Criptografie și securitate CTI

Laborator 3

1. Considerați cifrul Nihilist.

   (a) Cifrați mesajul "THEORY IS IMPORTANT" utilizând cheia $k =$ CIPHER pentru construcția alfabetului și KEY pentru cifrarea efectivă. Explicați cum se realizează cifrarea mesajelor.

   (b) Descifrați mesajul "90 54 49 45 84 44 57 54 59 64 85 66 56" utilizând cheia DECRYPT pentru reconstrucția alfabetului și SPRING pentru descifrarea efectivă. Explicați cum se realizează descifrarea mesajelor.

   Link suplimentar: `https://en.wikipedia.org/wiki/Nihilist_cipher`

2. Considerați cifrul Bifid.

   (a) Cifrați mesajul "BAZA CAPTURATA" utilizând cheia $k =$ CIPHER (și grupuri de câte 5 litere).

   (b) Descifrați mesajul "DRQQEKDSFPQHHELPQX" utilizând cheia $k =$ CIPHER (și grupuri de câte 5 litere).

   Link suplimentar: `https://en.wikipedia.org/wiki/Bifid_cipher`

3. Considerați cifrul Trifid.

   (a) Cifrați mesajul "ORDIN NATIONAL" utilizând cheia $k =$ FACULTATE (și grupuri de câte 5 litere). Explicați cum se realizează cifrarea mesajelor.

   (b) Descifrați mesajul "SBFRMSUYYXWGYWY" utilizând cheia $k =$ FACULTATE (și grupuri de câte 5 litere).

   Link suplimentar: `https://en.wikipedia.org/wiki/Trifid_cipher`

4. Considerați sistemul de cifrare Hill 2x2.

   (a) Cifrați mesajul "TODAY IS A GOOD DAY" utilizând cheia de cifrare $\begin{pmatrix} J & B \\ V & I \end{pmatrix}$.

   (b) Descifrați mesajul "KKAXNGQSPKGQ" utilizând cheia de cifrare $\begin{pmatrix} B & E \\ S & T \end{pmatrix}$.

   Link suplimentar: `https://en.wikipedia.org/wiki/Hill_cipher`

5. Considerați sistemul de cifrare RAILFENCE.

   (a) Cifrați mesajul "VREME FAVORABILA PENTRU ATAC" utilizând cheia $k = 3$.

(b) Decriptați următorul mesaj cifrat c = ATARICCEENCFUESIEUSRIUIRLTRMMCIO folosind cheia $k = 4$.

Link suplimentar: `https://en.wikipedia.org/wiki/Rail_fence_cipher`