Block ciphers

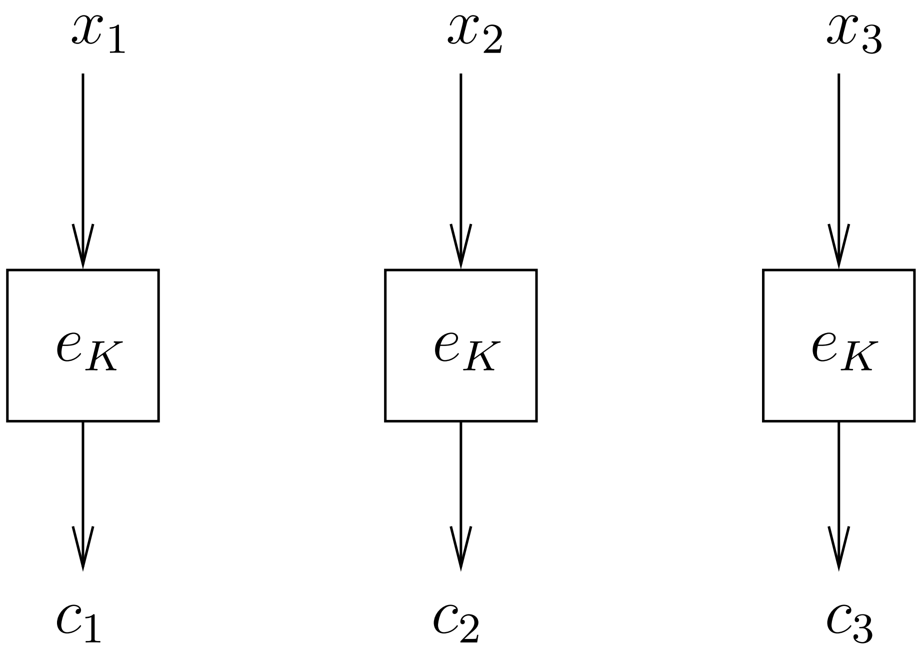
Block ciphers

- We defined a cryptosystem as a tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$.
- Our examples divided the plaintext to relatively short blocks and applied e_k to each of them.
  - Exception: text autokey, skytale
- There really were two things:
  - a block cipher;
  - a mode of operation.

Block ciphers

- Let Σ be an alphabet.
- Let $n \in \mathbb{N}$ be the block size/length.
- A block cipher is an encryption system $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where $\mathcal{P} = \mathcal{C} = \Sigma^n$.
- Example: Shift cipher and substitution cipher: $\Sigma = \mathbb{Z}_{26}$ and $n = 1$.

A mode of operation: Electronic Codebook (ECB)



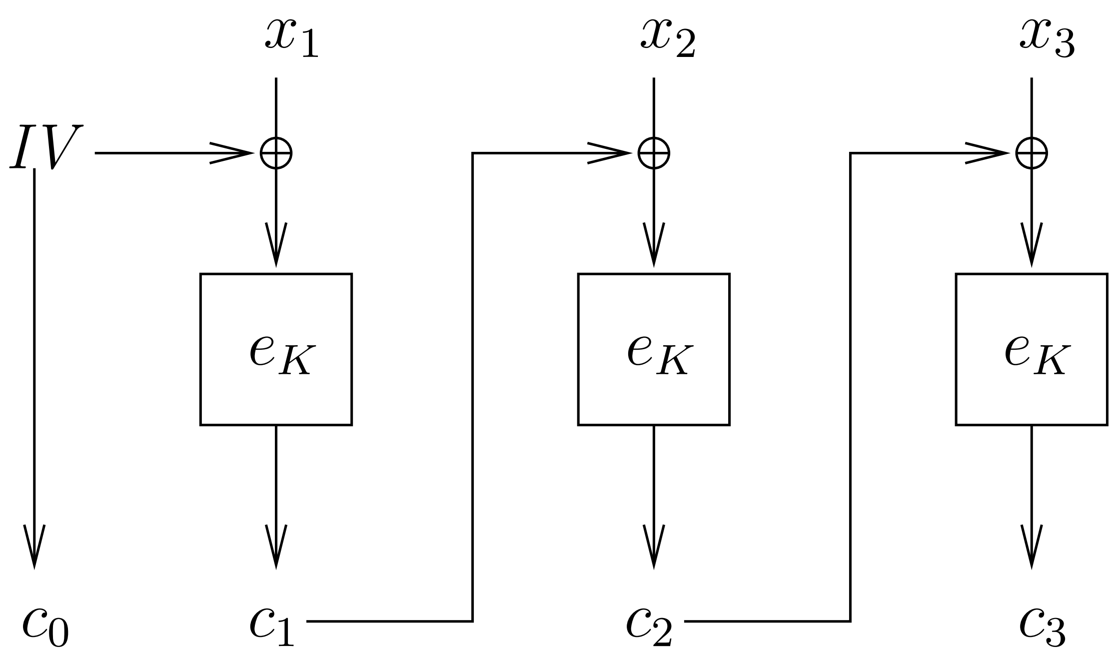
In our examples, this has been the mode we used.

