A cryptosystem is unconditionally secure (*absoluutselt turvaline*) (wrt. a class of attacks) if no adversary (no matter what resources it has) can break it with the help of these attacks.

Let $\mathbf{X}$ be a random variable over the set X and $\mathbf{Y}$ a random variable over the set Y.

$\Pr[\mathbf{X} = x]$ denotes the probability that $\mathbf{X}$ gets the value $x \in X$.

$\Pr[\mathbf{X} = x, \mathbf{Y} = y]$ denotes the probability that $\mathbf{X}$ gets the value $x \in X$ and simultaneously $\mathbf{Y}$ gets the value $y \in Y$.

$\Pr[\mathbf{X} = x | \mathbf{Y} = y]$ denotes the probability that $\mathbf{X}$ gets the value x, given that $\mathbf{Y}$ got the value y.

$$\begin{aligned} \Pr[\mathbf{X} = x, \mathbf{Y} = y] &= \Pr[\mathbf{Y} = y] \cdot \Pr[\mathbf{X} = x | \mathbf{Y} = y] \\ &= \Pr[\mathbf{X} = x] \cdot \Pr[\mathbf{Y} = y | \mathbf{X} = x] \end{aligned}$$

Bayes' theorem: if $\Pr[\mathbf{Y} = y] > 0$, then

$$\Pr[\mathbf{X} = x | \mathbf{Y} = y] = \frac{\Pr[\mathbf{X} = x] \cdot \Pr[\mathbf{Y} = y | \mathbf{X} = x]}{\Pr[\mathbf{Y} = y]} .$$

$\mathbf{X}$ ja $\mathbf{Y}$ are independent, if $\Pr[\mathbf{X} = x | \mathbf{Y} = y] = \Pr[\mathbf{X} = x]$ for all $x \in X$, $y \in Y$.

Let $\mathbf{P}$, $\mathbf{K}$ ja $\mathbf{C}$ be random variables over sets $\mathcal{P}$, $\mathcal{K}$ ja $\mathcal{C}$, describing the distribution of plaintexts, keys and ciphertexts. Then

$$\Pr[\mathbf{C}=y] = \sum_{\substack{x\in\mathcal{P}\\ k\in\mathcal{K}\\ e_k(x)=y}} \Pr[\mathbf{P}=x,\mathbf{K}=k] =$$

$$\sum_{k\in\mathcal{K}} \Pr[\mathbf{P}=d_k(y),\mathbf{K}=k] = \sum_{k\in\mathcal{K}} \Pr[\mathbf{P}=d_k(y)]\cdot\Pr[\mathbf{K}=k] \ .$$

$$\Pr[\mathbf{C}=y|\mathbf{P}=x] = \sum_{\substack{k\in\mathcal{K}\\ y=e_k(x)}} \Pr[\mathbf{K}=k]$$

$$\Pr[\mathbf{P}=x|\mathbf{C}=y] = \frac{\Pr[\mathbf{P}=x]\cdot\sum_{\substack{k\in\mathcal{K}\\ y=e_k(x)}} \Pr[\mathbf{K}=k]}{\sum_{k\in\mathcal{K}} \Pr[\mathbf{P}=d_k(y)]\cdot\Pr[\mathbf{K}=k]}$$

An encryption system has perfect secrecy, if $\Pr[\mathbf{P} = x | \mathbf{C} = y] = \Pr[\mathbf{P} = x]$ for all $x \in \mathcal{P}$, $y \in \mathcal{C}$.

Equivalently: $\Pr[\mathbf{C} = y | \mathbf{P} = x] = \Pr[\mathbf{C} = y]$ for all $x \in \mathcal{P}$, $y \in \mathcal{C}$.

Perfect secrecy is unconditional security wrt. ciphertext-only attacks.

Theorem. Shift cipher has perfect secrecy if its key is chosen with uniform probability and a key is used to encrypt a single character.

Proof. $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$.

- $\Pr[\mathbf{K} = k] = 1/26$ for all $k \in \mathbb{Z}_{26}$.
- $\Pr[\mathbf{C} = y] = 1/26$ for all $y \in \mathbb{Z}_{26}$, because $y = x + k$, x and k are independent and k is uniformly distributed.
- $\Pr[\mathbf{C} = y | \mathbf{P} = x] = \Pr[\mathbf{K} = y - x] = 1/26$.

$$\Pr[\mathbf{P} = x | \mathbf{C} = y] = \frac{\Pr[\mathbf{P} = x] \cdot (1/26)}{1/26} = \Pr[\mathbf{P} = x] \ .$$

Assume that $\Pr[\mathbf{C} = y] > 0$ for all $y \in \mathcal{C}$. If not, then remove this y from $\mathcal{C}$.

Lemma. If a cryptosystem has perfect secrecy then for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ there exists $k \in \mathcal{K}$, such that $e_k(x) = y$.

Proof. Assume the contrary, i.e. there exist x and y, such that $e_k(x) = y$ for no k. Then $\Pr[\mathbf{C} = y|\mathbf{P} = x] = 0$, but $\Pr[\mathbf{C} = y] > 0$. Hence there is no perfect secrecy.

Exercise

We have independent random variables $\mathbf{P}$ and $\mathbf{K}$ and the derived random variable $\mathbf{C}$.

The definition of perfect secrecy uses $\mathbf{P}$ and $\mathbf{K}$.

$\mathbf{K}$ is defined by the encryption system. So it's natural to use it.

But does perfect secrecy actually depend on $\mathbf{P}$?

Theorem. Let $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption system where $|\mathcal{P}| = |\mathcal{K}| = |\mathcal{C}|$. This encryption system has perfect secrecy iff the key is chosen uniformly and for all $x \in \mathcal{P}$, $y \in \mathcal{C}$ exists a unique $k \in \mathcal{K}$, such that $e_k(x) = y$.

Proof. $\Rightarrow$. Let the system have perfect secrecy. Then for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ there is at least one $k \in \mathcal{K}$, such that $e_k(x) = y$. Because the same key is usable for at most $|\mathcal{P}|$ pairs of (x, y), there cannot be more than one.

