Criptografie și securitate CTI

Laborator 5

Sistemul de cifrare One Time Pad (OTP) pe biţi

1. (a) Folosind sistemul OTP și codul ASCII, criptați primele 2 litere din numele vostru folosind cheia $k = 0100\ 1110\ 0110\ 1000$;

   (b) Decriptați mesajul cifrat $c = 1101\ 1111\ 0101\ 1011$ utilizând cheia $k = 1001\ 1101\ 0010\ 1101$.

   (c) Ce cantitate de date se poate cifra utilizând OTP cu o cheie de 1GB dacă se dorește păstrarea securității perfecte? De ce?

   (d) Proprietățile de confuzie și difuzie sunt satisfăcute?

2. Se poate construi un criptosistem similar cu OTP dar înlocuind operația XOR cu AND? Dar cu operația OR? Dar cu operația NOT?

3. (a) Folosind un tool online, decriptați ciphertextul c folosind cheia k, unde

   $$c = 0\text{x}6469f6670de9dd7e420264417a833151557b60a529f970833215425306014d,$$
   $$k = 0\text{x}211f93476cc9b410366716221ff34530215b0dc05a981af65e352330736c63.$$

   (b) Determinați cheia care duce ciphertext-ul anterior în mesajul $m =$ "OTP=Criptosistem perfect sigur!".

   (c) Arătați matematic cum poate Eve să găsească mesajul m_2 dacă știe că Alice refolosește aceeași cheie în criptosistemul OTP. De asemenea, Eve cunoaște și textul cifrat c_2 aferent mesajului m_2 și încă o pereche (m_1, c_1) la care știe că a fost folosită aceeași cheie în procesul de criptare.

Generatoare de numere (pseudo)aleatoare

1. *a*) Considerați generatorul liniar congruențial (LCG) definit prin $x_{n+1} = 3 \cdot x_n + 4 \pmod 8$ şi $x_0 = 0$. Generaţi o secvenţă de numere utilizând acest LCG. Este acesta un generator sigur din punct de vedere criptografic? Ce se întâmplă dacă $x_0 = 5$?

   b) Considerați generatorul liniar congruențial (LCG) definit prin $x_{n+1} = 3 \cdot x_n + 4 \pmod{15}$ şi $x_0 = 1$. Generaţi o secvenţă de numere utilizând acest LCG. Este acesta un generator sigur din punct de vedere criptografic?

2. *i*) Considerați un *linear feedback shift register* (LFSR) potrivit schemei din Figure 1. Fie x_i intrările inițiale pentru R_i, $0 \leq i \leq 3$, conform Table 1. Care sunt primii 8 biți de ieșire?

   Arătați că secvența de ieșire este definită de stările inițiale și de formula recursivă $x_{i+4} = x_{i+3} \oplus x_i$ și determinați periodicitatea șirurilor rezultate.

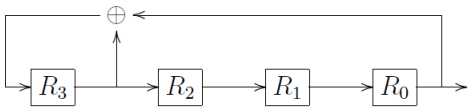

Figure 1: LFSR - exercițiul 4

	x_3	x_2	x_1	x_0
a)	0	1	1	0
b)	1	1	1	0

Table 1: Stări inițiale R_i - exercițiul 4

ii) Implementați un LFSR în care numărul stărilor să poată fi ales. Folosiți acest program pentru a crea un LFSR cu 10 stări și găsiți un *seed* care să dezvolte un șir de perioadă maximă.