Properties of ECB-mode

1. Equal blocks of plaintext are encoded to equal blocks of ciphertext.
2. Reordering the ciphertext blocks still yields a something that can be decoded without errors.
3. Bit errors in some ciphertext block do not affect the decoding of other blocks.
4. Encoding and decoding are doable in parallel.

Cipher Block Chaining (CBC) mode

Let a binary operation $\oplus$ be defined on blocks. Usually it is bit-wise XOR.



Properties of CBC-mode

1. Encoding the same plaintext twice with different values of the IV yields different ciphertexts.
2. Reordering the blocks yields garbage as decoded plaintext after the point of reordering. Deleting a number of blocks from the end of the ciphertext does not yield garbage.
3. Bit errors in the i-th block affect the decoding of i-th and $(i+1)$-st blocks.

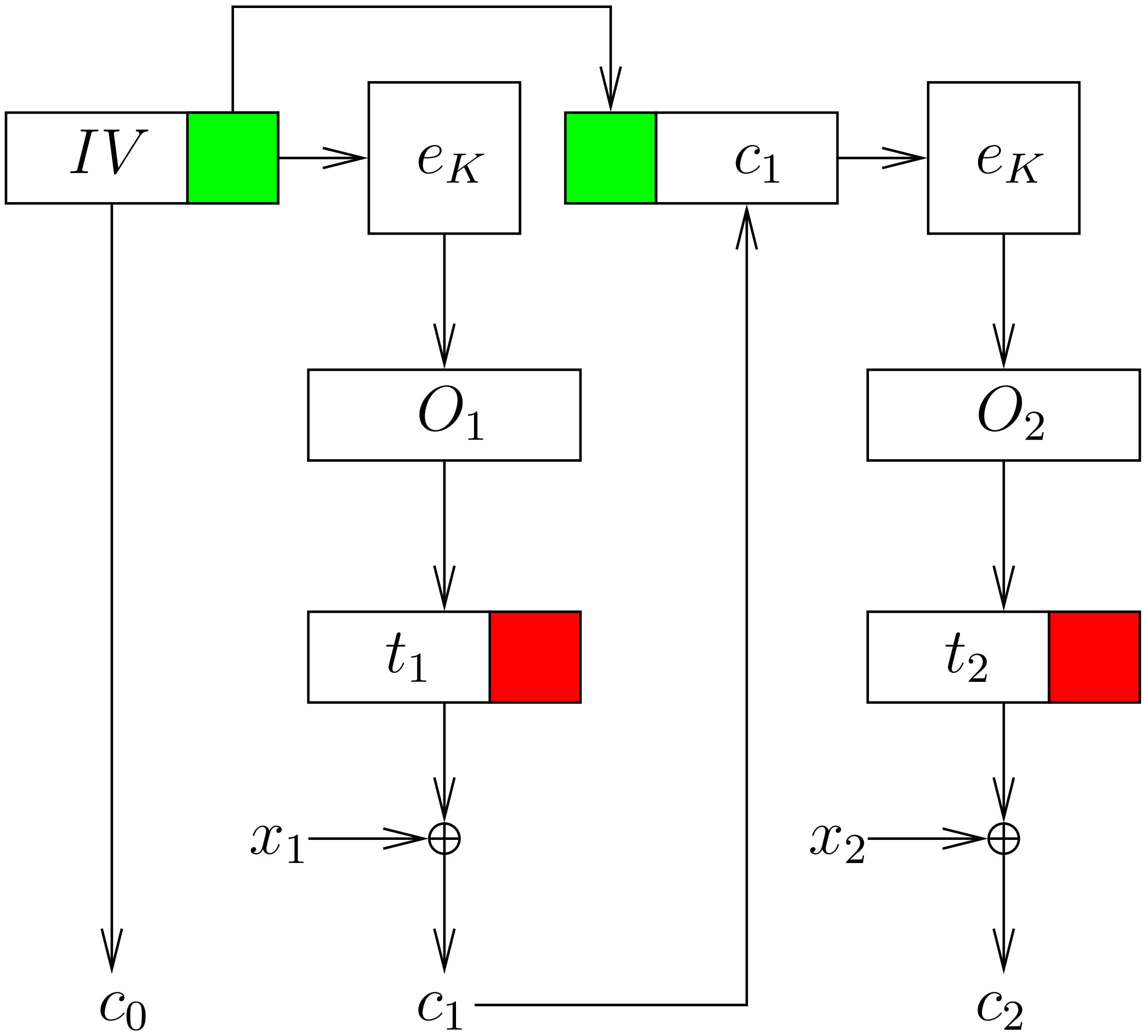
Exercise: how parallelizable are encoding and decoding?

