Kriptográfia 2. gyakorlat

1. * Aki szereti a kihívásokat, annak ajánlom Simos Singh: The Code Book c. könyvének fealdványait.

   `http://www.simonsingh.net/Cipher_Challenge.html`

   Igaz, már megfejtették őket, megoldás a fenti weblapon, a 10 feladványból van nagyon könnyű és nagyon nehéz is.

2. [Caesar/SHIFT titkosító] ,,Törjük fel" az alábbi üzenetet (az üzenet ékezetmentes magyar nyelvű):

   Xnwaf otxxe f anqflwf jx ptwzqtyyji rnsijsnp rtxtqdtl, nldjpjee zld jqsn, mtld rtxtqdtlaf yfateefq jx ptwzqtyyji rnsijspn xnwots. (Mnsiz ptertsifx)

3. [Egyábécés helyettesítés] Törjük fel az alábbi üzenetet (az üzenet ékezetmentes magyar nyelvű):

   http://www.inf.u-szeged.hu/ zlnemeth/crypto/3feladat.txt

4. Vegyük a 26 betűs ábécét, legyen $k = (a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$. Tekinsük a

   $$e_{(a,b)}(x) = (ax + b) \mod 26$$

   affin függvényt.

   a) Milyen kikötést kell tennünk a-ra és b-re, hogy a függvény injektív (ezért titkosításra alkalmas) függvény legyen?

   b) Általánosítsuk válaszunkat 26 helyett tetszőleges m betűs ábécére!

   c) Hány injektív affin függvény van (tetszőlesges m-re)? Így hány különböző affin kulcs van 26 betűs ábécé esetén?

5. [Stallings 2.3] Egy, a 26 betűs ékezetek nélküli ábécé feletti angol szöveget az affin titkosítóval titkosítottunk. A rejtjelezett szöveg leggyakoribb betűje 'B', a második leggyakoribb pedig 'U'. Mi a titkosítás kulcsa? (Az angolban a leggyakoribb az 'e', második leggyakoribb a 't' betű.)

6. [Stallings 2.9] Miután 1943 augusztus 2-án, a PT-109 nevű amerikai őrhajót Lieutenant John F. Kenedy (későbbi elnök) paracsnoksága alatt elsüllyesztette egy japán romboló, az ausztrál rádióállomáson a következő Playfair kóddal titkosított üzenetet vették:

   ```
   KXJEY  UREBE  ZWEHE  WRYTU  HEYFS
   KREHE  GOYFI  WTTTU  OLKSY  CAJPO
   BOTEI  ZONTX  BYBWT  GONEY  CUZWR
   GDSON  SXBOU  YWRHE  BAAHY  USEDQ
   ```

   A titkosítás kulcsa ,,Royal New-Zealand Navy". Fejtsük meg az üzenetet. (A pontot, vesszőt X-szel heyettesítették. Adatátviteli hibák lehetségesek!

7. [Stallings 2.10]

   a) Konstruáljunk Playfair mátrixot a ,,largest" kulcsszóval.

   b) Konstruáljunk Playfair mátrixot a ,,occurrence" kulcsszóval.

8. [Stallings 2.11]

   a) A következő Playfair mátrix használatával titkosítsunk:

   ```
   M F H  I/J K
   U N O   P  Q
   Z V W   X  Y
   E L A   R  G
   D S T   B  C
   ```

   Nyílt szöveg: ,,Must see you over Cadogan West. Comming at once.

   b) Ismételjük meg a títkosítást az előző feladat a) részének mátrixával.

   c) Mit tapasztalunk? Mi a probléma magyarázata? Általánosíthatjuk a következtetésünket?