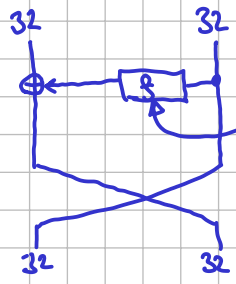
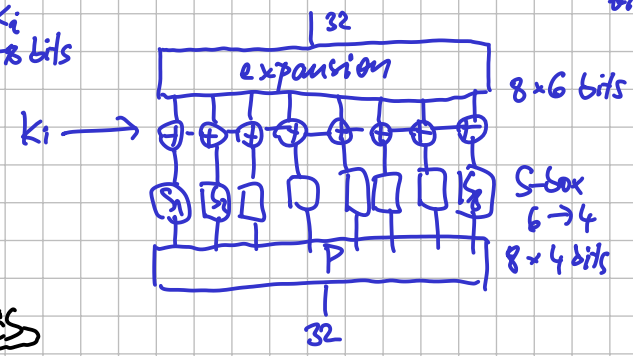
DES

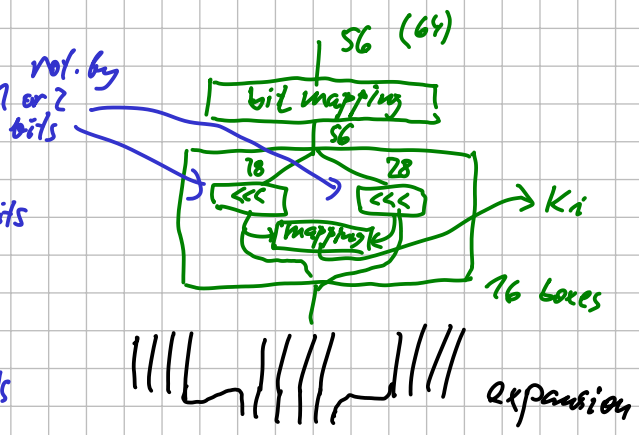
Feistel network with 16 rounds
64-bit blocks, 56-bit keys



Feistel function

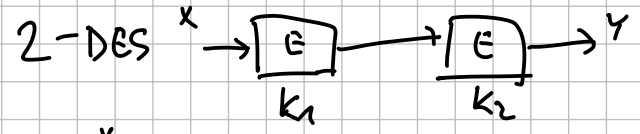


Key schedule



Critique of DES

- weak keys: if $K = 0^{56}$, then $\forall i\ k_i = 0^{48}$, so $\oplus$ in f has no effect
  ⇒ all round are identical
  ↳ $K = 1^{56}$ So $E_k = D_K$
- $E_{\bar{k}}(\bar{x}) = \overline{E_k(x)}$
- too short key: brute-force attacks 2012 ... FPGA-based machine which cracks DES in 26 hours
- too short blocks: in 2^{32} blocks we have block collision
  ↳ workaround: 2-DES



key size $2 \cdot 56 = 112$ bits
But: security level ≤ 57 (exercise)

3-DES

$3 \cdot 56 = 168$ bits of key
sec. level ≤ 113

? group structure?
$\forall k_1, k_2\ \exists k$
$E_{k_1} \circ E_{k_2} = E_k$

- too much secrets
- attacks on structure .... 2^{47} chosen plaintexts

AES (Advanced Encryption Standard)

- 1997 NIST public competition, 15 candidates, 3 rounds of evaluation
- Rijndael became AES in 2001

128-bit blocks, 128 or 192 or 256 bit keys
↓ 10 rounds, ↓ 12, ↓ 14

Structure: SPN with linear step
internal state & round key: matrix of bytes $\in GF(2^8)$ 4×4

$f(x \oplus k_i) = f(x) \oplus f(k_i)$

inversion in GF + affine transf.

Round: ByteSub (16 identical S-boxes)
P ShiftRows (fixed 1 byte, 2 byte, 3 byte)
– MixColumns: linear transform on every column
⊕ – AddRoundKey ... xor with k_i

Round of decryption: AddRoundKey, InvMixColumns, InvShiftRows, InvByteSub

InvMix
AddRK(fixed)
InvByteSub
InvShiftRows

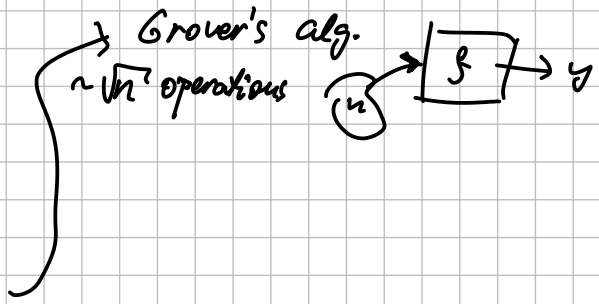
$m_1(b) = mix((s(x), 0, 0, 0))$
$m_2(x) = mix((0, s(x), 0, 0))$
m_3
m_4

