SISTEME DE CRIPTARE MODERNE

OTP

I. Descrierea sistemului de criptare OTP. Securitate perfecta.

II. Criptati textul de mai jos aplicand operatia XOR. (Encrypt/Decrypt -> Symmetric(classic) -> XOR)

Mesaj clar: dftv
Cheie: 01

Cum s-a realizat criptarea?
Comparati mesajul clar si mesajul criptat. Ce observati?

III. Care este paradoxul sistemului de criptare OTP?

IV. Cunoscand perechea de mesaj clar – mesaj criptat de mai jos (m, c), cum poate afla Oscar mesajul clar corespunzator lui c' ? (Mesajele m si m' au fost criptate cu aceeasi cheie)

m : 7A 69 64
c : 7B 68 65
c' : 7B 60 73

V. Maleabilitate.
Alice trimite o suma de bani catre Bob conform schemei de mai jos.
Mesajul care contine suma de bani este criptat cu OTP.
Oscar este prieten cu Bob si doreste sa mareasca suma.
Cum procedeaza?

Banca A ---------- c ---------- Banca B
Alice Bob

m = 38
k = 55

Oscar modifica c in c' = 6C

PRG

VI. Descrierea PRG.

VII. Aplicati un test de frecventa pentru mesajele de mai jos.
Analysis -> Analyze Randomness -> Frequency Test

1. G'(s) = G(s) || 00 00 00 00 00 00 00 00 00 00 stiind ca G este PRG

75 65 69 72 79 6A 68 66 76 67 64 6B 6A 69 64 6A 66 64 62 79 68 61 51 4B 51 57 4A 40 00 00 00 00 00 00 00 00 00

2. G'(s) = G1(s) || G2(s) Stiind ca G1 si G2 sunt PRG

6A 75 79 72 67 68 6F 70 66 62 76 75 6A 68 72 64 65 61 6C 69 77 6E 6A 6F 77 77 77 72 6B