Συνεπώς ο διαχωριστής θα επιστρέφει πάντα 1, άρα $\Pr\left[D^{F_{4_k}}(1^n) = 1\right] = 1$ $\Pr\left[D^{F_{1_k}}(1^n) = 1\right] = 1$

2. Αν $\mathcal{O} = f$, τότε $\Pr\left[D^{f}(1^n) = 1\right] = \epsilon$, ϵ: αμελητέο.

Είναι:

$$\left|\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}^{F_{4_k}}(1^n) = 1\right] - \Pr_{f\leftarrow Func_n}\left[\mathcal{D}^{f}(1^n) = 1\right]\right| = |1 - \epsilon| > \text{negl}(n)$$

Από τον ορισμό της ψευδοτυχαίας συνάρτησης έχουμε ότι η συνάρτηση **δεν** είναι ψευδοτυχαία.

Άσκηση 8

Ερώτημα 1

Ακολουθώντας το original paper των Blum, Blum, Shub [1], θα προσδιορίσουμε την περίοδο π της γεννήτριας.

Απόδειξη ότι $\pi \mid \lambda(\lambda(n))$ Έστω x_π η πρώτη έξοδος της γεννήτριας που ταυτίζεται με το seed $x_0 = s_0$. Η γεννήτρια παράγει αριθμούς με τη σχέση $x_{i+1} \equiv x_i^2 \pmod n$. Επομένως, για το i-οστό στοιχείο έχουμε τον κλειστό τύπο $x_i \equiv x_0^{2^i} \pmod p$. Αφού το x_π είναι η πρώτη φορά που εμφανίζεται ξανά το $x_0 \equiv x_\pi \equiv x_0^{2^\pi} \pmod n$, τότε οι εκθέτες είναι ίσοι, δηλαδή $2^\pi \equiv 1 \pmod n$.

Η τάξη του $x_0 \pmod n$ είναι ο ελάχιστος ακέραιος k για τον οποίο ισχύει $x_0^k \equiv 1 \pmod n$. Γράφουμε $x_0^{\text{ord}_n(x_0)} \equiv 1 \pmod n$.

Από τις τελευταίες 2 προτάσεις, αφού $\text{ord}_n(x_0)$ είναι ο ελάχιστος ακέραιος με την ιδιότητα, ο $2^\pi - 1$ θα είναι πολλαπλάσιό του, οπότε μπορούμε να γράψουμε:

$$x_0^{2^\pi} \equiv x_0 \equiv x_0^{a\cdot \text{ord}_n(x_0)} \cdot x_0 \equiv x_0^{a\cdot \text{ord}_n(x_0)+1} \pmod n \Rightarrow 2^\pi \equiv 1 \pmod{\text{ord}_n(x_0)} \quad (1)$$

Ακόμα, από την επέκταση του Carmichael για το θεώρημα του Euler, έχουμε:

$$2^{\lambda(\text{ord}_n(x_0))} \equiv 1 \pmod{\text{ord}_n(x_0)} \quad (2)$$

Συνδυάζοντας τις $(1, 2)$, γνωρίζοντας ότι ο π είναι ο ελάχιστος ακέραιος που ικανοποιεί τη σχέση (δηλαδή $\pi \leq \lambda(\text{ord}_n(x_0))$), έχουμε ότι:

$$\pi \mid \lambda(\text{ord}_n(x_0)) \quad (3)$$

Όμως, γνωρίζουμε ότι $x_0^{\text{ord}_n(x_0)} \equiv 1 \pmod n$ (προφανώς), $x_0^{\lambda}(n) \pmod n$ (ιδιότητα της συνάρτησης Carmichael) και $\lambda(n) \geq \text{ord}_n(x_0)$ (αφού $a \mid \lambda(n), \forall a : coprime(n)$), οπότε προκύπτει:

$$\text{ord}_n(x_0) \mid \lambda(n) \quad (4)$$

Από τις προτάσεις $(3, 4)$ συμπεραίνουμε ότι:

$$\pi \mid \lambda(\text{ord}_n(x_0)) \mid \lambda(\lambda(n))$$

Προϋποθέσεις ώστε $\lambda(\lambda(n)) \mid \pi$ Οι Blum, Blum, Shub εξηγούν πως αν επιλέξουμε:

$$n \text{ s.t. } \text{ord}_{\lambda(n)/2}(2) = \lambda(\lambda(n)) \quad (A)$$
$$x_0 \text{ s.t. } \text{ord}_n(x_0) = \lambda(n)/2 \quad (B)$$

