Τελικό Διαγώνισμα Κρυπτογραφία

Επώνυμο :
Όνομα :
Α.Μ.:

Οδηγίες : Κάθε θέμα είναι 2.5 βαθμοί. Ένα θέμα κενό (εντελώς λευκή σελίδα) είναι 0.5 βαθμοί. Μία εντελώς άσχετη απάντηση σε ένα θέμα είναι 0 βαθμοί. Έτσι π.χ. κάποιος μπορεί να πάρει 5 με μία τέλεια απάντηση (2.5) και μία που πιάνει το 60%.

Άσκηση 1

Έστω το εξής κρυπτοσύστημα $\langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$: η $\mathcal{G}$ με είσοδο 1^k παράγει το δημόσιο κλειδί $\langle n, e, H(\cdot) \rangle$, όπου n k-bit σύνθετος και το μυστικό κλειδί $\langle d, p, q \rangle$. Ισχύει ότι $e \cdot d = 1 \bmod \phi(n)$, $n = pq$ (όπως στο RSA) καθώς και $H : \mathbb{Z}_n \to \{0,1\}^k$ είναι μια συνάρτηση κατακερματισμού (hash). Η συνάρτηση $\mathcal{E}$ με είσοδο $M \in \{0,1\}^k$ επιστρέφει την τιμή $\langle r^e \bmod n, H(r) \oplus M \rangle$ όπου $\oplus$ συμβολίζει την πράξη exclusive-or μεταξύ δυαδικών συμβολοακολουθιών. Για την απόδειξη, φανταζόμαστε ότι το $H : \mathbb{Z}_n^* \to \{0,1\}^k$ λειτουργεί σαν τυχαίο μαντείο.

(1) Διατυπώστε την υπόθεση RSA και το μοντέλο ασφάλειας IND-CPA.

(2) Περιγράψτε πως πιστεύετε οτι πρέπει να δουλεύει η διαδικασία της αποκρυπτογράφησης $\mathcal{D}$.

(3) Δείξετε ότι το κρυπτοσύστημα ικανοποιεί ασφάλεια τύπου IND-CPA στο μοντέλο τυχαίου μαντείου κάτω από την υπόθεση RSA.

Επώνυμο:
Όνομα:
Α.Μ.:

Άσκηση 2

Έχετε τρία νομίσματα από τα οποία τα δύο είναι κίβδηλα. Ένα κίβδηλο επιστρέφει γράμματα με πιθανότητα $0 < \alpha < 1/2$ ενώ το άλλο επιστρέφει γράμματα με πιθανότητα $1 - \alpha$. Το τρίτο νόμισμα είναι γνήσιο και επιστρέφει γράμματα με πιθανότητα $1/2$. Τα νομίσματα είναι αδιαχώριστα 'με το μάτι.'

(1) Δώστε τον τύπο της στατιστικής απόστασης μεταξύ δύο πιθανοτικών κατανομών.

(2) Περιγράψτε έναν αλγόριθμο που τερματίζει πάντοτε και που χρησιμοποιεί τα τρία νομίσματα με τις ελάχιστες δυνατές ρίψεις ώστε να επιστρέψει έξοδο που είναι ομοιόμορφα κατανεμημένη στο $\{0, 1\}$. Αν δεν μπορείτε να βρείτε τέτοιο αλγόριθμο δώστε έναν αλγόριθμο που τερματίζει πάντοτε και πλησιάζει την ομοιόμορφη κατανομή όσο καλύτερα γίνεται (με τη έννοια της στατιστικής απόστασης). Σε κάθε περίπτωση δώστε πλήρη αιτολόγηση της απάντησης σας. Σημείωση: ο αλγόριθμος σας δεν πρέπει να χρησιμοποιεί άλλη πηγή τυχαιότητας πέρα από τα τρία νομίσματα.

