CTR - counter →

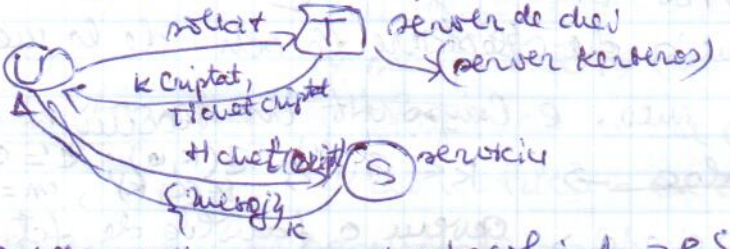
$m = m_1 \cdot m_2 \cdots m_l$

$r_0 \xrightarrow{F_K(r_0+1)} r_1 \longrightarrow r_2 = I_K(r_0+2)$

$c_i = m_i \oplus F_K(r_0+i)$

r_0 = random
F_K = pseudorandom. } metodo CPA sigură.

De ați făcute CPA sigure? → problema distribuției cheii →
→ Criptografia cu chei publice →
Centrul de distribuție de chei → Kerberos Protocol.



Diffie Hellman → protocol: $A \to B \{ x \leftarrow \{2 \cdots (p-2)\}, a^x \}$
$B \to A \; y \leftarrow \{2 \cdots (p-2)\} \to a^y$

Scop: A și B stabilesc materialul de chei (a^{xy})
Vulnerabilitate man in the middle.

STS → p = nr prim are, α = rădăcină primitivă publică modulo p; $sig_x(m)$ e semnătura RSA a lui x pe o valoare hash a lui m →

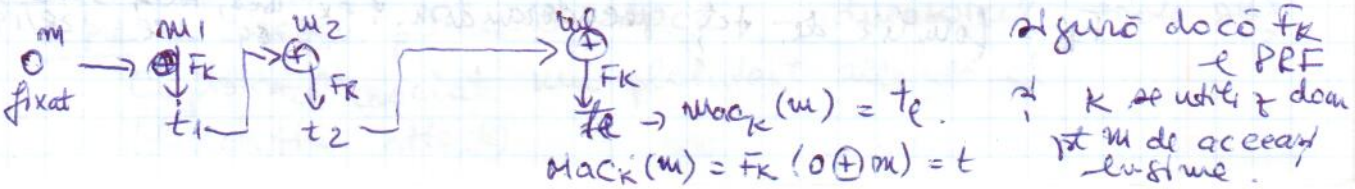
Protocol: $A \to B \; (\alpha^x)$, cu x ales între 2 și p-2
$B \to A \; \alpha^y$, cu $\{sig_B(\alpha^y, \alpha^x)\}_K$
$A \to B \; \{sig_A(\alpha^x, \alpha^y)\}_K$

$K = \alpha^{xy}$

a^{xy} = material de chei.

Proprietăți: autentificare mutuală a entităților.
și autentificare mutuală explicită a cheilor

MAC = message authentification code.
Schemă de autentificare: triplet $\Pi(G, Mac, V)$
gen de chei.
Mac = alg probabilist de compl polin → care pornind de la o cheie k și mesaj m → generează un mesaj de auth.
V = alg pob. polin. $V(k, m, t) = 1$, dacă $t \leftarrow Mac_K(m)$.
Mac tb să fie rezistent la falsificarea tagului (t)
CBC MAC = metodă de reducere a dimens. tagului (t)



sigură dacă F_K e PRF și k se ține secret și m de aceeași lungime.