Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

1η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 10 Νοεμβρίου 2023

Άσκηση 1. Παρακάτω δίνεται ένα κρυπτοκείμενο της Αγγλικής κρυπτογραφημένο με τη μέθοδο της αντικατάστασης (substitution cipher).

```
KVU HQBINKWALU DNBAURG BWO AU YUGHRCAUY ARCUPLO WG KVU RUWL DNBAURG ZVQGU
UTIRUGGCQDG WG W YUHCBWL WRU HWLHNLWALU AO PCDCKU BUWDG. WLKVQNJV KVU GNAEUHK
QP KVCG IWIUR CG QGKUDGCALO KVU HQBINKWALU DNBAURG. CK CG WLBQGK UFNWLLO
UWGO KQ YUPCDU WDY CDXUGKCJWKU HQBINKWALU PNDHKCQDG QP WD CDKUJRWL XWRCWALU
QR W RUWL QR HQBINKWALU XWRCWALU, HQBINKWALU IRUYCHWKUG, WDY GQ PQRKV. KVU
PNDYWBUDKWL IRQALUBG CDXQLXUY WRU, VQZUXUR, KVU GWBU CD UWHV HWGU, WDY C VWXU
HVQGUD KVU HQBINKWALU DNBAURG PQR UTILCHCK KRUWKBUDK WG CDXQLXCDJ KVU LUWGK
HNBARQNG KUHVDCFNU. C VQIU GVQRKLO KQ JCXU WD WHHQNDK QP KVU RULWKCQDG QP KVU
HQBINKWALU DNBAURG, PNDHKCQDG, WDY GQ PQRKV KQ QDU WDQKVUR. KVCG ZCLL CDHLNYU W
YUXULQIBUDK QP KVU KVUQRO QP PNDHKCQDG QP W RUWL XWRCWALU UTIRUGGUY CD KURBG
QP HQBINKWALU DNBAURG. WHHQRYCDJ KQ BO YUPCDCKCQD, W DNBAUR CG HQBINKWALU
CP CKG YUHCBWL HWD AU ZRCKKUD YQZD AO W BWHVCDU. C JCXU GQBU WRJNBUDKG ZCKV
KVU CDKUDKCQD QP GVQZCDJ KVWK KVU HQBINKWALU DNBAURG CDHLNYU WLL DNBAURG
ZVCHV HQNLY DWKNRWLLO AU RUJWRYUY WG HQBINKWALU. CD IWRKCHNLWR, C GVQZ KVWK
HURKWCD LWRJU HLWGGUG QP DNBAURG WRU HQBINKWALU. KVUO CDHLNYU, PQR CDGKWDHU,
KVU RUWL IWRKG QP WLL WLJUARWCH DNBAURG, KVU RUWL IWRKG QP KVU MURQG QP KVU
AUGGUL PNDHKCQDG, KVU DNBAURG IC, U, UKH. KVU HQBINKWALU DNBAURG YQ DQK,
VQZUXUR, CDHLNYU WLL YUPCDWALU DNBAURG, WDY WD UTWBILU CG JCXUD QP W YUPCDWALU
DNBAUR ZVCHV CG DQK HQBINKWALU. WLKVQNJV KVU HLWGG QP HQBINKWALU DNBAURG
CG GQ JRUWK, WDY CD BWDO ZWOG GCBCLWR KQ KVU HLWGG QP RUWL DNBAURG, CK CG
DUXURKVULUGG UDNBURWALU. C UTWBCDU HURKWCD WRJNBUDKG ZVCHV ZQNLY GUUB KQ IRQXU
KVU HQDKRWRO. AO KVU HQRRUHK WIILCHWKCQD QP QDU QP KVUGU WRJNBUDKG, HQDHLNGCQDG
WRU RUWHVUY ZVCHV WRU GNIURPCHCWLLO GCBCLWR KQ KVQGU QP JQYUL. KVUGU RUGNLKG
VWXU XWLNWALU WIILCHWKCQDG. CD IWRKCHNLWR, CK CG GVQZD KVWK KVU VCLAURKCWD
UDKGHVUCYNDJGIRQALUB HWD VWXU DQ GQLNKCQD.
```

Γράψτε κώδικα σε Python, C, C++, Java, ή άλλη γλώσσα της επιλογής σας (πχ. Haskell) που θα σας βοηθήσει να σπάσετε τον κρυπτοκείμενο. Ποιο είναι το αρχικό κείμενο, και ποιο το κλειδί που χρησι-

μοποιήθηκε; Δείξτε τον κώδικα που αναπτύξατε (άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφ' όσον τους αναφέρετε).

Άσκηση 2. 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.

