Kriptográfia 3. gyakorlat

1. Képezzünk két 10 hosszúságú permutációt a

   K_1 =,,NEM SZUPERBIZTOS" és a

   K_2 =,,EZ A MEGOLDÁS"

   kulcsokból a betűk **első** előfordulásainak ábécé sorrendje alapján. (Ehhez az ékezeteket vegyük figyelmbe, de a szóközöket ne.) Ezután titkosítsuk duplén keverő (duble transposition) titkosítással az alábbi szövet, majd fejtsük is vissza. Az egyszerűség kedvéért a táblázat utolsó üres sorár ‚X' karakterrel töltsük fel.

   ```
   ENNEK A BETUIT JOL OSSZEKEVERJUK
   ```

2. Fejtsük vissza az előző feladat szerint a

   K_1 =,,DUPLÁN KEVERŐ" és a

   K_2 =,,TITKOSÍTÁSI MÓDSZER"

   kulcsokkal készült alábbi rejtjelezett szöveget:

   ```
   ZOLEA XSIZE
   HSRNK ANENK
   XXMTC IEEKL
   ```

   A megfejtésnél természetesen visszafele kell dolgozni előbb a második, majd az első pemutációnak megfelelő oszlopokba kell a szöveget beírni, amit soronként kell kiolvasni.

3. Oldjuk meg az előző két feladatot a CrypTool segítségével is. Vigyázat: a CrypTool a szavakból a permutációkat más (jobb) algoritmussal származtatja, ezért nekünk kell a permutációkat kiszámolni és azt számokkal beírni.

4. [Stallings 2.18] A Vigenér titkosító használatával titkosítsuk az "explanation" szót a ,,leg" kulccsal.

5. [Stallings 2.19] Ez a feladat a one-time pad (egyszeri hozzáadásos) módszer verzióját mutatja be a Vigenére titkosítónak. Ebben az esetben a kulcs 0 és 25 kötötti számok véletlen sorozata. Például, ha a kulcs 3 19 5 ..., akkor a nyílt szöveg első betűjének titkosítása eltolás 3 betűvel, a második betűi eltolás 19 betűvel, a harmadiké eltolás 5 betűvel, és így tovább.

   a) Titkosítsuk a ,,sendmoremoney" nyíltszöveget a

   K_1 = 9 0 1 7 23 15 21 14 11 11 2 8 9

   kulccsal.

   b) Az a) részben kapott rejtelezett szöveg felhasználásával találjunk olyan másik K_2 kulcsot, mellyel a rejtjelezett szöveg a ,,cashnotneeded" nyíltszöveggé fejthető vissza.