Όνομα: ΑΜ:

Κρυπτογραφία – Γραπτή εξέταση Σεπτεμβρίου 2019

Οδηγίες:

- Απαντήστε και τα 4 (τέσσερα) θέματα. Τα θέματα είναι ισοδύναμα. Μέγιστη βαθμολογία είναι το 120.
- Για τους μεταπτυχιακούς υπάρχουν επιπλέον ερωτήματα με κατάλληλη ένδειξη.
- Δεν επιτρέπονται σημειώσεις ή υπολογιστικές συσκευές.
- Να απαντάτε στο ζητούμενο με σαφήνεια, και να εξηγείτε τη σκέψη σας.
- Πριν αρχίσετε να λύνετε, διαβάστε όλα τα θέματα.

Θέμα 1. (α΄) Να βρεθεί η τάξη του στοιχείου 7 της ομάδας $\mathbb{Z}_{15}$ με πράξη την πρόσθεση modulo 15.

[Μονάδες: 10 (Μεταπτυχιακοί: 5)]

(β΄) Να βρεθεί η τάξη του στοιχείου 7 της ομάδας $\mathbb{Z}_{15}^*$ με πράξη τον πολλαπλασιασμό modulo 15.

[Μονάδες: 10 (Μεταπτυχιακοί: 5)]

(γ΄) Δίνεται κρυπτοσύστημα ElGamal με παραμέτρους $\mathbb{G} = \mathbb{Z}_{23}^*$, $q = 11$, $g = 4$. Το ιδιωτικό κλειδί είναι 6. Να υπολογίσετε το δημόσιο κλειδί και να κρυπτογραφήσετε το μήνυμα 3 με randomness r ίσο με το τελευταίο ψηφίο του ΑΜ σας (εάν είναι 0, να θέσετε r=10).

[Μονάδες: 10]

(δ΄) **Μόνο Μεταπτυχιακοί.** Είναι η ομάδα $\mathbb{Z}_{15}^*$ κυκλική;

[Μονάδες: 10 (Μόνο Μεταπτυχιακοί)]

Θέμα 2. (α΄) Να δώσετε τον ορισμό της Στατιστικής Απόστασης ανάμεσα σε δύο κατανομές.

[Μονάδες: 10]

Σε μία συσκευή, υπάρχει μια γεννήτρια τυχαίων αριθμών η οποία σε κάθε κλήση επιστρέφει ένα τυχαίο bit. Στις προδιαγραφές της συσκευής, η γεννήτρια επιστρέφει 1 με πιθανότητα $\frac{1}{2}$.

Δυστυχώς, για λόγους κόστους, ο Λυκούργος προμηθεύτηκε συσκευές Β΄ διαλογής, στις οποίες η γεννήτρια δυσλειτουργεί, και επιστρέφει 1 με πιθανότητα $\frac{1}{2} + \delta$, όπου $0 < \delta < \frac{1}{2}$.

(β΄) Υπολογίστε τη στατιστική απόσταση που έχουν τα αποτελέσματα της συσκευής Β΄ διαλογής από μίας κανονικής.

[Μονάδες: 10]

(γ΄) Ο Λυκούργος πιστεύει ότι μπορεί να βελτιώσει την συμπεριφορά της γεννήτριας εάν κάθε φορά που χρειάζεται ένα bit καλεί τη γεννήτρια δύο φορές και κάνει XOR τα αποτελέσματα. Εξηγήστε τι σημαίνει «βελτιώσει» τη συμπεριφορά, και εξετάστε (αυστηρά) αν η διαίσθηση του Λυκούργου είναι σωστή.

[Μονάδες: 10]

Θέμα 3. Δίνεται η παρακάτω παραλλαγή του συστήματος υπογραφών RSA:

$\mathcal{M}$ Ο χώρος μηνυμάτων περιορίζεται στο $\mathbb{Z}_n^*$ (αντί του $\{0,1\}^*$). Υπενθυμίζεται ότι το $\mathbb{Z}_n^*$ αποτελείται από τα στοιχεία του $\mathbb{Z}_n$ που έχουν αντίστροφο (δηλ. όσα είναι σχετικά πρώτα με το n).