Fix $y \in \mathcal{C}$. Let $\mathcal{P} = \{x_1, \ldots, x_n\}$. Denote the elements of $\mathcal{K}$ in such a way: let $k_i \in \mathcal{K}$ be the key for which $e_{k_i}(x_i) = y$. From the perfect secrecy:

$$\Pr[\mathbf{P} = x_i] = \Pr[\mathbf{P} = x_i | \mathbf{C} = y] = \\ \frac{\Pr[\mathbf{P} = x_i] \cdot \Pr[\mathbf{C} = y | \mathbf{P} = x_i]}{\Pr[\mathbf{C} = y]} = \frac{\Pr[\mathbf{P} = x_i] \cdot \Pr[\mathbf{K} = k_i]}{\Pr[\mathbf{C} = y]},$$

i.e. $\Pr[\mathbf{K} = k_i] = \Pr[\mathbf{C} = y]$ for all i, i.e. the probabilities of all keys must be equal.

$\Leftarrow$: like the proof of perfect secrecy for the shift cipher.

Vernam's cipher or one-time pad (*ühekordne šifriblokk*):

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$;
- $e_{k_1 \ldots k_n}(x_1 \ldots x_n) = d_{k_1 \ldots k_n}(x_1 \ldots x_n) = (x_1 \oplus k_1) \ldots (x_n \oplus k_n)$.
  - $k_i, x_i \in \{0,1\}$.

Vernam's cipher has perfect secrecy (if the key is uniformly distributed and each key is used only once).

Exercises

- A latin square M is a $n \times n$ square filled with numbers $1, \ldots, n$, such that each i occurs exactly once in each row and column. Define an encryption system:
  - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, \ldots, n\}$;
  - $e_i(j) = M[i, j]$.

  Show that this encryption system has perfect secrecy.

- Show that affine cipher has perfect secrecy (if it is used to encrypt a single letter).

- Show that if an encryption system with perfect secrecy has $|\mathcal{P}| = |\mathcal{K}| = |\mathcal{C}|$, then all ciphertexts are equiprobable.

If we do not have perfect secrecy, then how much information about the key is leaked into the ciphertext? When can we determine the key (and the plaintext) with near-absolute certainty?

Let $\mathbf{X}$ be a random variable over the (finite) set X. The entropy of $\mathbf{X}$ is

$$H(\mathbf{X}) = -\sum_{x \in X} \Pr[\mathbf{X} = x] \cdot \log_2 \Pr[\mathbf{X} = x] \ .$$

Define $0 \cdot \log_2 0 = 0$, because $\lim_{x \to 0} x \log x = 0$.

$H(\mathbf{X})$ (more or less) corresponds to the average number of bits necessary to encode the value of $\mathbf{X}$.

$H(\mathbf{X}) = 0$ if and only if $\mathbf{X}$ always gets the same value. Then one of the probabilities is 1 and the rest are 0.

A prefix-free encoding of the set X is a mapping $\kappa : X \to \{0,1\}^*$, such that none of $\kappa(x)$-s is a prefix of another.

Given $\mathbf{X}$, the average length $\ell(\kappa)$ of κ is

$$\ell(\kappa) = \mathbf{E}[|\kappa(\mathbf{X})|] = \sum_{x \in X} \Pr[\mathbf{X} = x] \cdot |\kappa(x)| \enspace .$$

Theorem. For all prefix-free κ, $H(\mathbf{X}) \leq \ell(\kappa)$.

Theorem. There exists a κ, such that $\ell(\kappa) < H(\mathbf{X}) + 1$.

(One such κ is the Huffman code of X, where $\Pr[\mathbf{X} = x]$ is the weight of the element $x \in X$.)

$$H(\mathbf{X},\mathbf{Y}) = -\sum_{\substack{x\in X\\ y\in Y}} \Pr[\mathbf{X}=x,\mathbf{Y}=y]\cdot\log_2 \Pr[\mathbf{X}=x,\mathbf{Y}=y] \ .$$

Conditional entropy of $\mathbf{X}$ wrt. $\mathbf{Y}$:

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y\in Y}\sum_{x\in X} \Pr[\mathbf{Y}=y]\Pr[\mathbf{X}=x|\mathbf{Y}=y]\log_2 \Pr[\mathbf{X}=x|\mathbf{Y}=y] \ .$$

How many bits are necessary to encode $\mathbf{X}$ if everybody knows $\mathbf{Y}$?

A function f is concave (*kumer*) in an interval $[a, b]$ if for all $x_1, x_2 \in [a, b]$ and $\lambda \in [0, 1]$:

$$\lambda \cdot f(x_1) + (1 - \lambda) \cdot f(x_2) \leq f(\lambda \cdot x_1 + (1 - \lambda) \cdot x_2) \ .$$

I.e. the graph of the function (in the interval $[a, b]$) is above any straight line segment between two points of that graph.

Concavity is strict (*range*) if equality holds only for $\lambda \in \{0, 1\}$ (whenever $x_1 \neq x_2$).

Logarithm is a strictly concave function in $[0, \infty)$...

Jensen's inequality: let f be strictly concave function in the interval I. Let $x_1, \ldots, x_n \in I$ and let $a_1, \ldots, a_n \in (0, 1]$, such that $a_1 + \cdots + a_n = 1$. Then

$$\sum_{i=1}^{n} a_i f(x_i) \leq f\Big(\sum_{i=1}^{n} a_i x_i\Big)$$

and equality holds iff $x_1 = \cdots = x_n$.

Proof: induction over n. $n = 2$ is the def. of concavity.

Theorem. The maximum value of $H(\mathbf{X})$ is $\log_2 |X|$. It is attained only if $\mathbf{X}$ is uniformly distributed.

