Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

---

# Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

## 3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 10/1/2023

**Άσκηση 1.** Έστω $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ ψευδοτυχαία συνάρτηση. Εξετάστε τις παρακάτω συναρτήσεις ως προς την ψευδοτυχαιότητα τους:

1. $F_1(k,x) = F(k,x) \oplus x$
2. $F_2(k,x) = F(F(k,0^n),x)$
3. $F_3(k,x) = F(F(k,0^n),x)||F(k,x)$
4. $F_4(k,x) = F(k, x \oplus 1^n)$
5. $F_5(k,x) = F(k,x) \oplus F(k, x \oplus 1^n)$

**Άσκηση 2.** Θεωρήστε την γεννήτρια ψευδοτυχαίων bit BBS με Blum integer $n = pq$.
(α) Να προσδιορίσετε επακριβώς την περίοδο της γεννήτριας. Εξηγήστε γιατί πρέπει να είναι μικρό το $\gcd(p-1, q-1)$.
(β) Οι "safe primes" είναι ειδικοί πρώτοι αριθμοί της μορφής $p = 2p' + 1$ όπου $p'$ είναι επίσης πρώτος. Ονομάζουμε "SafeSafe primes" τους ειδικούς εκείνους πρώτους $p$ για τους οποίους ισχύει ότι αν $p''$ είναι πρώτος με $p'' \equiv 1 \pmod 4$, τότε $2p''+1$: πρώτος και $p = 2(2p''+1)+1$. Ποια είναι η **μέγιστη** περίοδος της γεννήτριας στην περίπτωση που τόσο ο $p$ όσο και ο $q$ είναι "SafeSafe" πρώτοι; Να αποδείξετε τον ισχυρισμό σας.

**Άσκηση 3.** 'Εστω $\mathsf{H}$ συνάρτηση σύνοψης, η οποία συμπιέζει ακολουθίες μήκους $2n$ σε ακολουθίες μήκους $n$ και έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων (collision free). Θέλουμε να φτιάξουμε μία συνάρτηση σύνοψης που να συμπιέζει ακολουθίες μήκους $4n$ σε ακολουθίες μήκους $n$, η οποία να έχει επίσης την ιδιότητα δυσκολίας εύρεσης συγκρούσεων. Έχουμε τις εξής υποψήφιες:

1. $\mathsf{H}_1(x_1||x_2||x_3||x_4) = \mathsf{H}(\mathsf{H}(x_1||x_2)||\mathsf{H}(x_3||x_4))$
2. $\mathsf{H}_2(x_1||x_2||x_3||x_4) = \mathsf{H}(x_1||x_2) \oplus \mathsf{H}(x_3||x_4)$

Για κάθε $i$ εξετάστε αν η $\mathsf{H}_i$ έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων ή όχι. Για να δείξετε ότι την έχει, δείξτε ότι αν μπορούσαμε να βρούμε συγκρούσεις για την $\mathsf{H}_i$, τότε θα μπορούσαμε να βρούμε συγκρούσεις και για την $\mathsf{H}$. Για να δείξετε το αντίθετο βρείτε μία ή περισσότερες συγκρούσεις για την $\mathsf{H}_i$.

**Άσκηση 4.** Δίνεται μια συνάρτηση σύνοψης $\mathsf{H}_1 : \{0,1\}^{2n} \to \{0,1\}^n$. Η συνάρτηση αυτή χρησιμοποιείται σε κάποιο δένδρο Merkle ύψους $h$ με είσοδο μια δυαδική ακολουθία $x_0x_1 \dots x_{2^h}$ όπου κάθε $x_i$ είναι μια δυαδική ακολουθία μεγέθους $n$ bits. Με διαδοχικές εφαρμογές της $\mathsf{H}_1$, το Merkle tree μπορεί να θεωρηθεί καθ'αυτό ως μια συνάρτηση σύνοψης $\mathsf{H}$ που συμπιέζει συμβολοσειρές μεγέθους $n2^h$ σε συμβολοσειρές μεγέθους $n$. Να δείξετε ότι αν η $\mathsf{H}_1$ διαθέτει δυσκολία εύρεσης συγκρούσεων τότε και η $\mathsf{H}$ διαθέτει δυσκολία εύρεσης συγκρούσεων.