$mix(s(x_1), s(x_2), s(x_3), s(x_4)) = m_1(x_1) \oplus m_2(x_2) \oplus m_3(x_3) \oplus m_4(x_4)$

1 KB
$[2^8] \to [2^{32}]$

Critique of AES:

- simple algebraic structure
- small margin in # rounds
- byte-aligned
- 128-bit key : quantum attacks
- 128-bit blocks : block collisions in $\sim 2^{64}$ blocks
  work-around: change keys after 2^{32} blocks (64GB)



Other finalists in AES comp.:

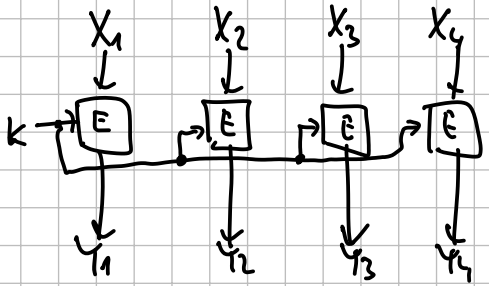
- Serpent : 128b blocks, 128–256b keys, 32 round SPN + linear
- Twofish : —"— , 16-round Feistel net with key-dependent S-boxes

---

Use of Block Ciphers: Padding

Block Cipher Modes of Operation

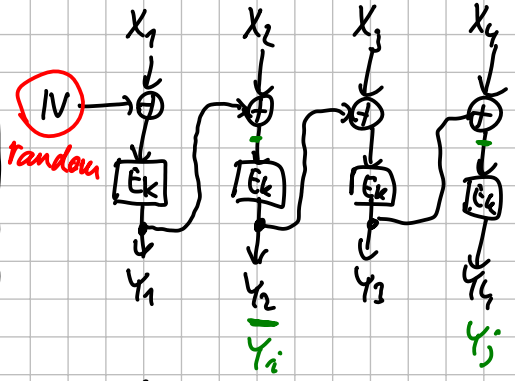
ECB: Electronic Code Book



AVOID AT ALL COSTS!

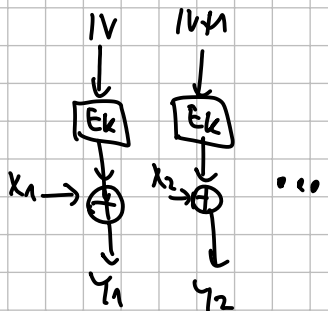
- no IV → reveals equality
- reveals $X_i = X_j \Leftrightarrow Y_i = Y_j$
- flip a bit in $Y_i \Rightarrow$ destroy X_i
- swap $Y_i \leftrightarrow Y_j \Rightarrow X_i \leftrightarrow X_j$

CBC: Cipher Block Chaining



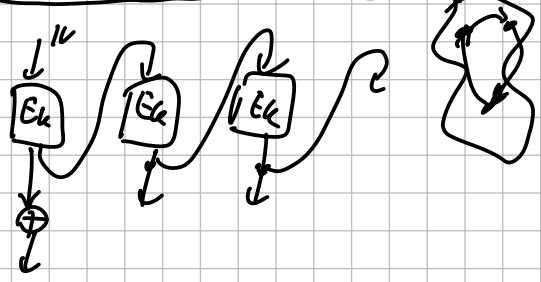
- requires random IV
- bit flip in Y_i
  → destroys X_i
  → flip in X_{i+1}
- $Y_i \leftrightarrow Y_j$
  X_{i+1} ⊕ed with $Y_i \oplus Y_j$
  X_{j+1} —"—
  $X_i \leftarrow X_j \oplus Y_{i-1} \oplus Y_{j-1}$
  sim. for $X_j \leftarrow X_i \oplus \dots$
- Proof of security wrt. CPA (chosen plaintext) for not-too-long messages ($\sqrt{\text{block space size}}$ blocks)

CTR: Counter



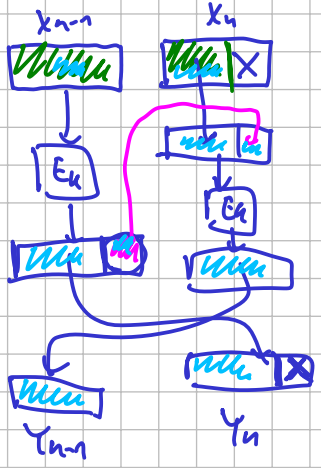
- a stream cipher → no padding needed
- MUST NOT REPEAT IV
- bit flip in Y_i → bit flip in X_i
- random access
- parallelizable

OFB: Output Feedback



Ciphertext Stealing

for ECB:



for CBC