Proof. Let $X = \{x_1, \ldots, x_n\}$ and denote $p_i = \Pr[\mathbf{X} = x_i]$ Assume that $p_i > 0$ (otherwise remove x_i from X). Then $|X| = n$.

$$H(\mathbf{X}) = -\sum_{i=1}^{n} p_i \log_2 p_i = \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i} \leq \log_2 \sum_{i=1}^{n} p_i \cdot \frac{1}{p_i} = \log_2 n \quad .$$

We used Jensen's inequality with $a_i = p_i$ and $x_i = 1/p_i$. The equality holds only if $1/p_1 = \cdots = 1/p_n$, i.e. $p_1 = \cdots = p_n$.

Theorem. $H(\mathbf{X}, \mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y})$ with equality holding iff $\mathbf{X}$ and $\mathbf{Y}$ are independent.

Proof. Let $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_m\}$ and denote

- $p_i = \Pr[\mathbf{X} = x_i]$;
- $q_i = \Pr[\mathbf{Y} = y_i]$;
- $r_{ij} = \Pr[\mathbf{X} = x_i, \mathbf{Y} = y_i]$. Then
  - $p_i = \sum_{j=1}^{m} r_{ij}$,
  - $q_j = \sum_{i=1}^{n} r_{ij}$.

$\mathbf{X}$ and $\mathbf{Y}$ are independent iff $r_{ij} = p_i q_j$ for all i, j.

$$H(\mathbf{X},\mathbf{Y}) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2 r_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2 \frac{1}{r_{ij}}$$

$$H(\mathbf{X}) + H(\mathbf{Y}) = -\sum_{i=1}^{n} p_i \log_2 p_i - \sum_{j=1}^{m} q_j \log_2 q_j =$$

$$-\left(\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2 p_i + \sum_{j=1}^{m}\sum_{i=1}^{n} r_{ij}\log_2 q_j\right) =$$

$$-\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}(\log_2 p_i + \log_2 q_j) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2(p_i q_j)$$

$$H(\mathbf{X},\mathbf{Y})-H(\mathbf{X})-H(\mathbf{Y}) = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2\frac{1}{r_{ij}} + \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2(p_iq_j) =$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\left(\log_2\frac{1}{r_{ij}}+\log_2(p_iq_j)\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2\frac{p_iq_j}{r_{ij}} \le$$

$$\log_2\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\cdot\frac{p_iq_j}{r_{ij}} = \log_2\sum_{i=1}^{n}\sum_{j=1}^{m} p_iq_j = \log_2\left(\sum_{i=1}^{n} p_i\right)\cdot\left(\sum_{j=1}^{m} q_j\right) = \log_2 1 = 0$$

We used Jensen's inequality with $a_{ij} = r_{ij}$ and $x_{ij} = p_iq_j/r_{ij}$.

Equality holds only if $\exists c\,\forall i\,\forall j : p_iq_j/r_{ij} = c$. Then also $\sum_{i=1}^{n}\sum_{j=1}^{m} p_iq_j = c\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}$. Both sums are equal to 1, hence $c = 1$, $p_iq_j = r_{ij}$, and $\mathbf{X}$ and $\mathbf{Y}$ are independent.

Theorem. $H(\mathbf{X},\mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y})$.

Proof. Let p_i, q_j, r_{ij} have the same meaning as before. Then

$$\Pr[\mathbf{X} = x_i|\mathbf{Y} = y_j] = \frac{\Pr[\mathbf{X} = x_i, \mathbf{Y} = y_j]}{\Pr[\mathbf{Y} = y_j]} = \frac{r_{ij}}{q_j} \quad .$$

$$H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y}) = -\sum_{j=1}^{m} q_j \log_2 q_j - \sum_{i=1}^{n}\sum_{j=1}^{m} q_j \frac{r_{ij}}{q_j} \log_2 \frac{r_{ij}}{q_j} =$$

$$-\left(\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} \log_2 q_j + \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} \log_2 \frac{r_{ij}}{q_j}\right) =$$

$$-\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} \log_2 r_{ij} = H(\mathbf{X},\mathbf{Y})$$

Corollary. $H(\mathbf{X}|\mathbf{Y}) \leq H(\mathbf{X})$ with equality iff $\mathbf{X}$ and $\mathbf{Y}$ are independent.

Theorem. In an encryption system, $H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C})$.

Proof.

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K},\mathbf{C}) - H(\mathbf{C}) = H(\mathbf{P},\mathbf{K},\mathbf{C}) - H(\mathbf{P}|\mathbf{K},\mathbf{C}) - H(\mathbf{C}) =^{1)}$$
$$H(\mathbf{P},\mathbf{K},\mathbf{C}) - H(\mathbf{C}) = H(\mathbf{P},\mathbf{K}) + H(\mathbf{C}|\mathbf{P},\mathbf{K}) - H(\mathbf{C}) =^{2)}$$
$$H(\mathbf{P},\mathbf{K}) - H(\mathbf{C}) =^{3)} H(\mathbf{P}) + H(\mathbf{K}) - H(\mathbf{C})$$

1. Ciphertext and key uniquely determine the plaintext, hence $H(\mathbf{P}|\mathbf{K},\mathbf{C}) = 0$.
2. Similarly, $H(\mathbf{C}|\mathbf{P},\mathbf{K}) = 0$.
3. Plaintext and key are independent — the key has been chosen beforehand and it should not influence the choice of the plaintext.

Exercises

- Show that the encryption system has perfect secrecy iff $H(\mathbf{P}|\mathbf{C}) = H(\mathbf{P})$.
- Show that $H(\mathbf{P}|\mathbf{C}) \leq H(\mathbf{K}|\mathbf{C})$.
- Compute $H(\mathbf{K}|\mathbf{C})$ and $H(\mathbf{K}|\mathbf{P}, \mathbf{C})$ for the affine cipher.

We know how to compute $H(\mathbf{K})$. But what is $H(\mathbf{P})$? How to estimate it? The possible values of $\mathbf{P}$ are meaningful texts. $\mathcal{P}$ is the set of strings over an alphabet (of, say, 26 letters).

The entropy of a random string of letters (uniformly chosen) is $\log_2 26 \approx 4.70$ per letter.

The entropy of a random string of letters (with probabilities of letters as in English) is ≈ 4.17 per letter.

But in a meaningful text, successive letters are not independent.