Επώνυμο :
Όνομα :
Α.Μ.:

Άσκηση 3

(1) Να ορίσετε τι είναι ένα πρωτόκολλο μηδενικής γνώσης για μία γλώσσα $\mathcal{L} = \{x \mid \exists w : R(x, w) = 1\}$ (όπου R πολυωνυμικός αλγόριθμος με έξοδο στο $\{0, 1\}$) δίνοντας τις τρεις ιδιότητες : πληρότητα (completeness), ορθότητα (soundness), μηδενική γνώση (zero-knowledge). Να δώσετε μόνο τη 'μαθηματική διατύπωση' των ιδιοτήτων - εξηγήσεις 'υψηλού επιπέδου'/περιγραφικές στα Ελληνικά δεν χρειάζονται και θα προσμετρηθούν αρνητικά. Επίσης να εξηγήσετε τι σημαίνει η ιδιότητα μηδενικής γνώσης για τίμιους επαληθευτές (honest verifier zero-knowledge).

(2) Να αποδείξετε οτι το παρακάτω πρωτόκολλο είναι πρωτόκολλο μηδενικής γνώσης για τίμιους επαληθευτές για το διακριτό λογάριθμο x του h βάσει του g στην υποομάδα $\langle g \rangle$ τάξης m της G. (Δηλαδή πρέπει να δείξετε τις τρεις ιδιότητες).

1. Ο prover διαλέγει τυχαία $\rho_1, \ldots, \rho_k$ από το $\mathbb{Z}_m$ και στέλνει τα $\langle y_1, \ldots, y_k \rangle = \langle g^{\rho_1}, \ldots, g^{\rho_k} \rangle$ στον verifier.
2. Ο verifier διαλέγει k bits $b_1, \ldots, b_k$ τυχαία και τα στέλνει στον prover.
3. Ο prover στέλνει στον verifier τις τιμές t_j που ορίζονται σαν $t_j = \rho_j$ αν $b_j = 0$ και $t_j = \rho_j + x$ αν $b_j = 1$.
4. Ο verifier ελέγχει για κάθε $j \in \{1, \ldots, k\}$, αν ισχύει το $(b_j = 0) \rightarrow (g^{t_j} = y_j)$ και αν ισχύει το $(b_j = 1) \rightarrow (g^{t_j} = y_j h)$.

Στην επιχειρηματολογία που θα παραθέσετε μπορείτε να υποθέσετε οτι είναι γνωστό το ακόλουθο (που έχουμε δείξει): αν ένας (κακός) prover είναι πειστικός στον verifier με πιθανότητα α τότε με ένα μόνο rewinding επιτυγχάνουμε δύο πειστικές conversations που έχουν διαφορετική δεύτερη κίνηση με πιθανότητα τουλάχιστον $\alpha^2/4 - 2^{-k}$.

Επώνυμο:
Όνομα:
Α.Μ.:

Άσκηση 4

Η Αλίκη και ο Βασίλης θέλουν να στρίψουν ένα νόμισμα μέσω Internet. Θέλουν να βρούν ένα πρωτόκολλο έτσι ώστε στο τέλος του πρωτοκόλλου να λάβουν ένα bit έτσι ώστε το αποτέλεσμα να είναι κατανεμημένο στο $\{0,1\}$ ομοιόμορφα ακόμη και αν ένας από τους δύο παίκτες δεν ακολουθεί το πρωτόκολλο. Η Αλίκη προτείνει το εξής πρωτόκολλο στο Βασίλη:

1. Η Αλίκη στο πρώτο βήμα διαλέγει μια πολλαπλασιαστική ομάδα G, ένα στοιχείο g τάξης m όπου m πρώτος αριθμός και στέλνει στο Βασίλη τα $\langle G, g, h, m\rangle$ όπου h είναι τυχαίο στοιχείο του $\langle g\rangle$.

2. Ο Βασίλης ελέγχει ότι το m είναι πρώτος αριθμός καθώς και ότι το $g^m = 1$ και $g \neq 1$. Ο Βασίλης διαλέγει $b \in \{0,1\}$ τυχαία και στέλνει στην Αλίκη το στοιχείο $c = g^r h^b$ με r τυχαίο στοιχείο του $\mathbb{Z}_m$.

