Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

1η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 15 Νοεμβρίου 2024

Άσκηση 1. Έστω το affine cipher: $c = \mathsf{Enc}((a, b), m) = (ax + b) \mod 26$.
Υποθέτουμε ότι ο αντίπαλος μπορεί να επιλέξει δύο μηνύματα m_1, m_2 και να αποκτήσει τις κρυπτογραφήσεις τους c_1, c_2 (CPA–Chosen Plaintext Attack).

1. Πώς μπορεί να χρησιμοποιήσει αυτή τη δυνατότητα ώστε να σπάσει το κρυπτοσύστημα; Πώς θα επιλέξει τα m_1, m_2;
2. Έστω ότι για μεγαλύτερη ασφάλεια αποφασίζουμε να χρησιμοποιήσουμε διπλή κρυπτογράφηση με διαφορετικά κλειδιά, δηλαδή:

$$\mathsf{Enc}(((a_1, b_1), (a_2, b_2), m) = \mathsf{Enc}((a_2, b_2), \mathsf{Enc}((a_1, b_1), m))$$

   - Πώς επηρεάζεται ο χώρος των κλειδιών σε μια εξαντλητική αναζήτηση;
   - Είναι το νέο κρυπτοσύστημα πιο ασφαλές;

   Αιτιολογήστε τις απαντήσεις σας.

Άσκηση 2. Να γράψετε πρόγραμμα σε γλώσσα Python, C/C++, ή άλλη γλώσσα της επιλογής σας, με τις συνήθεις βιβλιοθήκες, που να δέχεται ως είσοδο κρυπτοκείμενα κρυπτογραφημένα με Vigenère και να εξάγει τα 5 πιο πιθανά plaintexts και τα αντίστοιχα κλειδιά (ένα από αυτά θα πρέπει να ταυτίζεται με το σωστό κείμενο, με όλα τα γράμματα σωστά). Το πρόγραμμά σας θα πρέπει να εξάγει και τον δείκτη σύμπτωσης καθενός plaintext.
Να εξηγήσετε τις βασικές ιδέες που χρησιμοποιήσατε στον κώδικά σας.

Κρυπτοκείμενο εισόδου (κενά και σημεία στίξης παρέμειναν όπως στο αρχικό κείμενο):

jpig ysthxucwmqs yhw gpmksq aleea sec, zg sisb lbr zqti nvh mgw nhor wj ahk jvqr, irw vwpa mabs mgw ovyabebmk. voiem lx dflvcrl lbr krpvvb egc kqsmgchx, zff mse big xwcyw qqh gnl yleeg sy hl. dbx nb ptrl jpw umeks ujhrtmh,-tmv tpwvvk hmw ovvaqrz vavo xum vhrq fhaa, pi pdfv iiswvx szg zya, irw rhcri gpyl tfvv mg: blht ytleg axtq! ojhx jwyec tg all peioaplwf qj mggw oeqax gnl vosfm jhq ojvq gpsn rzkuifb! jhq lgu crivl gsua xuwy vkaoiiq pmmgwt brgw qr bsxl: xuwy pnmnkwg peod oghvvmh he ljf pvolm zff vj gpi cnmtuil, pew hl pvx omig egt ti, zqrx dsisi, nvh fx kgytrvx. utl yl ejimmdv voir mzxqq ovvaqrz, sgqr jewq mgwg alvvi huwtmpbe egc tnlwfmh mgwg mse qx. en! a ct arivr nx of avahhl, dkri gpi udw voeg pemg ycalrziw sgq typp lhmwa; p rrmh azffz shbwmqwvjlrl xh ssml mg. q ahtdf mevv fxrlqd eal hbrltpfhbi, nmlks xum abrw jhzr wrvd eqyi omghlw lvcbcw bm ljlme nsekq, cuh gpi ingt oecxc bm ljlme zmvgwu. alrziynjg tyfb m wdkelrq qrmn ljl hrmt: tr ljvy qwils ap alr mzxmapn, aumr mggw nsrax udzkuh gpi lds, cuh tqzxrl npkub eerg vv xum rxszgy-abzpw, szqb ikcfxqspa wgiv! ehcg alrm qnrl k ns qwag, zk olr fic, mn ojvq v altkd flwpmrw. adgzw zm, xadf, vosh bvtmiwpp rgi, mgsv jeaax udzqsh rdig szg nvrixxrl jhtcqrxrk ypxuwym dfxf! fymwl szg jyc blts au hfbcx mn gxlvstsp, szca xum atswt tel nphv yqshrv sns gh px, nvh vzjtf iimvrvzgyi gpi kdxnlggqsg nx voc otmlr! dq! alva gno au hknqr znapn xb mqisq kawrtj, tmv bhvnblnrlth mf ikthf ivmao xh aw c tea. blnr tgnea hekzljbwgze'l cgyu-kbqrz.