Let $\mathbf{P}^n$ be a random variable that ranges over plaintexts of length n with probabilities of the natural language L.

If we have a large enough corpus of texts then we can compute $\Pr[\mathbf{P}^n = s]$ for all $s \in \Sigma^n$, and also compute $H(\mathbf{P}^n)$.

Let $\mathbf{C}^n$ be the random variable ranging over n-letter ciphertexts.

The entropy H_L and the redundancy R_L of L (per letter) are

$$H_L = \lim_{n\to\infty} \frac{H(\mathbf{P}^n)}{n} \qquad\qquad R_L = 1 - \frac{H_L}{\log_2 |\Sigma|}$$

The limit exists because $(H(\mathbf{P}_n)/n)_n$ is a decreasing sequence bounded below by 0.

Various experiments estimate that $1.0 \leq H_{\text{English}} \leq 1.5$.

We have $H(\mathbf{P}^n) \geq nH_L = n(1 - R_L)\log_2 |\Sigma|$ and $H(\mathbf{C}^n) \leq n \log_2 |\Sigma|$. Hence

$$H(\mathbf{K}|\mathbf{C}^n) = H(\mathbf{K}) + H(\mathbf{P}^n) - H(\mathbf{C}^n) \geq H(\mathbf{K}) - nR_L \log_2 |\Sigma| \ .$$

If the encryption key is chosen uniformly then

$$H(\mathbf{K}|\mathbf{C}^n) \geq \log_2 |\mathcal{K}| - nR_L \log_2 |\Sigma| = \log_2 \frac{|\mathcal{K}|}{|\Sigma|^{nR_L}}$$

This inequality gives us some guarantees regarding the impossibility of completely determining the key from a ciphertexts. This guarantee vanishes if

$$\log_2 \frac{|\mathcal{K}|}{|\Sigma|^{nR_L}} \leq 0 \Leftrightarrow |\mathcal{K}| \leq |\Sigma|^{nR_L} \Leftrightarrow n \geq \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\Sigma|}$$

If we take $|\Sigma| = 26$, $|\mathcal{K}| = 26!$ (substitution cipher) and $R_L = 0.75$ (corresponding to $H_L \approx 1.18$) then the last fraction is ≈ 25.07. I.e. a ciphertext created using the substitution cipher should be uniquely decryptable if its length is at least 25.

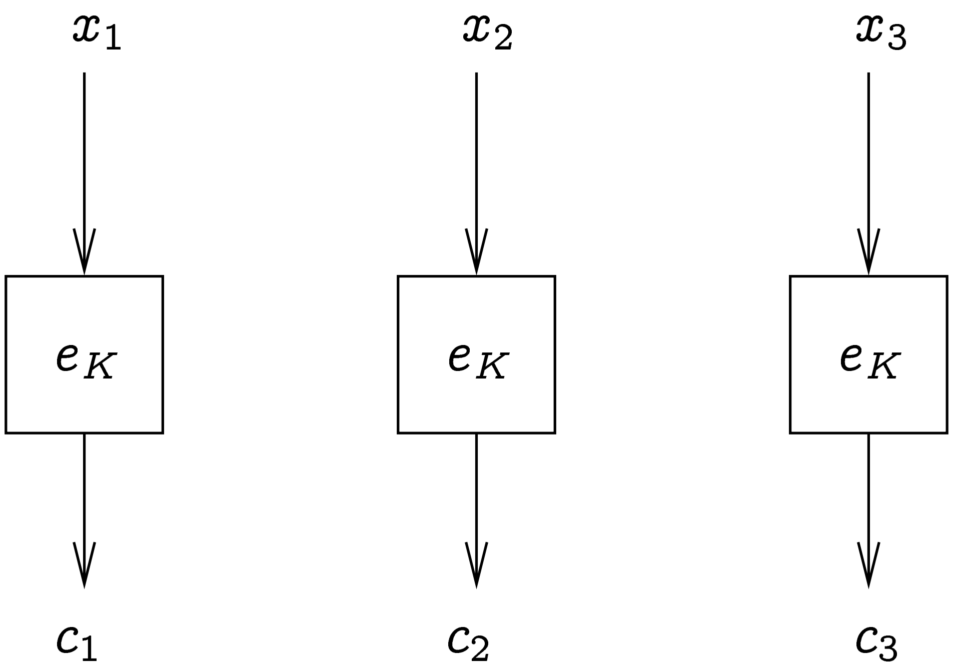
Block ciphers

- 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)



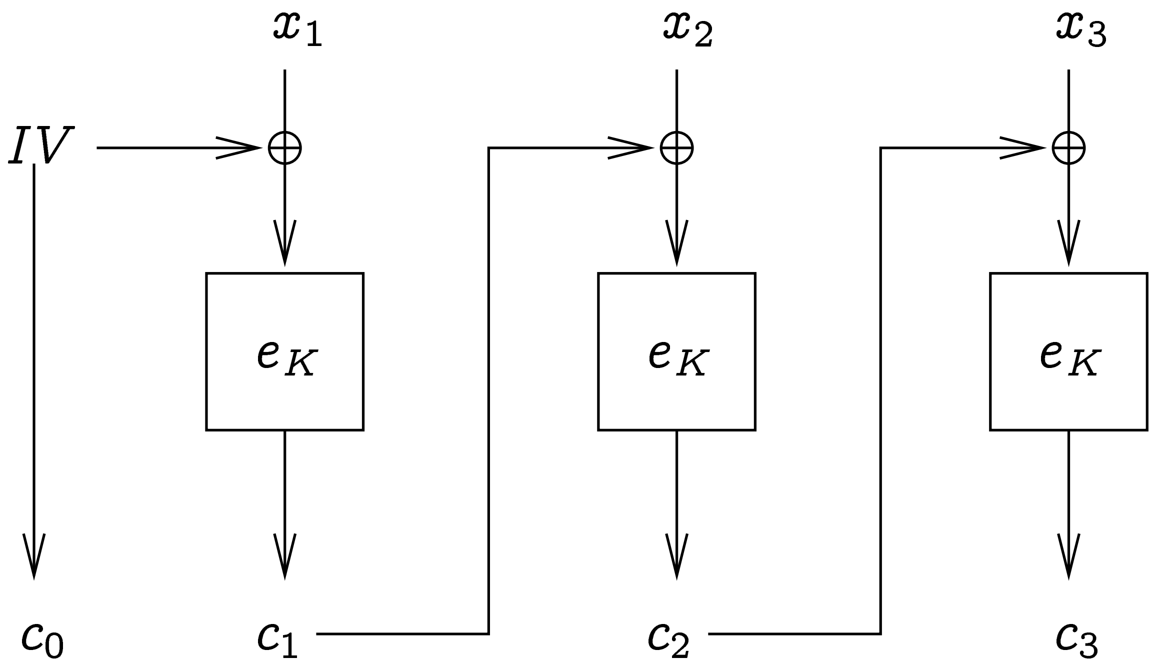
In our examples, this has been the mode we used.

