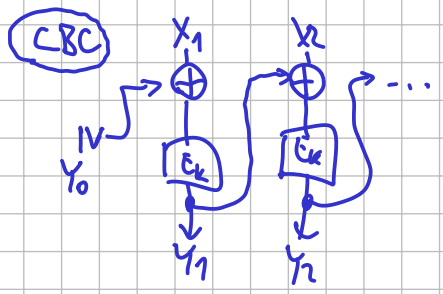
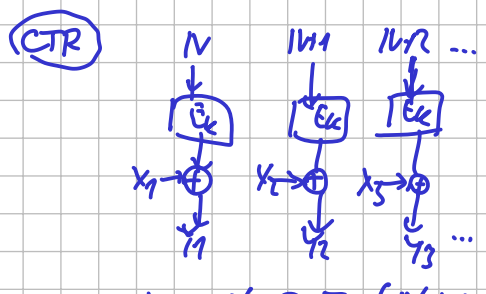




LEAKAGE

ECB: $Y_i = Y_j \Leftrightarrow X_i \Leftrightarrow X_j$

CBC: $Y_i = Y_j$: $E_k(X_i \oplus Y_{i-1}) = E_k(X_j \oplus Y_{j-1})$

likely to happen after $2^{b/2}$ blocks

$X_i \oplus Y_{i-1} = X_j \oplus Y_{j-1}$

$X_i \oplus X_j = Y_{i-1} \oplus Y_{j-1}$ — b bits

$Y_{i-1} \oplus Y_{j-1}$ known to attacker

leaks b bits per $\sim 2^{b/2}$ blocks

Don't use a single key for encrypting $2^{b/2}$ blocks

CTR: C_1 ___ C_m $\quad C_i = E_k(IV+i-1)$

All C_i's are different!

$Y_i \oplus Y_j = (X_i \oplus C_i) \oplus (X_j \oplus C_j) = (X_i \oplus X_j) \oplus (C_i \oplus C_j)$

$Y_i \oplus Y_j \neq X_i \oplus X_j$ ruling out 1 out of $2^b \neq 0$

$Y_i \oplus Y_j$ known

leak: $b - \log(2^b - 1) = \log \frac{2^b}{2^b - 1} = \log\left(1 + \frac{1}{2^b - 1}\right) \approx c \cdot \frac{1}{2^b - 1}$

$\approx c \cdot \frac{1}{2^b} = c \cdot 2^{-b}$

$e^x \approx 1 + x$

$x \approx \ln(1+x)$

bits leaked $\leq \binom{m}{2} \cdot c \cdot 2^{-b}$ ... const. for $m \sim 2^{b/2}$

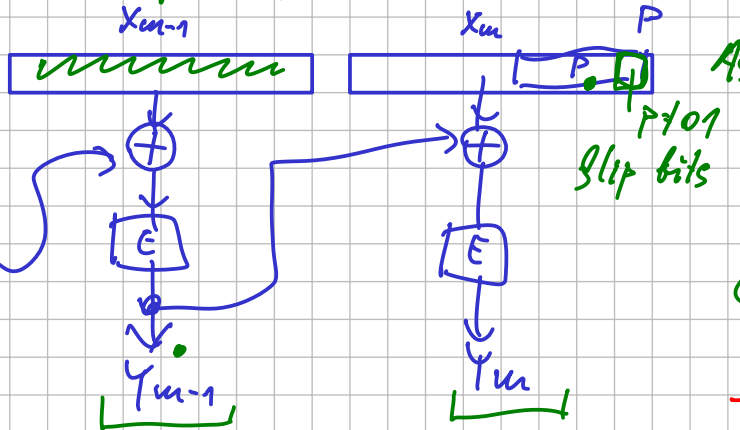
$\binom{m}{2} \sim m^2$ pairs; $c \cdot 2^{-b}$ leak per pair

| | | | | | |

60b 10% of plaintext

Padding Oracle Attack on CBC (CTR)

Assume padding: data P ... P



Assume P ≠ 01

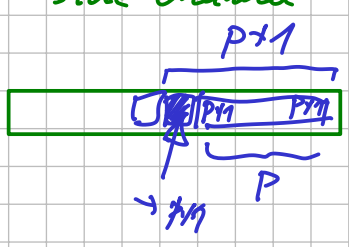
flip bits → P ≠ 01

exactly one solution with correct padding

$P \oplus F = 01$

↳ recovered P

TLS (HTTPS)



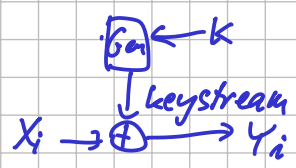
orig byte $\oplus F = P+1$

recover the last block

$\frac{B}{A} \cdot 2^8$

bytes/block 256

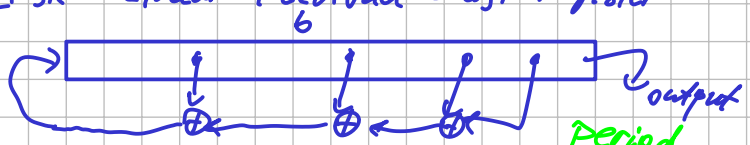
Stream Ciphers



eSTREAM project

- goal: find new stream ciphers
- init: 2004, finals: 2008
- profile 1: SW → 4 ciphers
- profile 2: HW → 3 ciphers
  - → Trivium
    - 288 bits of state
    - init with: key 80b, IV 80b, constants
    - run for 1152 steps
    - sec. level ≈ 80

LFSR - Linear-Feedback Shift Register

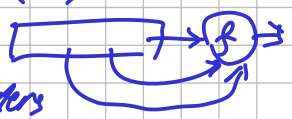


- trivial in blw
- trivial to crack given KPA
- period $= 2^b - 1$

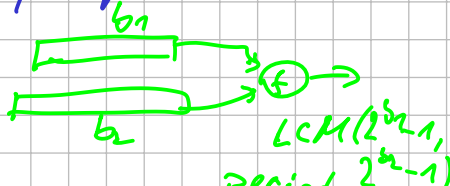
known-plaintext attack

Attempts to save LFSR

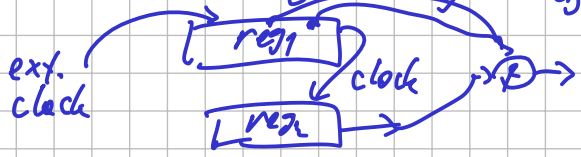
- non-linear feedback (f)
- non-linear output



- combine multiple registers



- control clock of reg. by out of reg.

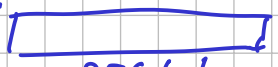


Example: A5/1 (GSM)

RC4 (Rivest 1987)

permutation-based
working on bytes

state:



BROKEN
KPA

ChaCha20 (Bernstein 2008)

eSTREAM SW profile
Salsa20

20 = # rounds

state: 4 × 4 = 16 32-bit values

20 rounds

ARX ← XOR, addition, rotation

256b key (32B)
64b nonce (8B)
64b block counter (8B)

→ ChaCha20 (not bijective) → 1 block of keystream

Hash Function

$\{0,1\}^* \xrightarrow{h} \{0,1\}^b$

$h(x) = h(x')$

1. no collision: $h(x) = h(x')$, $x \neq x'$
2. no second preimage: for given x, find x': $h(x) = h(x')$
3. no inversion: for given y, find x: $h(x) = y$

Use case: signatures