Η μορφή της εξόδου του προγράμματος θα πρέπει να είναι η εξής:

KEY1 PLAINTEXT1 IC1
KEY2 PLAINTEXT2 IC2
KEY3 PLAINTEXT3 IC3

... (κ.ο.κ. συνολικά 5 το πολύ γραμμές αυτής της μορφής)

Σημείωση: και άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφ'όσον τους αναφέρετε. Για παράδειγμα, η χρήση του online calculator του δείκτη σύμπτωσης που θα βρείτε εδώ: `https://www.dcode.fr/index-coincidence`. Η χρήση Vigenére solver δεν επιτρέπεται.

Άσκηση 3.

1. Σε ένα κρυπτοσύστημα που διαθέτει τέλεια μυστικότητα, είναι αναγκαίο κάθε κλειδί να επιλέγεται με την ίδια πιθανότητα; Είναι αναγκαίο οι χώροι να είναι ισοπληθικοί; Αποδείξτε τους ισχυρισμούς σας.
2. Να αποδείξετε ότι οι παρακάτω προτάσεις είναι ισοδύναμες με τη συνθήκη τέλειας μυστικότητας του Shannon:
   i. $\forall x \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y] = \Pr[C = y | M = x]$
   ii. $\forall x_1, x_2 \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y | M = x_1] = \Pr[C = y | M = x_2]$

Άσκηση 4. Η Αλίκη χρησιμοποιεί το one-time pad και συνειδητοποιεί ότι όταν το κλειδί της είναι το $k = 0^\lambda$ (όλο μηδενικά) τότε $\mathsf{Enc}(k, m) = m$. Δηλαδή το μήνυμα στέλνεται χωρίς καμία κρυπτογράφηση!

Για να αντιμετωπίσει το παραπάνω πρόβλημα, τροποποιεί τον αλγόριθμο παραγωγής κλειδιών του one-time pad ώστε το κλειδί να επιλέγεται ομοιόμορφα από το $\{0,1\}^\lambda \setminus 0^\lambda$. Δηλαδή το κλειδί μπορεί να είναι οποιαδήποτε συμβολοσειρά λ ψηφίων χωρίς όμως να λαμβάνεται υπόψιν η συμβολοσειρά που αποτελείται από λ μηδενικά.
Παραμένει το τροποποιημένο αυτό one-time pad τέλεια ασφαλές; Να αιτιολογήσετε την απάντησή σας.

Άσκηση 5. Ορίζουμε την πολλαπλασιαστική εκδοχή του one-time pad. Συγκεκριμένα αν p πρώτος η κρυπτογράφηση του plaintext m με κλειδί k ($m, k \in \mathbb{Z}_p^*$) ορίζεται ως $\mathsf{Enc}(k, m) = (k \cdot m) \bmod p$.

1. Να ορίσετε τη συνάρτηση αποκρυπτογράφησης.
2. Να αποδείξετε την ορθότητα του συστήματος (ότι δηλαδή κάθε αποκρυπτογράφηση δίνει το σωστό αρχικό μήνυμα).
3. Είναι αυτό το πολλαπλασιαστικό one-time pad τέλεια ασφαλές; Να αιτιολογήσετε την απάντησή σας.

Άσκηση 6.

1. Έστω ότι $2^n - 1$ είναι πρώτος. Να δείξετε ότι n είναι πρώτος.
2. Έστω $p \in \mathbb{N}^+$ ένας περιττός πρώτος και $M_p = 2^p - 1$.
   i. Δείξτε ότι $M_p \equiv 1 \pmod{p}$.
   ii. Δείξτε ότι $p \mid \varphi(M_p)$.
3. Αποδείξτε ότι αν p, q διαφορετικοί πρώτοι, τότε $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
4. Έστω $p > 2$ πρώτος αριθμός. Να δείξετε ότι:
$$\sum_{\beta \in \mathbb{Z}_p^*} \beta = \sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} \equiv 0 \pmod{p}.$$
5. Έστω ακέραιος $n > 2$. Να δείξετε ότι n είναι πρώτος ανν:
$$(n-1)! \equiv -1 \pmod{n}.$$

Άσκηση 7.

1. Έστω $a \in U(\mathbb{Z}_n)$ τάξης k και $b \in U(\mathbb{Z}_n)$ τάξης m. Αποδείξτε ότι ο αριθμός $ab \in U(\mathbb{Z}_n)$ έχει τάξη km αν και μόνο αν $gcd(k, m) = 1$. Ισχύει η ιδιότητα για οποιαδήποτε (πεπερασμένη) αβελιανή ομάδα;
2. Να δείξετε ότι σε μια (πεπερασμένη) αβελιανή ομάδα η τάξη κάθε στοιχείου διαιρεί την μέγιστη τάξη (μεταξύ όλων των στοιχείων της ομάδας).
   Υπόδειξη: μπορεί να σας φανεί χρήσιμη η διαδικασία απόδειξης του ερωτήματος (6.1).

Άσκηση 8. Έστω $\mathbb{Z}_p^*$ με p πρώτο και g ένας γεννήτορας, p, g γνωστά.