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.

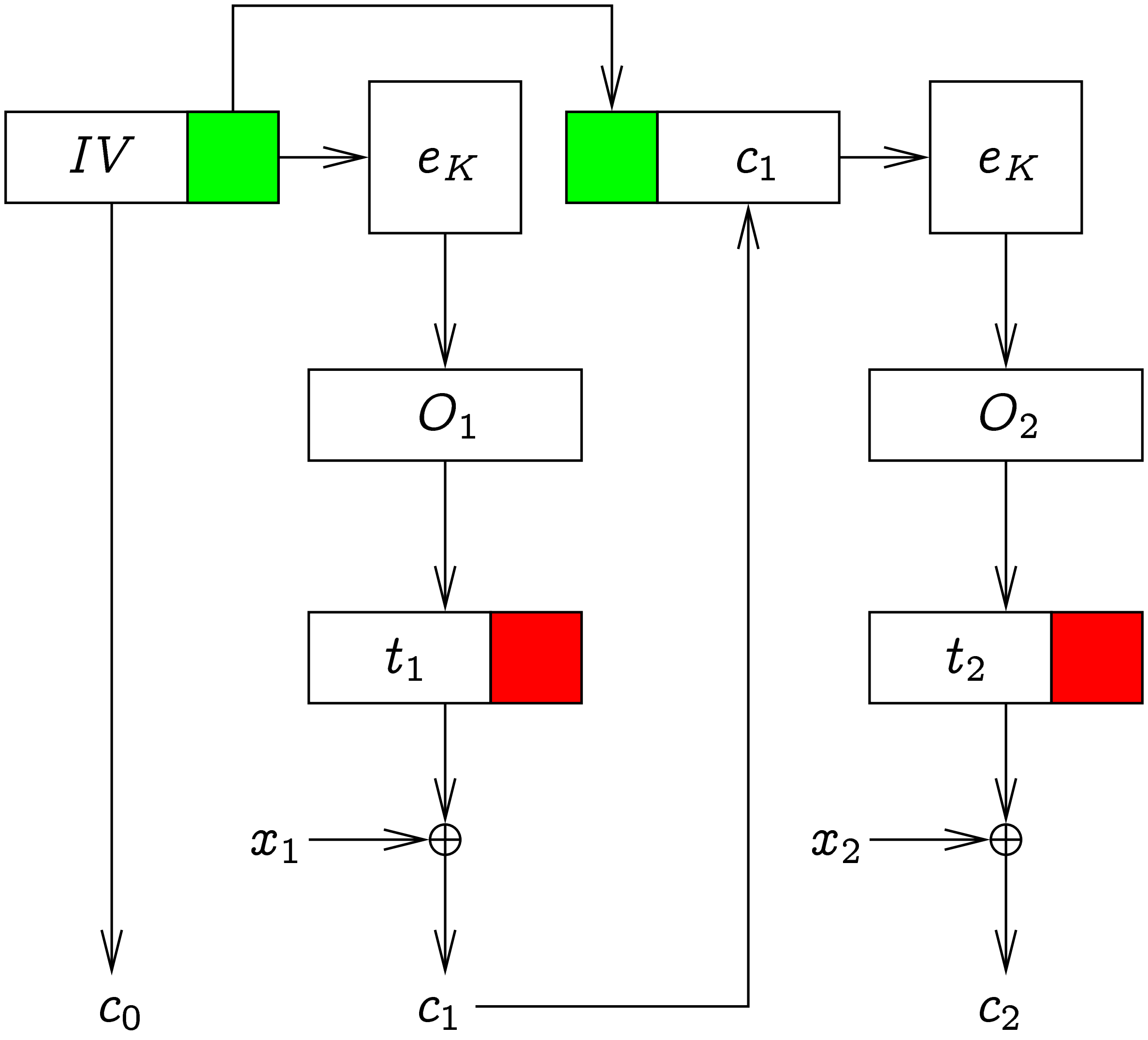
3. Bit errors in the i-th block affect the decoding of i-th and $(i+1)$-st blocks.

Exercise: how parallelizable are encoding and decoding?