**Άσκηση 5.** Σταθερό σημείο ενός κρυπτοσυστήματος ονομάζουμε ένα μήνυμα που το κρυπτοκείμενό του είναι το ίδιο το μήνυμα, δηλαδή $enc(m) = m$. Επομένως, στην περίπτωση του RSA, αν το δημόσιο κλειδί είναι το $(N, e)$, τότε για ένα σταθερό σημείο ισχύει $m^e \equiv m \pmod N$. Αποδείξτε ότι το πλήθος των σταθερών σημείων στο RSA είναι $[\gcd(e-1, p-1) + 1][\gcd(e-1, q-1) + 1]$.

**Άσκηση 6.** Να υλοποιήσετε σε γλώσσα προγραμματισμού της επιλογής σας μια επίθεση αποκρυπτογράφησης ενός κρυπτοκειμένου $c$ σε RSA που χρησιμοποιεί ένα oracle το οποίο μπορεί να αποφανθεί αν το μήνυμα που αντιστοιχεί στο κρυπτοκείμενο είναι στο 'πάνω' ή στο 'κάτω' μισό του $\mathbb{Z}_n$ (δηλ. συνάρτηση $\mathsf{loc}$ - βλ. διαφάνειες για διάλεξη RSA).

Συγκεκριμένα πρέπει να υλοποιήσετε 2 τμήματα κώδικα:

(1) Το πρώτο θα 'προσομοιώνει' το oracle, αποκρυπτογραφώντας (κανονικά με το ιδιωτικό κλειδί) το $c$ και υπολογίζοντας την $\mathsf{loc}$.

(2) Το δεύτερο θα υλοποιεί την επίθεση ρωτώντας επαναληπτικά το oracle κατάλληλες ερωτήσεις για την $\mathsf{loc}$.

Η παραγωγή των κλειδιών και η αρχική κρυπτογράφηση μπορεί να γίνει από δικό σας κώδικα ή χρησιμοποιώντας ένα έτοιμο εργαλείο όπως το Openssl.

**Άσκηση 7.** Δίνεται η παρακάτω πρακτική παραλλαγή του κρυπτοσυστήματος ElGamal η οποία έχει στόχο να μπορούν να κρυπτογραφούνται δυαδικές ακολουθίες μήκους $n$ αντί για στοιχεία της ομάδας $\mathbb{G}$.

- $\mathsf{KGen}(1^\lambda)$: Όπως στις διαφάνειες. Επιπλέον επιστρέφεται μία συνάρτηση σύνοψης $\mathsf{H} : \mathbb{G} \to \{0,1\}^n$.
- $\mathsf{Enc}_y(m) = (g^r, \mathsf{H}(y^r) \oplus m)$ με $r \in \mathbb{Z}_q$ ομοιόμορφα επιλεγμένο.
- $\mathsf{Dec}_x(c) = \mathsf{H}(c_1^x) \oplus c_2$ με $c = (c_1, c_2)$.

Να μελετήσετε την παραλλαγή αυτή ως προς την ασφάλεια. Συγκεκριμένα να εξετάσετε αν ικανοποιεί τις ιδιότητες OW-CPA, IND-CPA, IND-CCA. Καταγράψτε τις απαραίτητες υποθέσεις για τις ιδιότητες που πρέπει να διαθέτει η $\mathsf{H}$.

**Άσκηση 8.** Δίνεται σχήμα δέσμευσης $C$ με συνάρτηση δέσμευσης την $\mathsf{Commit}(y, m) = y^2 s^m \bmod n$ όπου:

- $m \in \{0,1\}$.

- $n = p \cdot q$ και $p = q = 3 \pmod 4$.
- $y \in \mathbb{Z}_n^*$ ομοιόμορφα επιλεγμένο.
- Το $s$ δεν είναι τετραγωνικό υπόλοιπο $\pmod n$.

Να εξετάσετε αν το $C$ έχει τις ιδιότητες της δέσμευσης και της απόκρυψης και υπό ποιες υποθέσεις.

Σε όλες τις ασκήσεις με "$\oplus$" συμβολίζουμε το XOR και με "||" την παράθεση.

**Σύντομες οδηγίες**: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο, με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Σε κάθε περίπτωση οι απαντήσεις πρέπει να είναι *αυστηρά ατομικές*.