Exercise

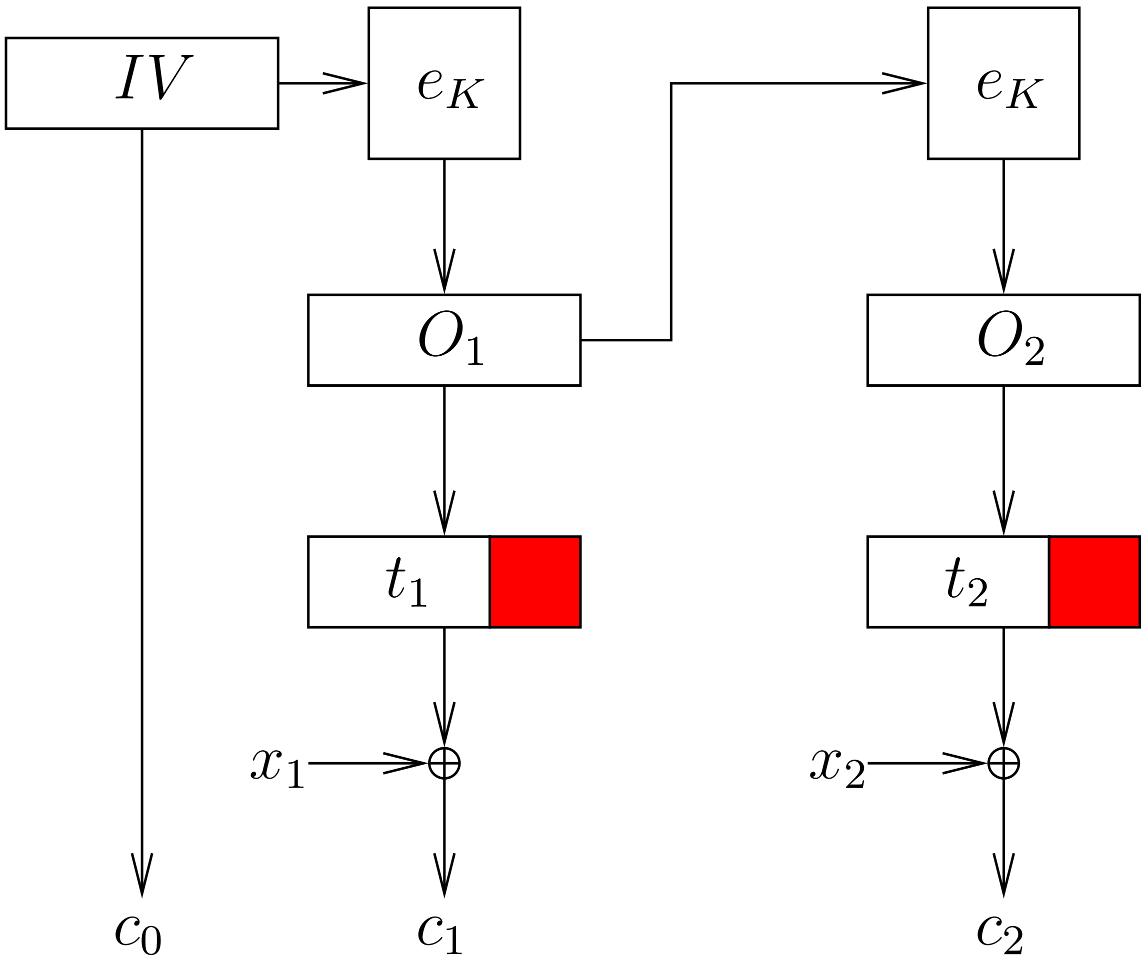
Consider Vigenère cipher that has been employed in the CBC-mode.
How to perform a ciphertext-only attack against it?

- Block length $=$ key length.
- Let $\oplus$ be addition *modulo* 26.