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:

$$\mathsf{Enc}(k, m) = \mathsf{Enc}(k_2, \mathsf{Enc}(k_1, m))$$

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

   Αιτιολογήστε τις απαντήσεις σας.

Άσκηση 3. 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 το πολύ 10 πιθανά plaintexts και τα αντίστοιχα κλειδιά (ένα από αυτά θα πρέπει να αντιστοιχεί ακριβώς στο σωστό, 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:

ZL CXCEB IHRDF YR VYC QKWQR YJ C ICKHZXASSP ZL RKMSAYKTRNWR. HKL NIXVJDIAHUD SH
TFTTD GPQMVRJ WTFGDKVG YYH YFHLN MV WPDF HKL NIUZEC EWPPDEVZMCL CI TOGJRLXVOO
JYQRLRXGU DUN FTFSVAH WOO GQJR DY VLNR KTRBT VFBWDSIIYEAWF KOZKTCH WCZU
DS YYCGX HKLI GCE ZT NGHK SR ULAW VCPTOVEZYA TDSSSGCKGDGG DZ BIOFRT VOVO
NMUGCCLSUZ KRF TMBIIWLB XGIKXGOOZ. SR VLPC, LIFO KTRCGRTHLVXW EICPMS D UOIF
WMG GSZ AITGJ MU VFBWDSIIYEAWF ZIWVVKH PVLJR QKEGBBNH ARI PVATLGLAI SH JCRNFH
ROC FZQIKWEBDMQE AWTBQLVW CEB HNDSSI XJV CFNWYHVIPK MU T KUPDXGE QXZBDAEVG. RR
IAS VHWI VZKT, MVHVBIVZAPE RHCOPQGKTGHV PX MPWMGFOWPYR VYCDKM DUN GQDNJMSU
ZMMGEAT LVRD ZVQDGHX CI WBSXZBXGU SYYZCSJN LSFBBI EIWEMCVFCXGDQ, RAOQNSRI
KFXL OQJSIPK YGM WQAY E UTGTGQH. ARI FVTTECSTORV FD RHASBDIT TMCMFRSVIF
TMBFIQPMEVZMC GSWDYVMJ NGHALZOW GWDDKHOLCW CEB XGSAWORUZTT VCQAKGV SCIPSHU
ZIQGJT HF FVWTWKCGL CQ VZTQJGIX GLKOW QW RWX KRYVH, TVNATQLUQ QQJR BTWO
HXH ORLN XLFBBWKFLH PWWO DINVADFAXUSGCKGDGG. IVB QCEW PIDOPMEVZMCL HKLCI
EFLITQWZ WYUK ZT FOGL CIELPT TUDPXWV SMIA SDCOWFIMEIWQN KRF KFT BBMLMXKFL DY
WOSOKKKGBTHH TOWURETL. OW WBIUVLI, ACZLFIT, KFT LCOBDMQE MU LSFBBMVP NGHPOLWW
NREH PSOS LIJZLS HHKLB ETVYH HT FVWQWEGRTHLVXW VVAWGCOVQC. EFLIXASVBETP
AGRDWVQVCGFN BG XUKFNV RD FSHA DLG ICFNWULWIPKQ, XG HKHD MVJ SHX KRBVH
KDNDLS VBML UVTTKS LUMSPMCCBSQJOW QE RWX GBZDIO LQTKG, DZ DS GCGBBBDAO QCEW
DY HKL LIPVDXMG RM DINVNGHQHZCMPX. RWX PHZD OPFUC VFBWDSIIYEAWF WBSDCCB BG
WOKX QW NGBJDJI: TTVTTGHLUQ XJV SCTIWOYVKQCS XLWYKGVZMC HT LUPSTDYIBCQ MBSO
TMBFIQPMEVZMCL CYLB EP ZLHXQXYO GJRLCXZ. LU YVFVP IH IVL MVAGRDZFDWRC VF CCLIUL
ZVKMYRR, VRDOZGI, GI BG FBBVGERAR BHJOWURPN YCU ARI EFKBNBLJKXKEE ETFWPOW VF
QWTFH H UIA NFXVV LZ URQNL IH BR VXI GCQT. MVLZ SW FFLT UM VLXHKEE IAS NLI MP
RBKTBFL YZGI QDFS VLMYTV AWTBQLV WWTF PL DUPFEVV ADNFLLB ST ICVBGWLBIF DYXE.
O SYSZCKC RHBYLBWCKGDG PHAGIGE RLH DHVZPG NGIA BR WBMQI YRJIDPXXCEAT BG D
JYQOFL DVQXYBIPTC XG PXZSRGJQ, WHKHCOV, CEB XM WV BXVGRJXLHLJ DS GONTVH LUSXKRJ
QNGLUOWU TMCMOFAC XQ SC EHGWWYRGU JDGU HUYYIY DDK YHFC XQ SC IKOQZWMVKCS
UM VVWI RYWHBQDS WICEQ. IAS FVCX CEB SXZDF SQRFQTW PB ARMU BCN WWVABMDLRXHB
SYYFNVK XL O PHTST SYGKWHY DS VYC IKOQZPIT FD QNGLUOWU TMBFIQPMEVZMCL HR SKVIV
RTESSYYGGJQXGU QLDAQIIH.