1. Αν d ένας ακέραιος που διαιρεί το $p-1$, βρείτε με αποδοτικό τρόπο ένα στοιχείο b του $\mathbb{Z}_p^*$ τάξης d (δηλαδή d ο μικρότερος ακέραιος με $b^d \equiv 1 \pmod{p}$)
2. Πόσα στοιχεία τάξης d υπάρχουν μέσα στο $\mathbb{Z}_p^*$;
3. Πόσους γεννήτορες έχει η κυκλική υποομάδα που παράγει ένα στοιχείο b τάξης d;
4. Πόσες κυκλικές υποομάδες τάξης d υπάρχουν στο $\mathbb{Z}_p^*$;
5. Αν μας δώσουν ένα στοιχείο h, την τάξη του d και ένα τυχαίο στοιχείο a, πώς μπορούμε να δούμε αν το a ανήκει στην υποομάδα που παράγει το h σε πολυωνυμικό χρόνο;

Άσκηση 9. Υλοποιήστε τον έλεγχο πρώτων αριθμών Miller-Rabin σε πρόγραμμα (απαιτείται γλώσσα ή βιβλιοθήκη που να υποστηρίζει πράξεις μεγάλων αριθμών, χιλιάδων ψηφίων). Εφαρμόστε τον για να ελέγξετε τους παρακάτω αριθμούς:
$67280421310721, 170141183460469231731687303715884105 7, 2^{1001} - 1, 2^{2281} - 1, 2^{9941} - 1.$

Bonus Άσκηση (χωρίς αυστηρή προθεσμία)

Το παιχνίδι του σιδεροθρόνου

Πριν από πολλά χρόνια, στον μακρινό τόπο της Βασιλοπροσγείωσης, ζούσε ο Τζοφραίος ο Αντιπαθητικός με τους υπηκόους του. Συνολικά ήταν $2^{19}-1$ άνθρωποι και όλοι τους είχαν από ένα θανάσιμο εχθρό, εκτός από τον Καλικάτζαρο που τον συμπαθούσαν όλοι.

Κάθε ένας από αυτούς είχε ένα προσωπικό μαχαίρι (όλα τα μαχαίρια ήταν διαφορετικά μεταξύ τους) και κάθε ένας από αυτούς είχε τραυματίσει με κάποιο μαχαίρι κάθε έναν από τους υπόλοιπους.Έτσι τελικά όλοι τους τραυματίστηκαν από όλα τα μαχαίρια (ειδικότερα, το μαχαίρι κάθε ανθρώπου χρησιμοποιήθηκε από κάποιον για να τον τραυματίσει).

Ο Καλικάτζαρος, τον οποίο κάθε άτομο τραυμάτισε με κάποιο μαχαίρι, είχε ένα μαχαίρι που ο καθένας χρησιμοποίησε για να τραυματίσει τον εαυτό του. Επίσης, ο Καλικάτζαρος τραυμάτισε κάθε άνθρωπο με το μαχαίρι του θανάσιμου εχθρού του ανθρώπου αυτού και μιας και ο ίδιος δεν είχε θανάσιμο εχθρό, αυτοτραυματίστηκε με το ίδιο του το μαχαίρι.

Για κάθε τριάδα ανθρώπων, ο άνθρωπος που τραυμάτισε τον τρίτο χρησιμοποιώντας το μαχαίρι αυτού που τραυμάτισε τον δεύτερο με το μαχαίρι του πρώτου, είναι ο ίδιος άνθρωπος που χρησιμοποίησε το μαχαίρι του πρώτου για να τραυματίσει αυτόν που τραυμάτισε τον τρίτο με το μαχαίρι του δεύτερου.

1. Αν η Δρακομάνα ήταν αυτή που τραυμάτισε τον Γιάννη τον Χιονιά με το μαχαίρι του Τζοφραίου του Αντιπαθητικού, ποιος τραυμάτισε τον Τζοφραίο τον Αντιπαθητικό με το μαχαίρι του Γιάννη του Χιονιά;

2. Αν ξέρουμε ότι η Δρακομάνα και ο Τζοφραίος ο Αντιπαθητικός είναι θανάσιμοι εχθροί, ποιος τραυμάτισε την Δρακομάνα, με το μαχαίρι της;

3. Ποιος χρησιμοποίησε το μαχαίρι αυτού που τραυμάτισε τον Γιάννη τον Χιονιά με το ίδιο του το μαχαίρι, για να τραυματίσει αυτόν που τραυμάτισε τον Τζοφραίο τον Αντιπαθητικό με το ίδιο του το μαχαίρι;

Υπόδειξη: όσο περίεργο και αν σας φαίνεται η άσκηση επιδέχεται μια αυστηρά μαθηματική λύση. Δοκιμάστε να την βρείτε χωρίς να δείτε την υποσημείωση. [1]

Σύντομες οδηγίες: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητ(ρι)ές 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*. Για την βαθμολόγηση, θα σας ζητηθεί να παρουσιάσετε σύντομα κάποιες από τις λύσεις σας.

Καλή επιτυχία!

[1] Προσπαθήστε να ορίσετε μια κατάλληλη πράξη ομάδας που να εκφράζει το ότι ο τραυματίστηκε τον y με το μαχαίρι του z.