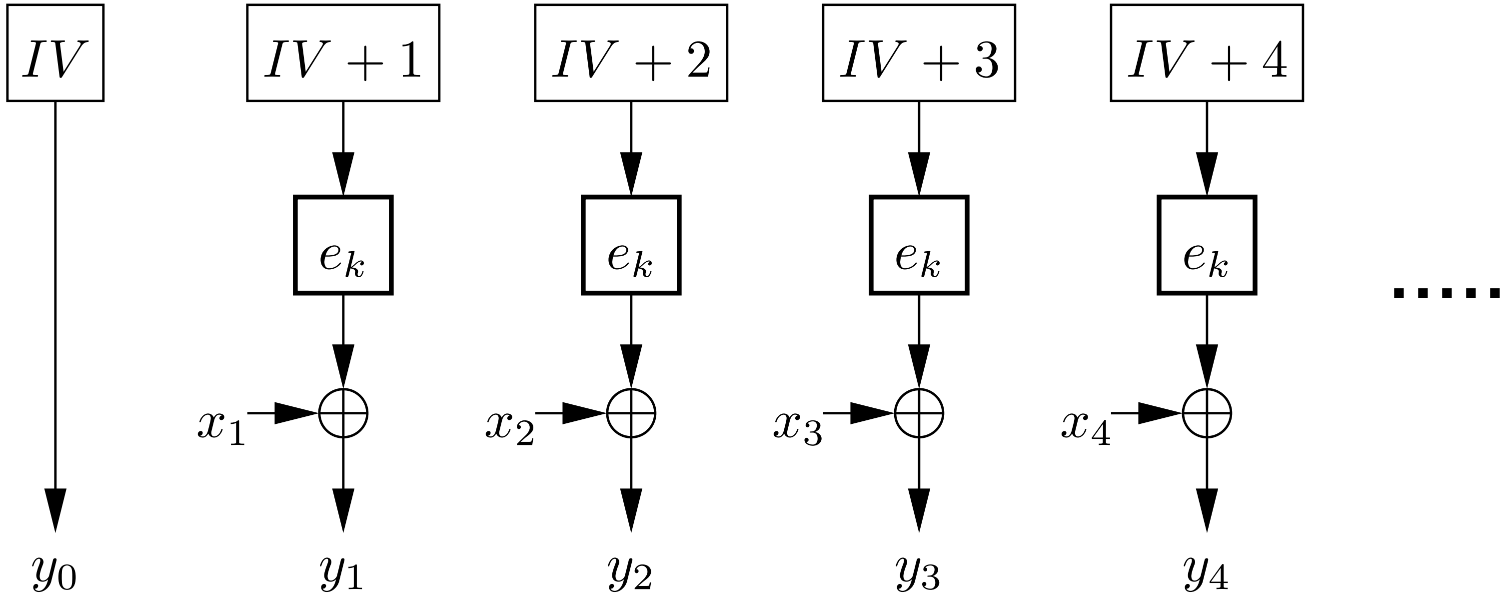
Cipher Feedback (CFB) mode



Output feedback (OFB) mode



Counter (CTR) mode



Properties of CFB-, OFB- and CTR-modes

Exercise: What can be said about the

- determinism
- resiliency to reordering of ciphertext blocks
- propagation of bit errors
- parallelizability of encryption and decryption

for CFB, OFB and CTR modes?

Product of encryption systems

- Given two encryption systems $\mathbf{S}_i = (\mathcal{P}_i, \mathcal{C}_i, \mathcal{K}_i, \mathcal{E}_i, \mathcal{D}_i)$ $(i \in \{1,2\})$ with the key distributed according to $\mathbf{K}_i$.
- We require $\mathcal{C}_1 = \mathcal{P}_2$.
- Their product is an encryption system $\mathbf{S}_1 \times \mathbf{S}_2 = (\mathcal{P}_1, \mathcal{C}_2, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$, where
  - probability of getting the key (k_1, k_2) is $\Pr[\mathbf{K}_1 = k_1] \cdot \Pr[\mathbf{K}_2 = k_2]$;
  - $e_{(k_1,k_2)}(x) = e_{k_2}(e_{k_1}(x))$;
  - $d_{(k_1,k_2)}(y) = d_{k_1}(d_{k_2}(y))$.

Exercises

Let: $\mathbf{N}$ — shift cipher; $\mathbf{M}$ — multiplicative shift cipher; $\mathbf{A}$ — affine cipher. Show that

- $\mathbf{N} \times \mathbf{N} = \mathbf{N}$;
- $\mathbf{M} \times \mathbf{M} = \mathbf{M}$;
- $\mathbf{M} \times \mathbf{N} = \mathbf{N} \times \mathbf{M} = \mathbf{A}$;
- $\mathbf{A} \times \mathbf{A} = \mathbf{A}$.