μπορούμε να δείξουμε ότι $\lambda(\lambda(n)) \mid \pi$.

Από την πρόταση (B) έχουμε ότι το $\lambda(n)/2$ είναι ο ελάχιστος εκθέτης ώστε $x_0^{\lambda(n)/2} \equiv 1 \pmod n \quad (C)$. Οπότε, αφού επίσης $x_0^{2^\pi} \equiv x_0 \pmod n \Rightarrow x_0^{2^\pi - 1} \equiv 1 \pmod n \quad (D)$ και $\lambda(n)/2 = \text{ord}_n(x_0) < 2^\pi - 1$ (αφού η τάξη είναι ελάχιστη), τότε από τις σχέσεις (C, D) έχουμε:

$$\lambda(n)/2 \mid 2^\pi - 1 \Rightarrow 2^\pi \equiv 1 \pmod{\lambda(n)/2} \quad (E)$$

Τελικά, από (A) έχουμε ότι $2^{\lambda(\lambda(n))} \pmod{\lambda)(n)/2}$ ενώ η (E) μας έδειξε ότι $2^\pi \equiv 1 \pmod{\lambda(n)/2}$ και επειδή το $\lambda(\lambda(n))$ είναι τάξη, άρα ελάχιστο, έχουμε ότι

$$\lambda(\lambda(n)) \mid \pi$$

Από τα παραπάνω, βλέπουμε ότι με επιλογή

$$n \text{ s.t. } \text{ord}_{\lambda(n)/2}(2) = \lambda(\lambda(n)) \quad (A)$$
$$x_0 \text{ s.t. } \text{ord}_n(x_0) = \lambda(n)/2 \quad (B)$$

Καταλήγουμε στη σχέση που δίνει τη μέγιστη περίοδο της γεννήτριας BBS:

$$\pi \mid \lambda(\lambda(n)) \wedge \lambda(\lambda(n)) \mid \pi \Rightarrow \pi = \lambda(\lambda(n))$$

Ακόμα, από τις ιδιότητες της συνάρτησης Carmichael, έχουμε ότι αν το n μπορεί να γραφτεί ως γινόμενο 2 πρώτων p, q, είναι

$$\lambda(n) = \lambda(p \cdot q) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(\phi(p), \phi(q)) = \text{lcm}(p-1, q-1)$$

Επιπλέον, από την ταυτότητα Bezout προκύπτει $(p-1)\cdot(q-1) = \text{lcm}(p-1,q-1)\cdot\gcd(p-1,q-1)$. Συνεπώς, όσο μικρότερο είναι το $\gcd(p-1,q-1)$, τόσο μεγαλύτερο θα είναι το $\text{lcm}(p-1,q-1) = \lambda(n)$, ως ποσά αντιστρόφως ανάλογα. Η συνάρτηση Carmichael, βέβαια, δεν είναι μονότονη, συνεπώς αυτή η σχέση δεν εγκυάται τη μεγιστοποίηση της $\pi = \lambda(\lambda(n))$. Όμως, όπως μπορούμε να παρατηρήσουμε από τη γραφική της παράσταση, όσο μεγαλώνει το όρισμα της n, τόσο αυξάνεται και η αναμενόμενη τιμή της $\mathbb{E}[\lambda(\lambda(n))]$. Συνεπώς, επιδιώκουμε μικρές τιμές $\gcd(p-1,q-1)$ καθώς δίνουν μεγάλη τιμή $\mathbb{E}[\lambda(\lambda(n))] = \mathbb{E}[\pi]$
Μάλιστα, από το paper των P. Erdős, C. Pomerance και E. Schmutz [2] προκύπτει ότι καθώς $n \to \infty$ είναι:

$$\lambda(n) = n\exp(-(1+o(1))\log\log n\log\log\log n)$$

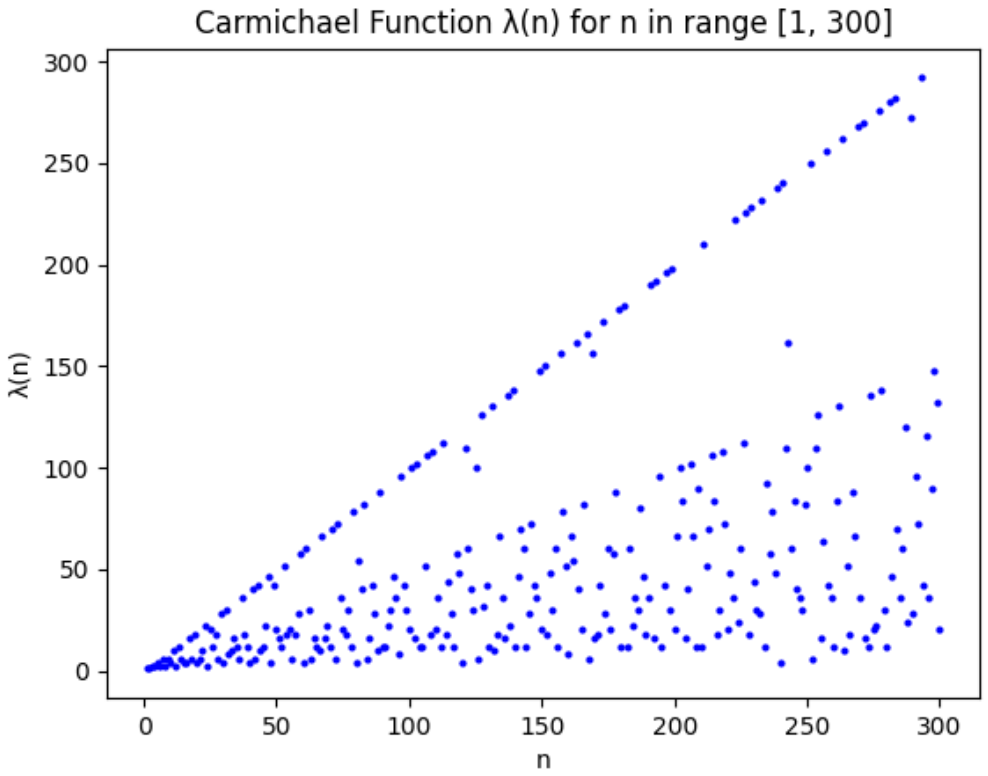

Figure 1: Carmichael Function $\lambda(n)$ for n in the range [1, 300]

Ερώτημα 2

Έστω τώρα $n = pq$, με p, q safe-safe primes. Υπολογίζουμε:

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

$$\lambda(\lambda(n)) = \lambda(2p'q') = \text{lcm}(\lambda(2),\lambda(p'),\lambda(q')) = \text{lcm}(1,\phi(p'),\phi(q')) = \text{lcm}(p'-1,q'-1) = \text{lcm}(2p'',2q'') = 2p''q''$$

Ακόμα θα δείξουμε ότι $\lambda(\lambda(n)/2) = \lambda(\lambda(n))$:

$$\lambda(\lambda(n)/2) = \lambda(2p'q'/2) = \text{lcm}(1,\phi(p'),\phi(q')) = 2p''q'' \text{ από τα παραπάνω}$$

