Criptosistemele simetrice → 2 clase fundamentale

- șir (stream)
- bloc

- Criptosist. stream (șir) criptează un mesaj $m = m_1 \dots m_l$ folosind o cheie - șir de aceeași lungime cu mesajul. $k = k_1 \dots k_l$ ; dar cheia k este de obicei generată de un generator de chei pornind de la o cheie. 4 mică 4


Exemple: RC4 (se utilizează în TLS) → o-a arăt că e slab.

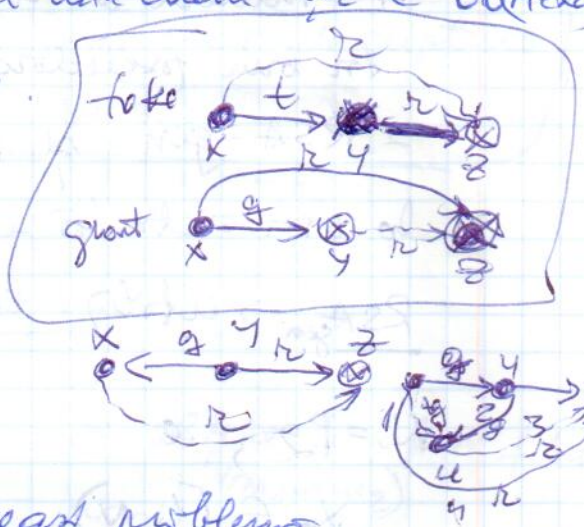
- Cu probabilitate mare pot fi prezise decurgând din chei șir -, ex: al doilea octet din cheia șir e 0 (Hexa) ($0^8$) cu probabilitate 1/128.

$m = m_1 \dots m_l$

$k = k_1 \dots k_l$

XOR: $(m_1 \oplus k_1) \dots (m_l \oplus k_l)$

$k_2 \rightarrow$ cunosc $m_2$




- Criptosistemul A5/1. - aceeași problemă - ca la fel pt EØ (pt bluetooth)

generatorul G îl fă să fie mocar pseudoaleator (PRG