Let $\mathbf{V}_n$ be the Vigenère cipher with the key length n. What can be said about

- $\mathbf{V}_n \times \mathbf{V}_n$;
- $\mathbf{V}_m \times \mathbf{V}_n$ where $m \mid n$;
- $\mathbf{V}_m \times \mathbf{V}_n$ in general?

More exercises

- Let $\mathbf{N}'$ be shift cipher with some skewed distribution of keys. What is $\mathbf{N} \times \mathbf{N}'$?
- Let G be group and g a uniformly chosen element of g. Show that
  - g^{-1} is uniformly distributed;
  - for a random $h \in G$ (with any distribution), $g \cdot h$ is uniformly distributed.
- Let a and b be two independently uniformly chosen elements of some finite ring R. Is $a \cdot b$ uniformly distributed? What if a were uniformly chosen from the multiplicative group R^*?

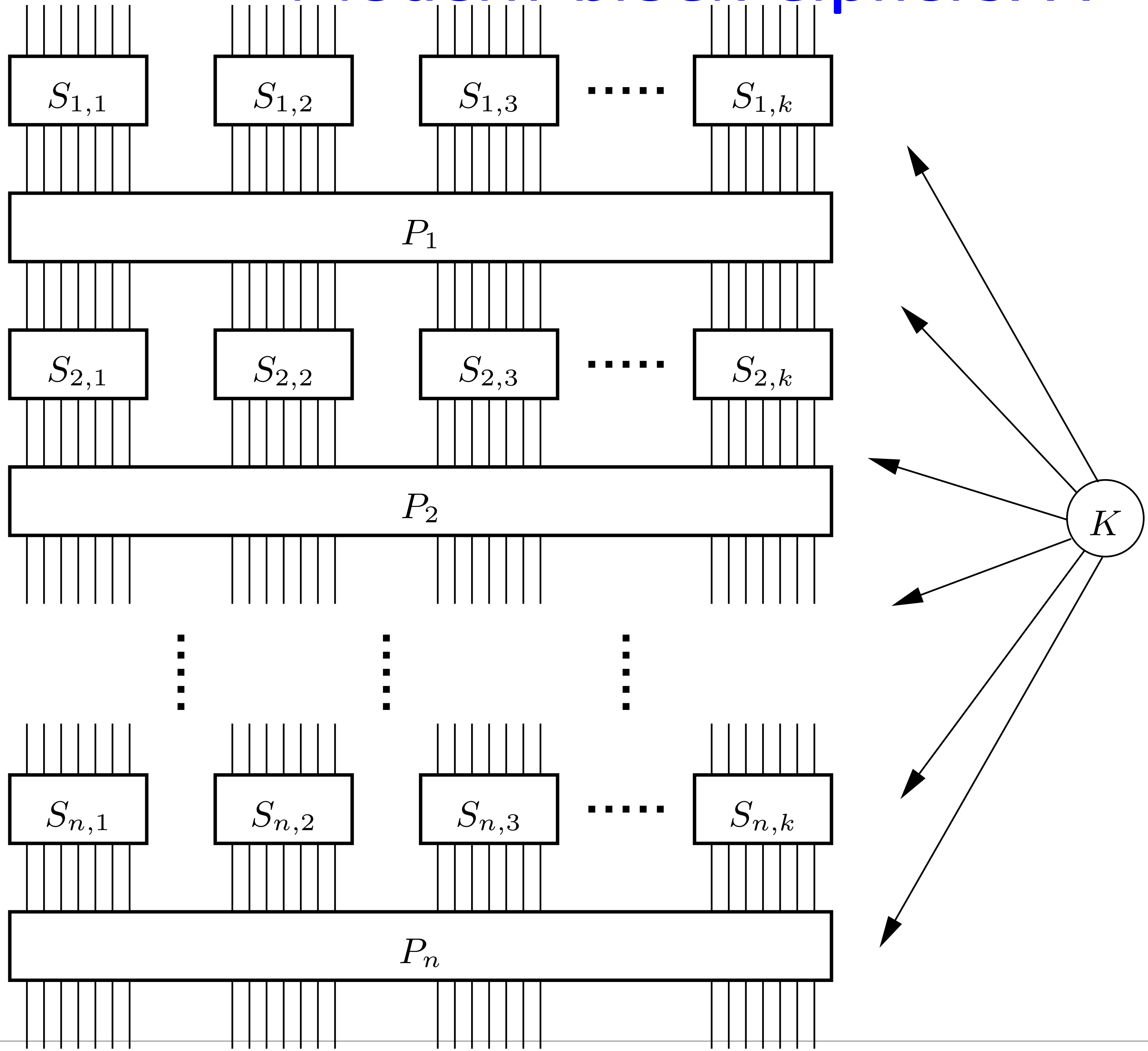
“Block cipher” and Estonian language

Rasked sõnad on plokk ja blokk. Esimese taga on inglise ja prantsuse *block* ning eesti ploki tähendused on: ühtne risttahukakujuline tervik, nt ehitusplokk; märkmik; otstarbelt kokkukuuluv kogum, nt reklaamiplokk, uudisteplokk; hoonete või ruumide rühm, nt haigla köögiplokk, operatsiooniplokk; tõsteseadme osa; konstruktsioonilt terviklik seadiste, detailide vm kogum, nt toiteplokk. Bloki taga on prantsuse ja inglise sõna *bloc* ja tema tähendus on riikide, parteide, ühenduste liit.

Tiiu Erelt. *Need rasked võõrsõnad*. Oma Keel 2001(**2**):38–46

Hence “plokkšiffer”.