Τώρα θα δείξουμε ότι $\text{ord}_{\lambda(n)/2}(2) \mid \lambda(\lambda(n))$:
Από τον ορισμό του λ, το $\lambda(\lambda(n)/2)$ είναι ο ελάχιστος ακέραιος στον οποίο αν υψώσουμε οποιονδήποτε πρώτο με το $\lambda(n)/2$, προκύπτει $1 \pmod{\lambda(n)/2}$. Επειδή $\lambda(n)/2 = p'q' = (2p''+1)(2q''+1) = odd$ τότε είναι πρώτος με το 2. Άρα $2^{\lambda(\lambda(n)/2)} \equiv 1 \pmod{\lambda(n)/2}$
Όμως, η τάξη $\text{ord}_{\lambda(n)/2}(2)$ είναι ο ελάχιστος ακέραιος στον οποίον αν υψώσουμε το 2 προκύπτει $1 \pmod{\lambda(n)/2}$. Άρα

$$2^{\lambda(\lambda(n)/2)} \equiv 1 \pmod{\lambda(n)/2} \bigwedge 2^{\text{ord}_{\lambda(n)/2}(2)} \equiv 1 \pmod{\lambda(n)/2} \bigwedge \text{ord}_{\lambda(n)/2}(2) < \lambda(\lambda(n)/2) \Longrightarrow$$

$$\Rightarrow \text{ord}_{\lambda(n)/2}(2) \mid \lambda(\lambda(n)/2) = \lambda(\lambda(n)) = 2p''q''$$

Έστω τώρα ότι $\text{ord}_{\lambda(n)/2}(2) \neq 2p''q''$. Τότε θα είναι είτε $\text{ord}_{\lambda(n)/2}(2) \mid p''q''$ είτε $\text{ord}_{\lambda(n)/2}(2) \mid 2p''$ είτε $\text{ord}_{\lambda(n)/2}(2) \mid 2q''$ ή αλλιώς, χωρίς βλάβη της γενικότητας, θα είναι είτε $\text{ord}_{\lambda(n)/2}(2) \mid p''q''$ είτε $\text{ord}_{\lambda(n)/2}(2) \mid 2p''$.

Περίπτωση $\text{ord}_{\lambda(n)/2}(2) \mid p''q''$ Είναι
$2^{p''q''} \equiv 1 \pmod{p'q'} \Rightarrow 2^{p''q''} \equiv 1 \pmod{q'}$.
Έστω ότι $2^{q''} \equiv -1 \pmod{q'}$. Τότε $(2^{q''})^{p''} \equiv (-1)^{p''} \equiv -1 \pmod{q'}$, αφού p'' είναι περιττός. Άρα προέκυψε ότι $2^{p''q''} \equiv -1 \pmod{q'}$ δηλαδή άτοπο. Άρα είναι $2^{q''} = 2^{(q'-1)/2} \not\equiv -1 \pmod{q'}$. Όμως, $2 \in \mathbb{Z}_{q'}^*$, οπότε $2^{(q'-1)/2} \equiv \pm 1 \pmod{q'}$ και από τα προηγούμενα είναι υποχρεωτικά $2^{(q'-1)/2} \equiv 1 \pmod{q'}$. Άρα το 2 είναι τετραγωνικό υπόλοιπο ως προς q'. Συμμετρικά προκύπτει ότι το 2 είναι τετραγωνικό υπόλοιπο και ως προς p'. Αυτό όμως είναι άτοπο.

Περίπτωση $\text{ord}_{\lambda(n)/2}(2) \mid 2p''$ Έχουμε
$\text{ord}_{\lambda(n)/2}(2) \mid 2p'' \Rightarrow 2^{2p''} = 2^{k \cdot \text{ord}_{\lambda(n)/2}(2)} \equiv 1 \pmod{\lambda(n)/2} \equiv 1 \pmod{p'q'}$. Αυτό όμως συνεπάγεται ότι $2^{2p''} \equiv 1 \pmod{p'} \bigwedge 2^{2p''} \equiv 1 \pmod{q'}$. Επίσης από το μικρό θεώρημα του Fermat έχουμε

