Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

1η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 23 Νοεμβρίου 2025

Άσκηση 1. 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 2. 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 3. 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 4. 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 5. Αποδείξτε ότι για κάθε θετικό ακέραιο $n = p_1^{e_1} \cdots p_k^{e_k}$ και κάθε $a \in \mathbb{Z}_n^*$,

$$a^{\lambda(n)} \equiv 1 \pmod{n},$$

όπου $\lambda(n) = \text{lcm}(\phi(p_1^{e_1} \cdots \phi(p_k^{e_k})$.
Εξηγείστε γιατί το παραπάνω αποτελεί γενίκευση το θεωρήματος του Euler.
Αποδείξτε ότι αν n αριθμός Carmichael, τότε έχει τουλάχιστον 3 πρώτους διαιρέτες και είναι "square-free" (για κάθε πρώτο p, το p^2 δεν διαιρεί το n).

Άσκηση 6. Έστω p, q, n όπως στη γεννήτρια Blum-Blum-Shub (p, q πρώτοι με $p \equiv q \equiv 3 \pmod{4}$). Δείξτε ότι κάθε τετραγωνικό υπόλοιπο $a \in \mathbb{Z}_n^*$, έχει ακριβώς μία ρίζα που είναι επίσης τετραγωνικό υπόλοιπο. (Υπόδειξη: Είναι το -1 τετραγωνικό υπόλοιπο mod$p$ ή mod$q$;)
Τι συμπεραίνετε για τις ακολουθίες τετραγώνων που παράγονται από την γεννήτρια Blum-Blum-Shub;

Άσκηση 7. Δείξτε ότι η κατασκευή $F : \{0,1\}^n \times \{0,1\}^{t(n)} \to \{0,1\}^n$ από $G : \{0,1\}^n \to \{0,1\}^{n2^{t(n)}}$ (σελ. 23 των διαφανειών) είναι ψευδοτυχαία συνάρτηση αν η G είναι ψευδοτυχαία γεννήτρια.

Άσκηση 8. Έστω $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ ψευδοτυχαία συνάρτηση. Εξετάστε τις παρακάτω συναρτήσεις ως προς την ψευδοτυχαιότητά τους:

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

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 y που να εκφράζει το ότι ο x τραυμάτισε τον z.