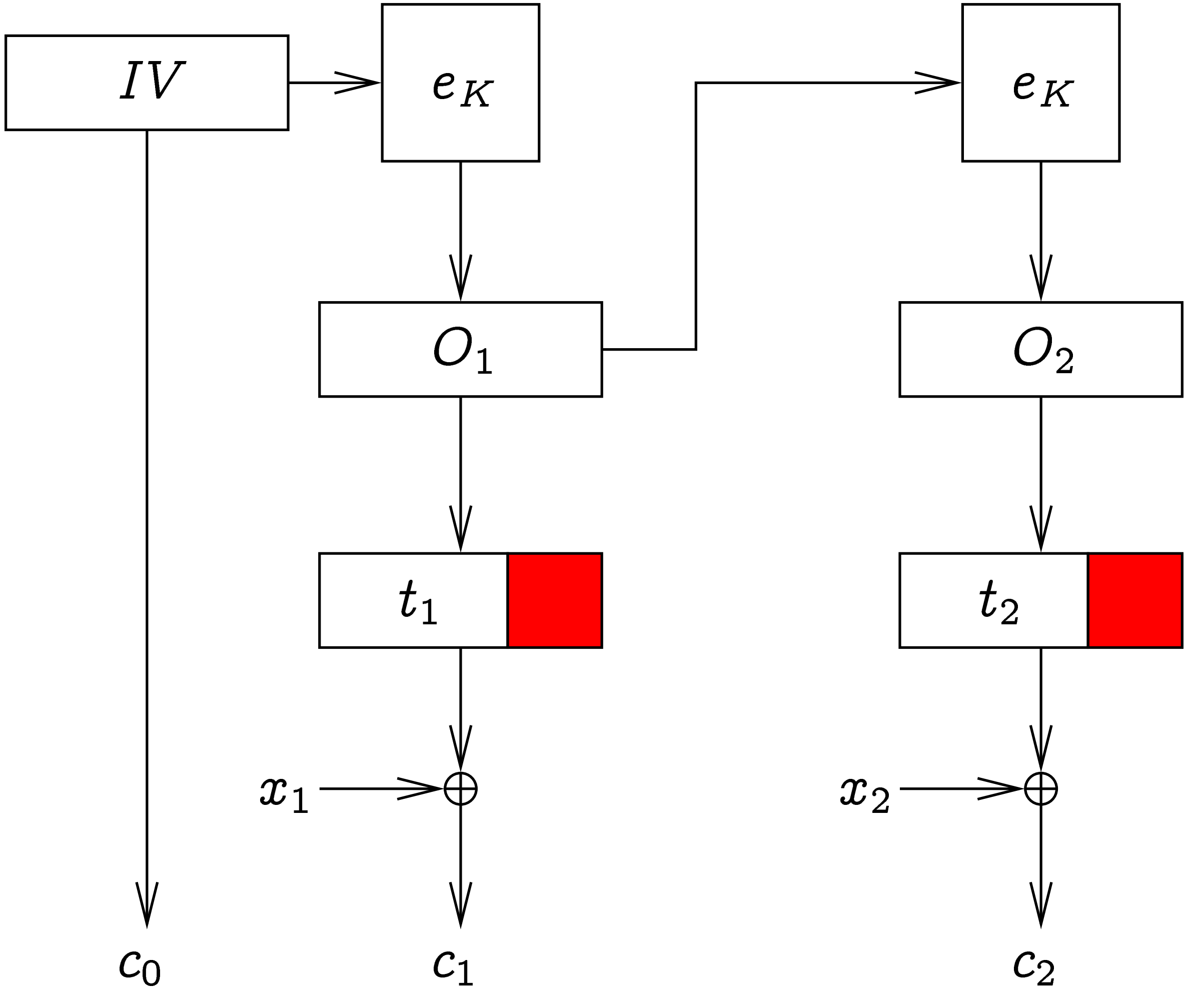
Exercise. Consider Vigenère cipher that has been employed in the CBC-mode. How to perform a ciphertext-only attack against it?

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

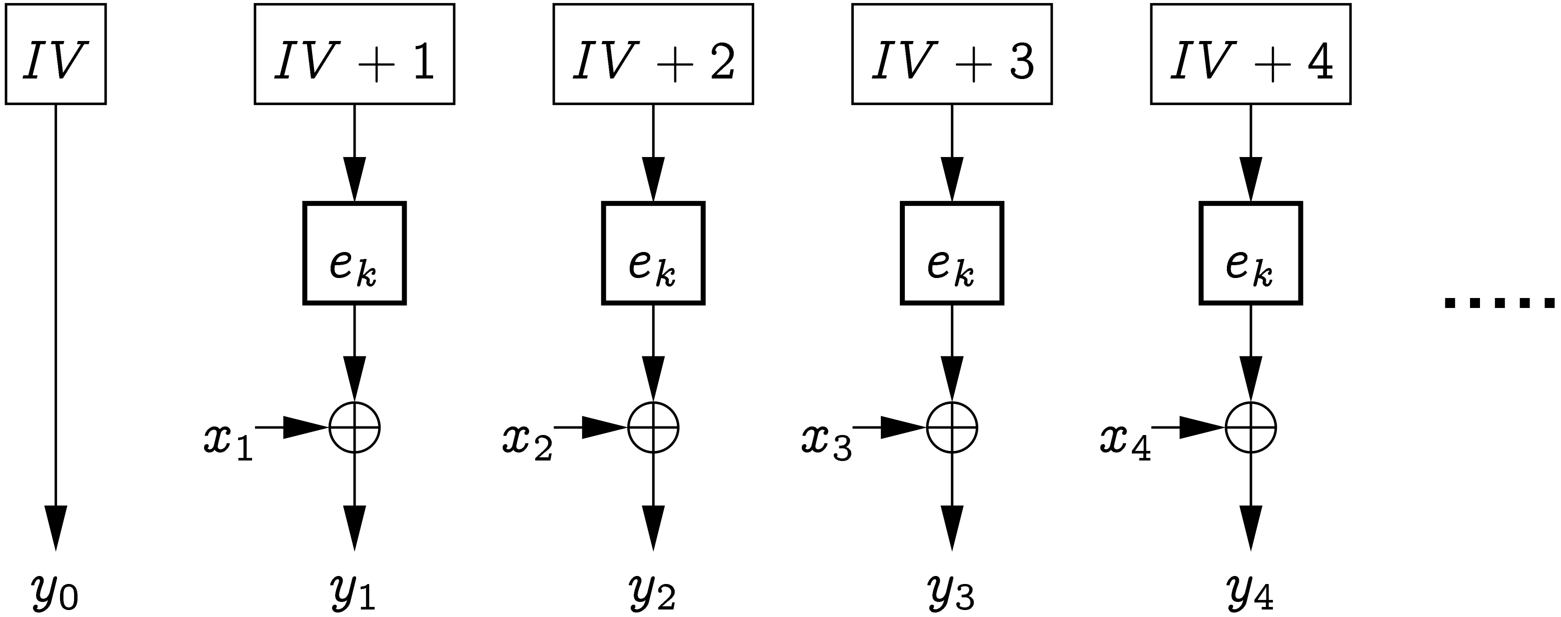
Cipher Feedback (CFB) mode



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.