$H()$ Αντί συνάρτησης κατακερματισμού, χρησιμοποιούμε τη συνάρτηση id από το $\mathcal{M}$ στο $\mathbb{Z}_n^*$ όπου $\mathrm{id}(x) = x$.

Οι υπόλοιπες συναρτήσεις και παράμετροι είναι όπως στις σημειώσεις: συνοπτικά, η Gen παράγει ως δημόσιο κλειδί ένα ζευγάρι (n, e) και ως ιδιωτικό κλειδί ένα d, τέτοια ώστε $n = p \cdot q$ για p, q διαφορετικούς πρώτους, και $e \cdot d = 1 \mod \phi(n)$). Η υπογραφή σ πάνω σε ένα μήνυμα $m \in \mathcal{M}$ υπολογίζεται ως $m^d \mod n$. Η επαλήθευση γίνεται όπως στις σημειώσεις.

(α΄) Εξετάστε, ξεχωριστά, αν το σύστημα υπογραφών μετά τις αλλαγές είναι ορθό και ασφαλές (ως προς UF-CMA).

[Μονάδες: 15]

(β΄) Δείξτε ότι η λειτουργία του παραλλαγμένου πρωτοκόλου παραμένει ορθή (αν όχι πάντα, αρκεί με συντριπτική πιθανότητα ως προς μια τυχαία επιλογή μηνύματος) εάν στη θέση του $\mathbb{Z}_n^*$ για τον χώρο μηνυμάτων θέσουμε $\mathbb{Z}_n$. Μπορείτε να χρησιμοποιήσετε την έννοια της στατιστικής απόστασης.

[Μονάδες: 15]

Θέμα 4. Δίνεται μια παραλλαγή του πρωτοκόλλου του Schnorr με το οποίο θέλουμε να να αποδείξουμε τη γνώση ενός διακριτού λογαρίθμου, δηλαδή οτι για κάποια πρόταση της μορφής $\langle \mathbb{G}, q, g, h \rangle$ γνωρίζουμε w ώστε να ισχύει $h = g^w$ χωρίς να το φανερώσουμε.

i. Ο $\mathcal{P}$ διαλέγει $t \xleftarrow{\text{r}} \mathbb{Z}_q$ και στέλνει τα $y = g^t$ στον $\mathcal{V}$.
ii. Ο $\mathcal{V}$ διαλέγει μια πρόκληση $c \xleftarrow{\text{r}} \mathbb{Z}_q$ και την στέλνει στον $\mathcal{P}$.
iii. Ο $\mathcal{P}$ υπολογίζει το $s = t \cdot c + w \mod q$ και στέλνει το s στον $\mathcal{V}$.
iv. Ο $\mathcal{V}$ ελέγχει και αποδέχεται αν και μόνο αν $g^s =$ _____.

(α΄) Να συμπληρώσετε το κενό στον ορισμό του verifier ώστε να ισχύει η πληρότητα και η εγκυρότητα. Για την πληρότητα να δώσετε απόδειξη, η εγκυρότητα αξιολογείται στο επόμενο υποερώτημα.

[Μονάδες: 15 (Μεταπτυχιακοί: 10)]

(β΄) Να εξετάσετε το συμπληρωμένο πρωτόκολο ως προς την ειδική εγκυρότητα, και τη μηδενική γνώση τίμιου επαληθευτή (να εξεταστούν και οι δύο ιδιότητες).

[Μονάδες: 15 (Μεταπτυχιακοί: 10)]

(γ΄) **Μόνο Μεταπτυχιακοί.** Να εξετάσετε το συμπληρωμένο πρωτόκολο ως προς την μηδενική γνώση. **Υποδειξη**: μπορείτε να υποθέσετε ότι εργαζόμαστε με ομάδες όπου το πρόβλημα του διακριτού λογαρίθμου είναι δύσκολο.

[Μονάδες: 10 (Μόνο Μεταπτυχιακοί)]

Καλή Επιτυχία