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

KEY1 PLAINTEXT1 IC1
KEY2 PLAINTEXT2 IC2
KEY3 PLAINTEXT3 IC3
KEY4 PLAINTEXT4 IC4

... (κ.ο.κ. συνολικά 10 το πολύ γραμμές αυτής της μορφής)

Σημείωση: 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 4.

1. Σε ένα κρυπτοσύστημα που διαθέτει τέλεια μυστικότητα, είναι αναγκαίο κάθε κλειδί να επιλέγεται με την ίδια πιθανότητα; Έχει σημασία αν οι χώροι 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 5. 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 6. 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. Παραμένει το τροποποιημένο αυτό one-time pad τέλεια ασφαλές; Να αιτιολογήσετε την απάντησή σας.

Άσκηση 7.

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 $p \mid \varphi(M_p)$.

Άσκηση 8.
Αποδείξτε ότι αν p, q διαφορετικοί πρώτοι, τότε $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Άσκηση 9. Έστω $p > 2$ πρώτος αριθμός. Να δείξετε ότι:

$$\sum_{\beta \in \mathbb{Z}_p^*} \beta = \sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} \equiv 0 \pmod p.$$

Άσκηση 10.

1. Να δείξετε ότι για $n > 3$ και $m = \lfloor \sqrt{n} \rfloor$, ο n είναι πρώτος αν και μόνο αν $\sum_{j=1}^{m} \gcd(n, j) = m$.
2. Να σχεδιάσετε αλγόριθμο ελέγχου πρώτων αριθμών βάσει του κριτηρίου, να υπολογίσετε την πολυπλοκότητα του και να τη συγκρίνετε με την πολυπλοκότητα του αλγορίθμου που αναζητά όλους τους πιθανούς διαιρέτες έως $\sqrt{n}$ και του αλγορίθμου Miller-Rabin.

Άσκηση 11. Έστω $n \in \mathbb{N}^+$ και το σύνολο:

$$L_n = \{\alpha \in \mathbb{Z}_n^+ : \quad \alpha^{n-1} = \alpha^{t2^h} = 1, t \text{ περιττός, και} \\ \text{αν } \alpha^{t2^{k+1}} = 1 \text{ τότε } \alpha^{t2^k} = \pm 1 \text{ για } k = 0, \ldots, h-1.\}.$$

Να δείξετε ότι αν n είναι πρώτος τότε $L_n = \mathbb{Z}_n^*$.

Άσκηση 12. Έστω $(\mathbb{G}_1, +_1)$ και $(\mathbb{G}_2, +_2)$ αβελιανές ομάδες και $\mathbb{B}$ μια υποομάδα του $(\mathbb{G}_1 \times \mathbb{G}_2, +)$, όπου η πράξη $+$ ορίζεται ως:

$$(a_1, b_1) + (a_2, b_2) = (a_1 +_1 a_2, b_1 +_2 b_2)$$

Έστω ακόμη

$$\mathbb{B}_1 = \{a_1 \in \mathbb{G}_1 : (a_1, b_1) \in \mathbb{B} \text{ για κάποιο } b_1 \in \mathbb{G}_2\}.$$

Δείξτε ότι $\mathbb{B}_1$ είναι υποομάδα του $\mathbb{G}_1$.

Άσκηση 13. 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 14. Υλοποιήστε τον έλεγχο πρώτων αριθμών Miller-Rabin σε πρόγραμμα (απαιτείται να υποστηρίζονται πράξεις μεγάλων αριθμών, χιλιάδων ψηφίων). Εφαρμόστε τον για να ελέγξετε τους παρακάτω αριθμούς:

$67280421310721, 170141183460469231731687303715884105 7, 2^{1001}-1, 2^{2281}-1, 2^{9941}-1, 2^{19939}-1$

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*. Ενδεχομένως να σας ζητηθεί να παρουσιάσετε σύντομα κάποιες από τις λύσεις σας.

Καλή επιτυχία!

[1] Προσπαθήστε να ορίσετε μια κατάλληλη πράξη ουράνιας τόξου ώστε το ότι ο x τραυμάτισε τον y με το μαχαίρι του z.