3. Η Αλίκη καταγράφει το c και στέλνει στο Βασίλη το b' όπου $b' \in \{0,1\}$ το διαλέγει τυχαία.

4. Ο Βασίλης στέλνει στην Αλίκη τα στοιχεία r, b και τερματίζει επιστρέφοντας $(b + b') \bmod 2$.

5. Η Αλίκη ελέγχει ότι $c = g^r h^b$ και $b \in \{0,1\}$ και εάν ισχύει τερματίζει επιστρέφοντας $(b + b') \bmod 2$. Στην άλλη περίπτωση ($c \neq g^r h^b$) η Αλίκη τερματίζει επιστρέφοντας fail.

Να δείξετε τα εξής : (1) Ακόμη και αν η Αλίκη δεν ακολουθεί το πρωτόκολλο, ο Βασίλης, ακολουθώντας το πρωτόκολλο πιστά, είναι σίγουρος ότι η τιμή με την οποία τερματίζει είναι κατανεμημένη τυχαία στο $\{0,1\}$. Υπόδειξη: Για να δικαιολογήσετε την απάντηση σας μπορείτε να υποθέσετε μια οποιαδήποτε συναρτησιακή σχέση $f_A : \langle g\rangle \to \{0,1\}$ που μπορεί να έχει το b' με το c (δηλαδή η f_A αντιπροσωπεύει τον τρόπο που η Αλίκη διαλέγει το b' βάσει του c) και να δείξετε ότι η έξοδος του Βασίλη (που τώρα είναι $(f_A(c) + b) \bmod 2$) εξακολουθεί να είναι τυχαία κατανεμημένη στο $\{0,1\}$. (2) Σε περίπτωση που ο Βασίλης δεν ακολουθεί το πρωτόκολλο, ας υποθέσουμε ότι ο Βασίλης χρησιμοποιεί το πρόγραμμα B το οποίο λειτουργεί σε δύο στάδια ως εξής : με είσοδο $\langle G, g, h, m\rangle$ δίνει ένα c (η πρώτη κίνηση του Βασίλη) και κατόπιν με είσοδο b' επιστρέφει τα r, b (η δεύτερη κίνηση του Βασίλη). Έστω το γεγονός OK ότι το πρόγραμμα B περνάει τον έλεγχο της Αλίκης όταν αυτή ακολουθεί το πρωτόκολλο. Υποθέτουμε ότι $Pr[\text{OK}] = 1$ δηλαδή το πρόγραμμα B απαντάει πάντοτε με τρόπο που Αλίκη δεν κάνει fail.

Έστω ότι το πρόγραμμα B όταν επικοινωνεί με την Αλίκη (που παίζει τίμια) την κάνει να επιστρεψει 1 με πιθανότητα $3/4$, δηλαδή $Pr[(b + b') \bmod 2 = 1] = 3/4$, και έτσι η Αλίκη **δεν εξάγει** ένα τίμιο νόμισμα. Ας υποθέσουμε $Pr[b = 1 | b' = 0] = \alpha$. (2α) Τι πρέπει να ικανοποιεί το α ; (2β) Με τι πρέπει να είναι ίση η δεσμευμένη πιθανότητα $Pr[b = 0 | b' = 1]$; (2γ) Χρησιμοποιώντας το πρόγραμμα B να κατασκευάσετε πρόγραμμα B^* που να λύνει το πρόβλημα του διακριτού λογαρίθμου στην στην ομάδα $\langle g\rangle$ δηλαδή με είσοδο g, h να επιστρέφει x τέτοιο ώστε $h = g^x$. Με αυτό τον τρόπο συμπεραίνουμε ότι το πρωτόκολλο επιτρέπει και στην Αλίκη να είναι σίγουρη ότι και ο Βασίλης δεν μπορεί να κλέψει (αν πιστεύει στη δυσκολία του διακριτού λογαρίθμου).