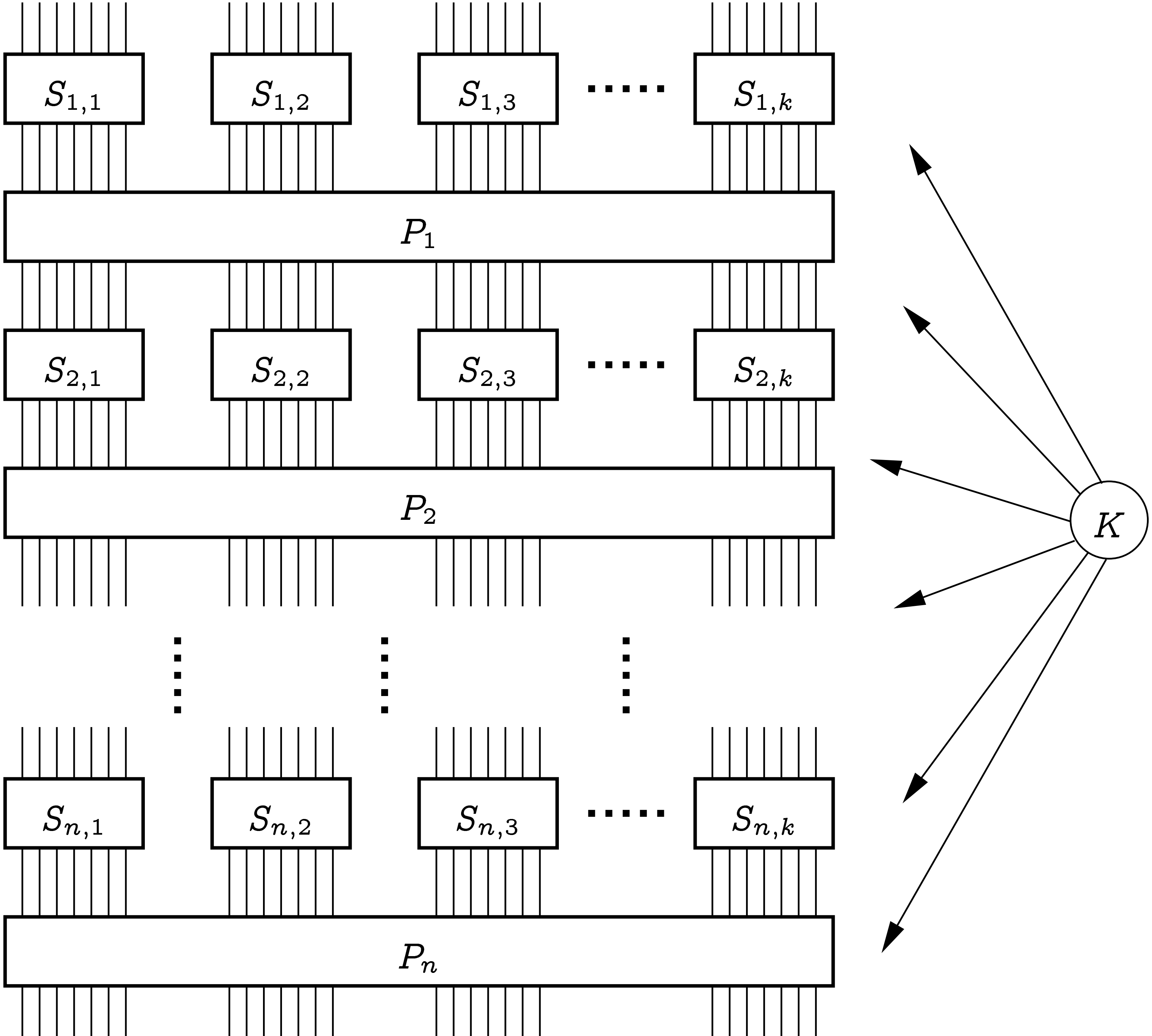
- Let a and b be two independently uniformly chosen elements of some finite ring R. Is $a \cdot b$ uniformly distributed? What if a were uniformly chosen from the multiplicative group R^*?

“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

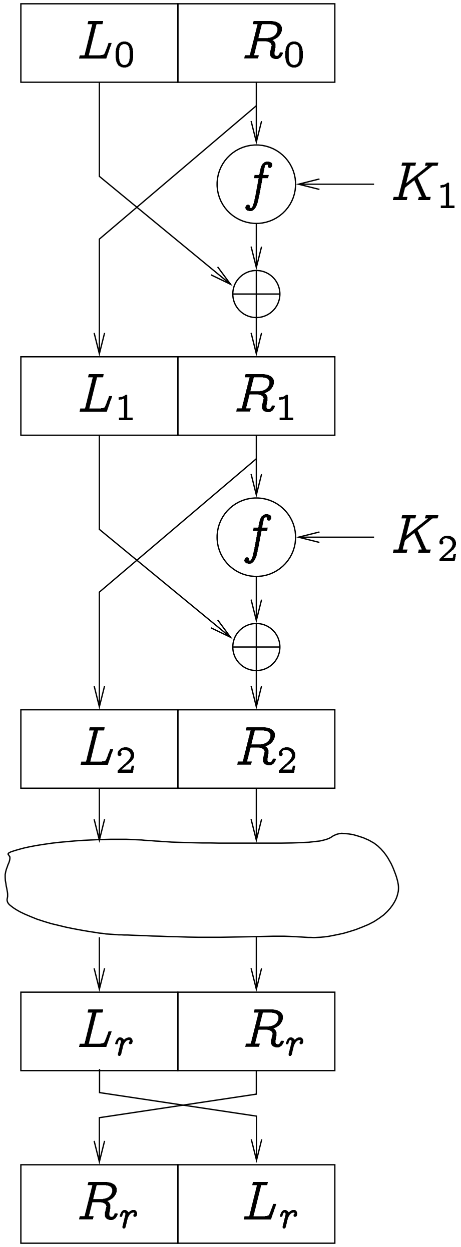
Hence “plokkšiffer”.

