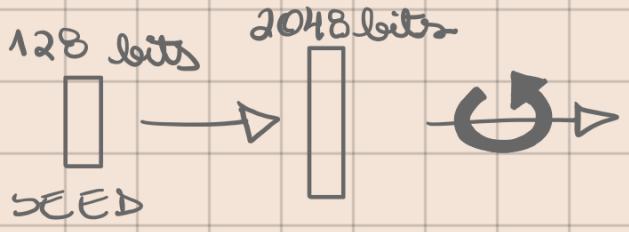
REAL-WORLD STREAM CIPHERS 4

RC4

↳ antigo (1987)



* utilizado no HTTP e no WEB (de forma errada)

FRAQUEZAS:

I. Início: $P_R[2^{nd} \text{Byte} = 0] = 2/256$. → problema conhecido como "Key Scheduling Algorithm (KSA)"

II. Prob. de (0,0) é $1/256^2 + 1/256^3$.

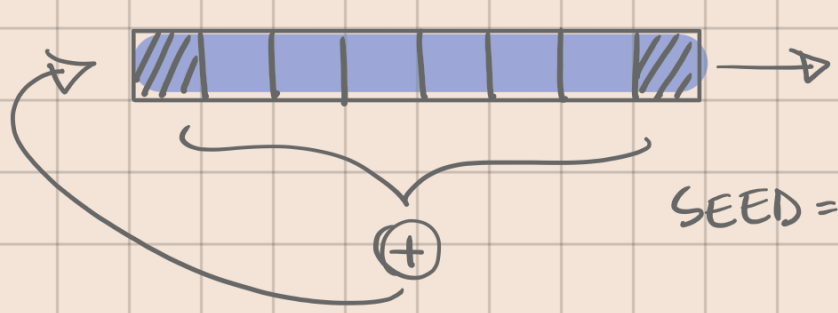
III. Ataques de chaves relacionadas.

CSS → antigo

↳ hardware

↳ já quebrado!

* Linear feedback shift register (LSFR):



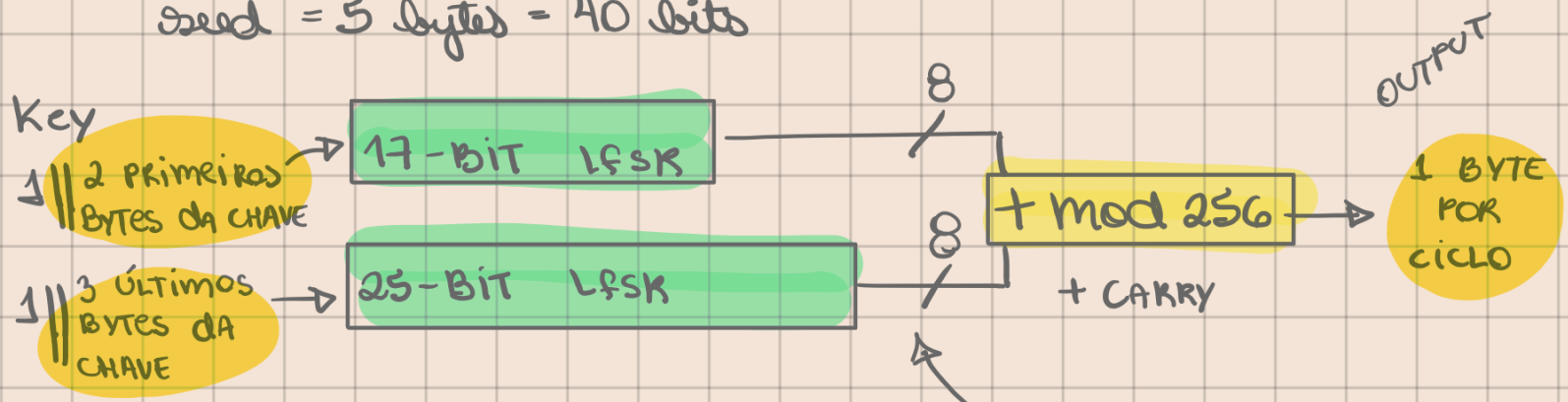
SEED = initial state of LSFR

*** USOS:** * Criptografia no DVD (CSS): 2 LFSRs } já quebrados

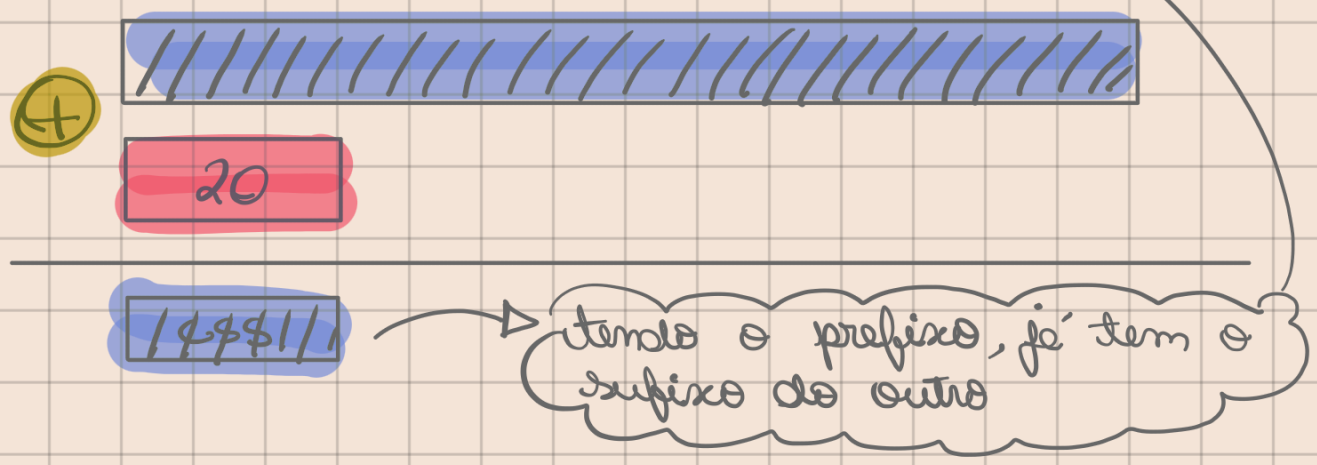
* Bluetooth (E0): 4 LFSRs

* CSS em si:

seed = 5 bytes = 40 bits



Isso é fácil de quebrar $\cong 2^{17}$ tempo



eSTREAM

→ 2008

* $PRG: \{0,1\}^s \times R \rightarrow \{0,1\}^n$; $n >> s$

seed

nonce: valor que nunca se repete tendo a mesma chave.

* $E(K, m; r) = m \oplus PRG(K; r)$

par (K,r) nunca é utilizado mais de uma vez. Então, é possível reutilizar a chave (K e r diferentes)

Exemplo de implementação: Salsa 20 (SW + HW)

$Salsa20: \{0,1\}^{128 \text{ ou } 256} \times \{0,1\}^{64} \rightarrow \{0,1\}^n$ (MAX. $n = 2^{73}$ bits)

→ barato! SEED NONCE

$$\text{Salsa20}(K;r) := H(K,(r,0)) \,||\, H(K,(r,1)) \,||\, \ldots$$