Σχήματα Δέσμευσης & Diffie Hellman

1. Η Καρολίνα και ο Λυκούργος χρησιμοποιούν το σχήμα δέσμευσης του Pedersen. Η Καρολίνα έχει ορίσει τις παραμέτρους και ο Λυκούργος της έχει στείλει τη δέσμευση c. Πριν γίνει οτιδήποτε άλλο, ο Λυκούργος διαπιστώνει ότι από τυπογραφικό λάθος στις σημειώσεις του, υπολόγισε την τιμή $g^m h^r$ αντί $g^r h^m$. Είναι δυνατό με τις ανάλογες διορθώσεις από τη μεριά της Καρολίνας να συνεχίσουν την επικοινωνία τούς ή πρέπει ο Λυκούργος να δημιουργήσει νέα δέσμευση;

2. Ο Λυκούργος αποφασίζει για καλό και για κακό να δημιουργήσει νέα δέσμευση c' έχοντας διορθώσει το λάθος στον υπολογισμό, αλλά για οικονομία χρόνου επαναχρησιμοποιεί την ίδια τιμή r. Δεδομένου ότι δεσμεύεται στο ίδιο μήνυμα με πριν (άρα και η τιμή m είναι ίδια), είναι σωστή η αποφασή του;

3. Στον πρώτο υποψήφιο ορισμό ασφαλείας για σχήματα ανταλλαγής κλειδιών, αναφέραμε ότι ένα σχήμα που είναι ασφαλές σύμφωνα με τον ορισμό, μπορεί στην πράξη να αποκαλύπτει όλο το κλειδί εκτός από $\log^2(\lambda)$ bits. Εξηγήστε από που προκύπτει το όριο (κατ'ελάχιστο, εξηγήστε γιατί δεν θα μπορούσαμε να αλλάξουμε το όριο σε $\log \lambda$).

4. Στη διάλεξη αναφερθήκαμε στο γεγονός ότι δεδομένης μίας ομάδας $\mathbb{G}$ τάξης q, όπου q πρώτος, παραγόμενη από το g, μια μεταβλητή A που ακολουθεί την κατανομή $K := g^{x \cdot y}$ όπου $x, y \leftarrow \mathbb{Z}_q$ και μια μεταβλητή B που ακουλουθεί την κατανομή $U := g^z$ όπου $z \leftarrow \mathbb{Z}_q$ έχουν μικρή στατιστική απόσταση. Επιβεβαιώστε αυτό τον ισχυρισμό.

5. Κατά τη διαδικασία ανταλλαγής κλειδιού, είναι πιθανό να καταλήξουμε σε ένα κλειδί διαφορετικής μορφής από αυτό που θα θέλαμε να χρησιμοποιήσουμε. Σε ένα παράδειγμα από τις σημειώσεις, η διαδικασία ανταλλαγής κλειδιού μας δίνει ένα τυχαίο στοιχείο του $\mathbb{Z}_q$, ενώ εμείς θα επιθυμούσαμε μια συμβολοσειρά από bits. Διατυπώστε ένα απλό αλγόριθμο για να μετατρέψουμε τον ένα ακέραιο από το 0 ως το $q-1$ σε μια συμβολοσειρά από bits με το μέγιστο δυνατό[1] μήκος. Κατόπιν υπολογίστε τη στατιστική απόσταση των συμβολοσειρών που παράγονται σε σχέση με την ομοιόμορφη κατανομή για το ίδιο μήκος.

6. Σε συνέχεια της προηγούμενης άσκησης, έστω ότι έχουμε κατασκευάσει μία διαδικασία που παράγει συμβολοσειρές s bits μήκους λ σύμφωνα με μια κατανομή S που είναι δ-κοντά στην ομοιόμορφη στο $\{0,1\}^\lambda$. Να δείξετε ότι για ένα οποιοδήποτε ψηφίο s_i $(0 \leq i < \lambda)$ αυτών των συμβολοσειρών, ισχύει ότι η κατανομή που ακολουθεί το ψηφίο, έστω S_i είναι δ-κοντα στην ομοιόμορφη κατανομή στο $\{0,1\}$;

*. Θεωρήστε την εξής παραλλαγή του σχήματος του Pedersen: αντί $h := g^t, t \leftarrow \mathbb{Z}_q$ κατασκευάζουμε δύο παραμέτρους $h_1, h_2 := g^{t_1}, g^{t_2}, t_i \leftarrow \mathbb{Z}_q$ και υπολογίζουμε (για ζεύγος μηνυμάτων m_1, m_2) την δέσμευση ως $c := g^r {h_1}^{m_1} {h_2}^{m_2}$.

   Να εξετάσετε την ασφάλεια της παραλλαγής σε σχέση με το αρχικό σύστημα, πάντα υπό την υπόθεση ότι το DDH είναι δύσκολο.

[1] Δεν μας ενδιαφέρει να προσθέσουμε τετριμμένα bits που θα είναι σταθερά 0 ή 1