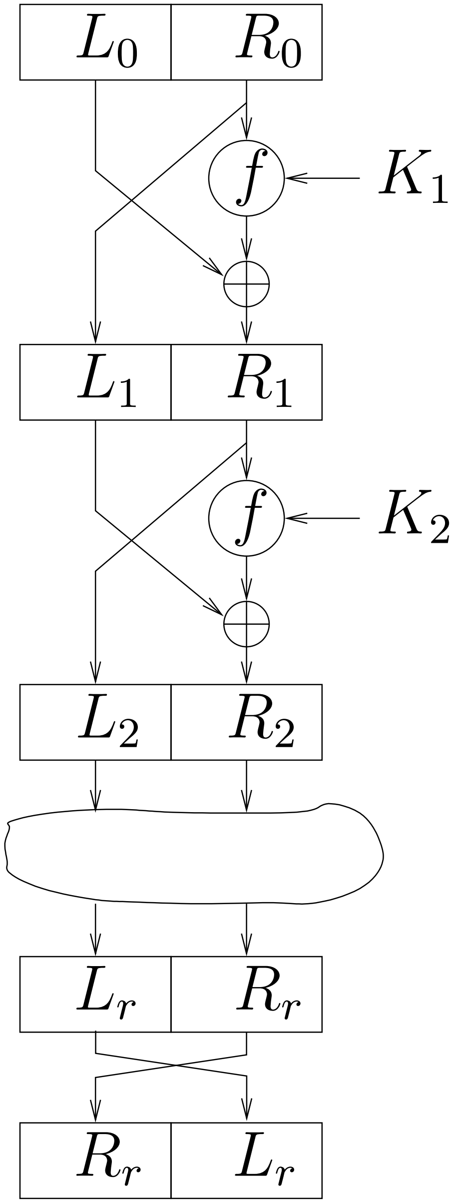
Modern block ciphers. . .



Substitution-Permutation network

- One round consists of
  - Mixing in the key;
  - Substitution on short bit-strings;
  - Permutation of the entire block.
- A round has to be a permutation on the entire set Σ^n.
- The entire block cipher is the product of rounds.
  - though usually the round keys are not independent.

Feistel's construction



- A way to specify the round functions for the block cipher.
- The definition of the block cipher must specify the function f and the number of rounds r.
  - f does not have to be a permutation.
- $K_1, \ldots, K_r$ are round keys, they're found somehow from the key of the block cipher K.
  - The key of the block cipher is usually not $K_1 \cdots K_r$, but something shorter.

Exercise. How to decrypt?

DES

DES (Data Encryption Standard) (January 15th, 1977).

- $\mathcal{P} = \mathcal{C} = \{0,1\}^{64}$.
- $\mathcal{K} = \{0,1\}^{56}$.
- Encoding bit-string x with the key K:

  1. Let $x_0 = IP(x)$, where IP is a certain permutation of bits. Let L_0 [R_0] be the first [last] 32 bits of x.
  2. 16 rounds of Feistel construction:

     $$L_i = R_{i-1} \qquad R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

     Here $1 \leq i \leq 16$, $K_i \in \{0,1\}^{48}$ consist of certain 48 bits of K.
  3. Let $y = IP^{-1}(R_{16}L_{16})$. y is the ciphertext.