$$2^{2q''} = 2^{2q'-1} \equiv 1 \pmod{q'}$$

Τελικά αφού $q'' \geq 3 \Rightarrow q' \geq 7$ είναι

$$2^{\gcd(2p'',2q'')} = 2^2 = 4 \equiv 1 \pmod{q'} \Rightarrow \text{Άτοπο}$$

Τελικά δείξαμε ότι η αρχική υπόθεση $\text{ord}_{\lambda(n)/2}(2) \neq 2p''q''$ είναι άτοπη, άρα $\text{ord}_{\lambda(n)/2}(2) = 2p''q''$.

Οπότε αποδείξαμε ότι όταν $n = pq$, με p, q safe-safe primes, είναι $\text{ord}_{\lambda(n)/2}(2) = 2p''q''$, δηλαδή ικανοποιούνται οι προϋποθέσεις που περιγράψαμε στο ερώτημα 1 ώστε να έχουμε μέγιστη περίοδο!

Άσκηση 9

Άσκηση 10

Ερώτημα 1

Θεωρούμε τη hash function $H : \{0,1\}^* \to \{0,1\}^n$ για την οποία είναι $H(m = x \oplus w) = H(x) \oplus H(w)$.

Έστω η H είναι collision resistant. Σε αυτήν την περίπτωση, θα έχει αντίσταση πρώτου ορίσματος. Αυτό σημαίνει ότι για κάποιο y είναι δύσκολο να βρεθεί m τέτοιο ώστε $H(m) = y$. Παρατηρούμε όμως ότι με $y = 0$ και $m = x \oplus x$ τότε $H(m) = H(x) \oplus H(x) = 0 = y$ (το "$\oplus$" 2 ίδιων στοιχείων ισούται με 0). Άρα αφού η H δεν έχει αντίσταση πρώτου ορίσματος, κατλήξαμε σε άτοπο: Η H **δεν** είναι collision resistant.

Ερώτημα 2

Θεωρούμε τη hash function $H(x) = H_1(x)\|H_2(x)\|H_3(x)$, όπου μόνο μία H_i είναι collision resistant.

Έστω ότι υπάρχουν x_1, x_2 που οδηγούν σε collision στην H. Αυτό σημαίνει ότι:

$$H(x_1) = H(x_2) \Rightarrow H_1(x_1)\|H_2(x_1)\|H_3(x_1) = H_1(x_2)\|H_2(x_2)\|H_3(x_2)$$

Επειδή η H είναι παράθεση συμβολοσειρών, οι αντίστοιχες υπακολουθίες των $H(x_1), H(x_2)$ θα είναι ίσες για να ισχύει η ισότητα $H(x_1) = H(x_2)$. Δηλαδή $H_1(x_1) = H_1(x_2) \wedge H_2(x_1) = H_2(x_2) \wedge H_3(x_1) = H_3(x_2)$. Αφού μία H_i είναι collision resistant, τότε εξαναγκάζει την ολική H να είναι collision resistant, αφού είναι computationally infeasible να βρεθούν τα x_1, x_2 που θα έχουν ίδιο output.

Άσκηση 11

Έστω η Hash Function $H_1 : 0,1^{2n} \to 0,1^n$.
Έστω $h = 3$ και ότι η H δεν είναι Collision Resistant. Τότε ένας αντίπαλος μπορεί να βρεί μέσω PPT $x_0x_1 \dots x_8$ και $x'_0x'_1 \dots x'_8$ διαφορετικά μεταξύ των τέτοια ώστε (από ορισμό Merkle Tree):

$$H(x_0x_1 \dots x_8) = H(x'_0x'_1 \dots x'_8) \Rightarrow$$

$$H_1\left(H_1\left(H_1\left(x_0x_1\right)H_1\left(x_2x_3\right)\right)H_1\left(H_1\left(x_4x_5\right)H_1\left(x_6x_7\right)\right)\right) = H_1\left(H_1\left(H_1\left(x'_0x'_1\right)H_1\left(x'_2x'_3\right)\right)H_1\left(H_1\left(x'_4x'_5\right)H_1\left(x'_6x'_7\right)\right)\right)$$

