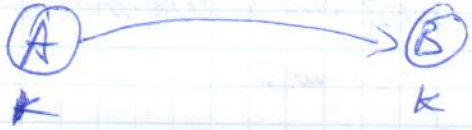
Decriptare:

$$\begin{cases} c_i = F_K(m_i \oplus c_{i-1}) & c_{i-1} \rightsquigarrow m_{i-1} \\ m_i = F_K^{-1}(c_i) \oplus c_{i-1} \end{cases}$$

Metodele CBC, OFB, CTR – nu sunt în forma actuală CCA sigure. ; pot fi modificate să a fi făcute sigure.

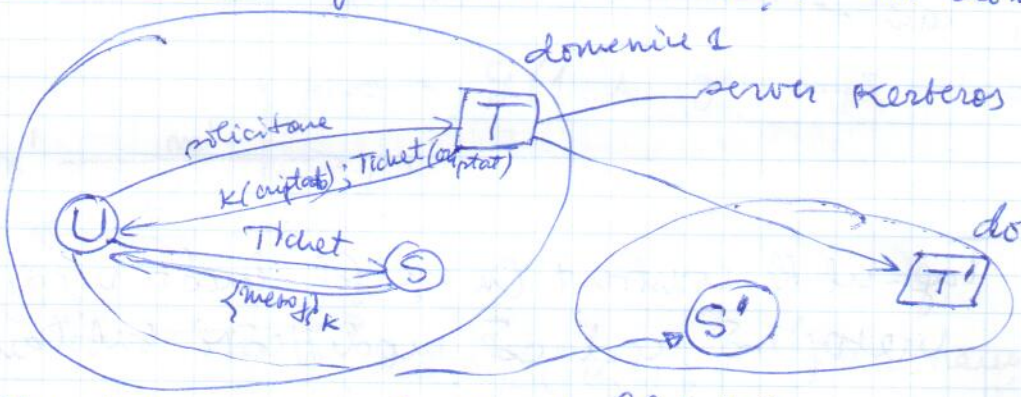


problema distribuției cheii
cum ajung A și B să aibă aceeași cheie de criptare?

→ a luat naștere criptografia cu chei publice

→ protocoale de distribuție a cheii → KDC = centru de distribuție a cheilor -

→ Kerberos = protocolul deservește un domeniu



Ticketul = criptat ai doar S îl înțelege -

- Ticketul conține accesul cheie K pe care a primit-o și u

dacă ∃ mai multe domenii → fiec dom. fiind deservit de către un server Kerberos, atunci accesul lui U spre S' se face prin deservirea Kerberos din dom propriu ce utilizează serviciile serverului Kerberos din primul domeniu.

Săptămâna de la 10 – recuperare curs – C11?.