Key schedule

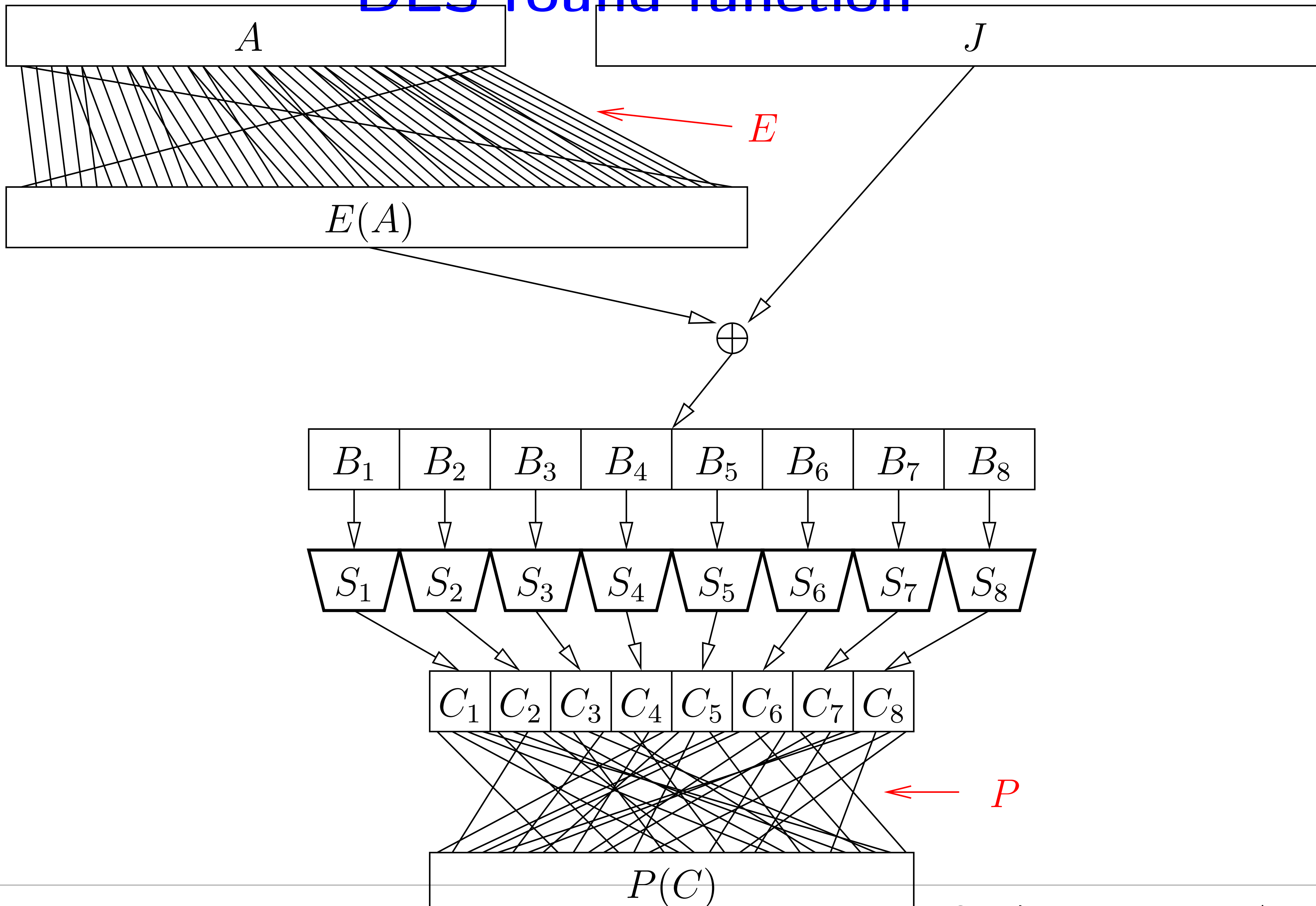
- 16 rounds $\times$ 48 bits/round $=$ 768 bits.
  - Too large to conveniently manage.
  - But a single round should also use a relatively large key.
    - **Exercise.** Why?
- All round-based block ciphers expand the master key into the sequence of round keys.
- The complexity of expansion is different for different ciphers.
  - DES's is about the easiest possible.
    - At least if we consider hardware implementations.

DES round function

$f : \{0,1\}^{32} \times \{0,1\}^{48} \to \{0,1\}^{32}$. $f(A, J)$ works as follows:

1. "Expand" A to $E(A)$ of length 48. The function E outputs the bits of its argument in certain order (16 bit positions occur once and 16 occur twice).
2. Let $B_1 \cdots B_8 = E(A) \oplus J$, where $B_i \in \{0,1\}^6$.
3. Let $C_i = S_i(B_i)$, where $S_i : \{0,1\}^6 \to \{0,1\}^4$ is a fixed mapping. (the *S-box*)
4. return $P(C_1 \cdots C_8)$ where P is a certain permutation of bits.