Ορίζουμε $H_1(x_ix_j) = H_1^{ij}$ και $H_1(x'_ix'_j) = \hat{H_1}^{ij}$

$$H_1\left(H_1\left(H_1^{01}H_1^{23}\right)H_1\left(H_1^{45}H_1^{67}\right)\right) = \hat{H_1}\left(\hat{H_1}\left(\hat{H_1}^{01}\hat{H_1}^{23}\right)\hat{H_1}\left(\hat{H_1}^{45}\hat{H_1}^{67}\right)\right)$$

Και $H_1\left(H_1^{ij}H_1^{kl}\right) = H_1^{ijkl}, \hat{H_1}\left(\hat{H_1}^{ij}\hat{H_1}^{kl}\right) = \hat{H_1}^{ijkl}$

$$H_1\left(H_1^{ijkl}\right) = \hat{H_1}\left(\hat{H_1}^{ijkl}\right)$$

Είδαμε λοιπόν πως ο αντίπαλος μπορεί να βρίσκει εισόδους $x \neq y$ τέτοιες ώστε $H_1(x) = H_1(y)$, οπότε η H_1 **δεν** είναι Collision Resistant. Επαγωγικά μπορούμε να το δείξουμε αυτό για κάθε $h > 3$.
Συνεπώς, αν η H_1 διαθέτει δυσκολία εύρεσης συγκρούσεων τότε και η H διαθέτει δυσκολία εύρεσης συγκρούσεων.

Άσκηση 12

Ερώτημα 1

Έστω ένα κρυπτοσύστημα $\mathcal{CS}$ και αντίπαλος $\mathcal{A}$ που μπορεί να ανακτήσει το κλειδί από κρυπτοκείμενο του $\mathcal{CS}$ με μη-αμελητέα πιθανότητα.
Εξηγούμε το παίγνιο IND - CPA:
Ο $\mathcal{A}$ στέλνει στον $\mathcal{CS}$ τυχαίο μήνυμα m^*. Ο $\mathcal{CS}$ απαντάει με το $c^* = encrypt(m^*)$. Ο $\mathcal{A}$ υπολογίζει ένα κλειδί k' για το οποίο είναι $\Pr[k = k'] = p > negl$ (k το πραγματικό κλειδί). Τότε ο $\mathcal{A}$ στέλνει τα μηνύματα m_0 και m_1 στον $\mathcal{CS}$, αφού υπολογίσει πρώτα τις κρυπτογραφήσεις $c_0 = encrypt(k', m_0), c_1 = encrypt(k', m_1)$. Ο $\mathcal{CS}$ επιλέγει τυχαία ποιο από τα 2 μηνύματα (m_0, m_1) θα κρυπτογραφήσει και το στέλνει (έστω c) στον $\mathcal{A}$. Αν $c \neq c_0 \wedge c \neq c_1$ (δηλαδή $k \neq k'$) τότε ο $\mathcal{A}$ επιλέγει τυχαία ένα b' από το $\{0, 1\}$ και το επιστρέφει, αλλιώς ο $\mathcal{A}$ συγκρίνει το c με τα c_0, c_1 (έχουμε την περίπτωση $k = k'$). Αν $c = c_0$ τότε $b' = 0$, ενώ αν $c = c1$ τότε $b' = 1$ οπότε σε αυτήν την περίπτωση θα είναι $b = b'$ με πιθανότητα 1.
Η πιθανότητα επιτυχίας του $\mathcal{A}$ είναι:

$$\begin{aligned}\Pr[b = b'] &= \sum_c \Pr[b = b', c] = \Pr[b = b', c = c_0] + \Pr[b = b', c = c_1] + \Pr[b = b', c \notin \{c_0, c_1\}] = \\ &= \Pr[b = b' \mid c = c_0] \Pr[c = c_0] + \Pr[b = b' \mid c = c_1] \Pr[c = c_1] + \Pr[b = b' \mid c \notin \{c_0, c_1\}] \Pr[c \notin \{c_0, c_1\}] = \\ &= 1 \cdot \frac{1}{2} \cdot p + 1 \cdot \frac{1}{2} \cdot p + \frac{1}{2} \cdot (1 - p) = \frac{p+1}{2} > negl \text{ αφού } p > negl\end{aligned}$$