DES round function



DES: details

Decryption: like encryption, but round keys taken in order $K_{16}, K_{15}, \ldots, K_1$.

In the standard, the encryption key is actually 8 bytes long.

- The least significant bit in each byte is a parity check bit. Not used in actual encryption.
- The number of 1-s in each byte is odd.

Exercises

- Show that $\mathrm{DES}(K, X) = \sim\mathrm{DES}(\sim K, \sim X)$. How does that simplify brute-force attacks?
  - $\sim X$ — bitwise complement of X.
- Because of the short key length of DES, triple-DES finds use in practice. Why isn't double-DES used? What is the "effective key length" of triple-DES?
- Keys k_1 and k_2 are dual if $e_{k_1} = d_{k_2}$. Show that keys $00\cdots0$ and $11\cdots1$ are both self-dual.

AES

- 128-, 192-, or 256-bit key, 128-bit blocks.
    - A block — a vector of 16 bytes.
    - All operations are byte-oriented.
- 10, 12, or 14 rounds.
- Complex key schedule.
    - Slightly different for different key-lengths.
- A round consists of the following steps:
    - *SubBytes* — apply the S-box to each byte.
    - *ShiftRows* and *MixColumns* — linear transformations of the 16-element vector.
    - *AddRoundKey* — XOR with the 128-bit round key.

Recent attacks against AES

- By Alex Biryukov, Dmitry Khovratovich, et al.
- Against AES-192 and AES-256.
  - Do not work against AES-128.
- Exploit weaknesses in key schedules.
- Break 9 or 10 rounds of AES-256 in practical time.
- related-key attacks.
  - Encryption with several different keys is available, with the attacker choosing (or at least knowing) the relation between them.

Linear cryptanalysis

- Let $x_1, \ldots, x_n$ be the bits of the plaintext, $k_1, \ldots, k_m$ the bits of the key, $y_1, \ldots, y_n$ the bits of the ciphertext.
- Let E be a linear expression over $x_1, \ldots, x_n, k_1, \ldots, k_m, y_1, \ldots, y_n$.
  - Denote $E(x, k, y)$.
  - E picks a subset E_{supp} of those bits and XOR-s them together.
  - Possibly also negates them, but this is not important for us. . .
- What is the probability of $E(x, k, y) = 0$ if x and k are chosen randomly?
- The bias of E (away from $1/2$) can be computed by analysing the cipher.
- Given a large number of plaintext-ciphertext pairs, we compute E for all of them and get an idea what the XOR of key bits in E_{supp} should be.
- Such known-plaintext attack gives a single bit of information about the key.

Linear cryptanalysis

- Consider a cipher that works in r rounds.
- Let key K be fixed.
- Let $x_1, \ldots, x_n$ be the bits of the plaintext, and $v_1, \ldots, v_n$ be the bits of the result of applying $r-1$ rounds.
- Let E be a linear expression over $x_1, \ldots, x_n, v_1, \ldots, v_n$.
- If x is randomly chosen then what is the the probability of $E(x, v) = 0$?

Linear cryptanalysis

- Let E have a relatively large bias ε.
- Let us have plaintext-ciphertext pairs $(x^1, y^1), (x^2, y^2), \ldots$.
- The bits v_i in E_{supp} will map to certain bits of y with the help of certain bits of the last round key K_r.
- For all possible values k of those bits of K_r:
  - For all pairs (x^i, y^i):
    - Do partial one-round decryption of y^i, using the key bits k_r.
    - Let the resulting bits be a subsequence of $v'_1, \ldots, v'_n$.
    - Compute $E(x, v')$.
  - Let B_k be the bias of $E(x, v')$.
- Likely value k of the interesting bits of K_r is such, where the bias B_k is large.
- Needs $O(1/\varepsilon^2)$ plaintext-ciphertext pairs.

Differential cryptanalysis

- Consider pairs of plaintexts x, x^* with a fixed $\bar{x} = x \oplus x^*$.
  - Chosen-plaintext attack, because $\bar{x}$ is given.
- Given $\bar{x}$, consider the possible values $\bar{v} = v \oplus v^*$. Suppose one of the $\bar{v}$-s has a significant probability.
- Such $\bar{x}$ and $\bar{v}$ are found by analysing the cipher.
- Consider all possible values k of the last round key K_r.
- A likely value for k is such, that one-round decrypting y and y^* with k gives intermediate values with XOR $\bar{v}$.