Επομένως, το $\mathcal{CS}$ δεν έχει ασφάλεια CPA.

Ερώτημα 2

Έστω αντίπαλος και challenger $\mathcal{C}$. Ο έχει τις εξής ιδιότητες:
Ο ρωτάει τον $\mathcal{C}$ για το μήνυμα $m = 0^{n-1}1$ και ο τελευταίος του επιστρέφει το ciphertext που χρησιμοποιήθηκε για initial vector IV. Αν το IV τελειώνει σε 0 τότε ο $\mathcal{A}$ επιστρέφει τυχαίο $b' \in 0, 1$. Αν το IV τελειώνει σε 1 τότε ο $\mathcal{A}$ στέλνει μηνύματα $m_0 = 0^n, m_1 = random(0, 1^n)$. Τότε ο $\mathcal{C}$ επιστρέφει το challenge $c', IV + 1$, όπου c' η κρυπτογράφηση του m_0 ή του m_1. Το ποιο μήνυμα θα κρυπτογραφηθεί προσδιορίζεται από το τυχαίο $b' \in 0, 1$. Τέλος, αν $c = c'$ τότε ο επιστρέφει $b' = 0$ ενώ αν $c \neq c'$ θα επιστραφεί $b' = 1$.
Η πιθανότητα επιτυχίας του είναι:

$$\begin{aligned}\Pr[b = b'] &= \sum_{IV[-1]} \Pr[b = b', IV[-1] = \Pr[b = b', IV[-1] = 1] + \Pr[b = b', IV[-1] = 0] = \\ &= \Pr[b = b' \mid IV[-1] = 1] \Pr[IV[-1] = 1] + \Pr[b = b' \mid IV[-1] = 0] \Pr[IV[-1] = 0] = \\ &= \frac{1}{2} \cdot \frac{1}{2} + \Pr[b = b' \mid IV[-1] = 0] \cdot \frac{1}{2}\end{aligned}$$

Έχουμε ότι αν $IV[-1] = 0$ τότε $IV + 1 = IV \oplus 0^{n-1}1$ και άρα:

$$c = enc(IV \oplus m) = enc(IV \oplus 0^{n-1}1 \oplus m \oplus 0^{n-1}1) = enc(IV \oplus m)$$

Δηλαδή αν ο $\mathcal{C}$ κρυπτογράφησε το m_0, θα είναι $c = c'$ και άρα ο $\mathcal{A}$ θα επιστρέψει 0, ενώ αν ο $\mathcal{C}$ κρυπτογράφησε το m_1 ο $\mathcal{A}$ θα επιστρέψει 1, δηλαδή πάντα θα επιστρέφει το σωστό b, οπότε

$$\Pr[b = b'] = \frac{1}{2} \cdot \frac{1}{2} + \Pr[b = b' \mid IV[-1] = 0] \cdot \frac{1}{2} = \frac{1}{4} + \frac{1}{2} \cdot 1 = \frac{3}{4} > negl$$

Επομένως, το $\mathcal{CS}$ δεν έχει ασφάλεια CPA.

Ερώτημα 3

References

[1] Andrey Sidorenko and Berry Schoenmakers. Concrete security of the blum-blum-shub pseudorandom generator. In Nigel P. Smart, editor, *Cryptography and Coding*, pages 355–375, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[2] P. Erdős, C. Pomerance, and E. Schmutz. Carmichael's lambda function. *Acta Arithmetica*, 58:363–385, 1991.