Modern block ciphers...



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

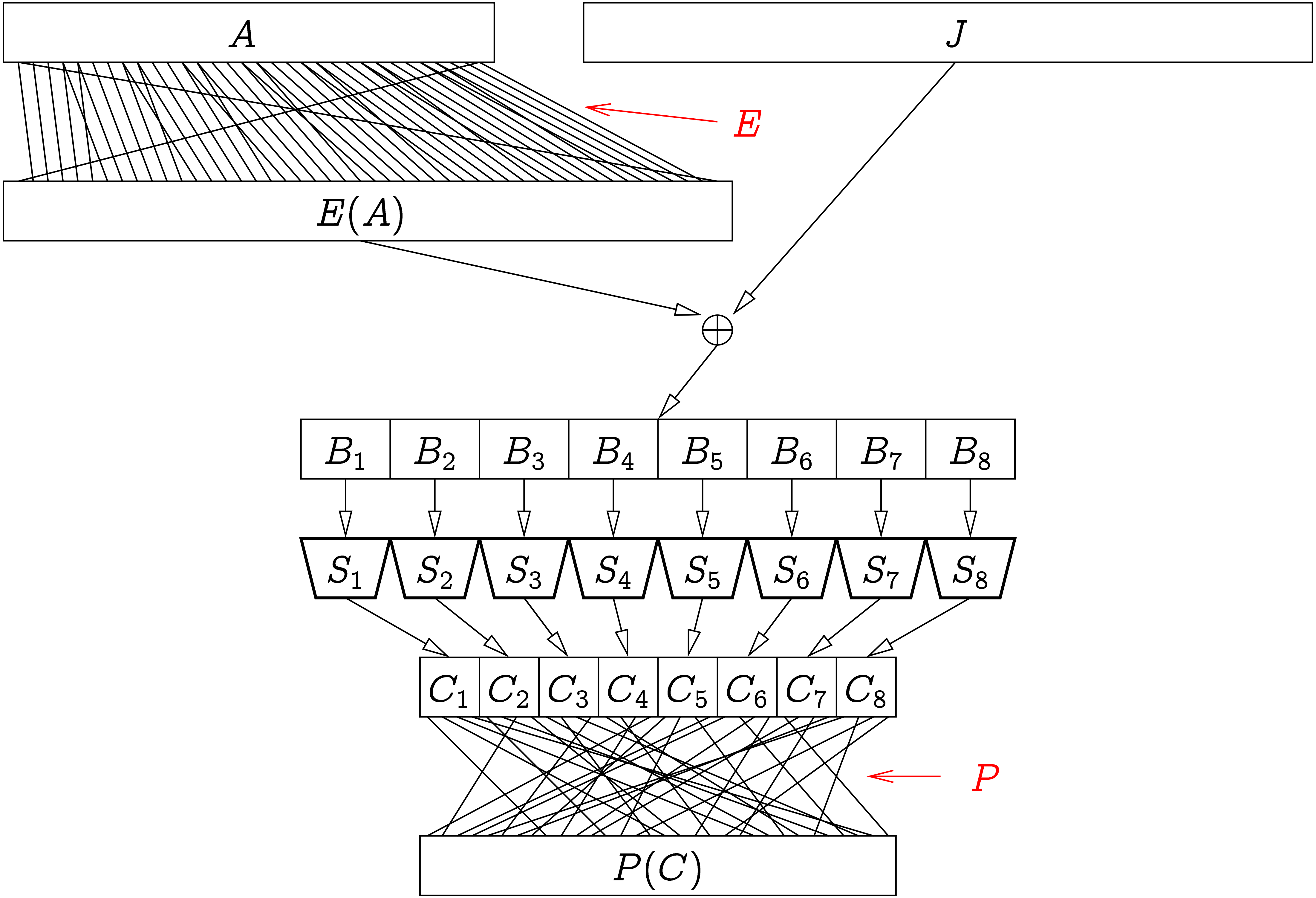
- $\mathcal{P} = \mathcal{C} = \{0,1\}^{64}$.
- $\mathcal{K} = \{0,1\}^{56}$.
- Encoding bit-string x with the key K:
  1. Let $x_0 = IP(x)$, where IP is a certain permutation of bits. Let L_0 $[R_0]$ be the first [last] 32 bits of x.
  2. 16 rounds of Feistel construction:

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

     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.

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


A
J
E
$E(A)$
$\oplus$
B_1
B_2
B_3
B_4
B_5
B_6
B_7
B_8
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
C_1
C_2
C_3
C_4
C_5
C_6
C_7
C_8
P
$P(C)$

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.

Differential cryptanalysis — a chosen-plaintext attack.

For reduced-round DES, it is more efficient than brute-force search.

n-round DES — $L_0R_0 \mapsto L_nR_n$. We ignore the bit-permutations IP, IP^{-1}, nor do we swap L_n and R_n.

Idea, given two bit-strings L_0R_0 and $L_0^*R_0^*$ with a fixed xor $L_0'R_0' = L_0R_0 \oplus L_0^*R_0^*$, we compare the xor-s of their encryptions. This will help us to exclude certain values for the key.

We attempt to reconstruct the xor-s of the intermediate computations.

Example: three-round DES. We'll attack the last round.

If the plaintext is $L_0 R_0$ and ciphertext is $L_3 R_3$ then

$$R_3 = L_2 \oplus f(R_2, K_3) = L_0 \oplus f(R_0, K_1) \oplus f(R_2, K_3)$$
$$L_3 = R_2 = L_1 \oplus f(R_1, K_2) = R_0 \oplus f(R_1, K_2)$$

Pick another plaintext $L_0^* R_0^*$. Then $R_3' = R_3 \oplus R_3^*$ equals

$$R_3' = L_0' \oplus f(R_0, K_1) \oplus f(R_0^*, K_1) \oplus f(R_2, K_3) \oplus f(R_2^*, K_3)$$

We choose $R_0^* = R_0$. Then $R_0' = \mathbf{0}^{32}$ and

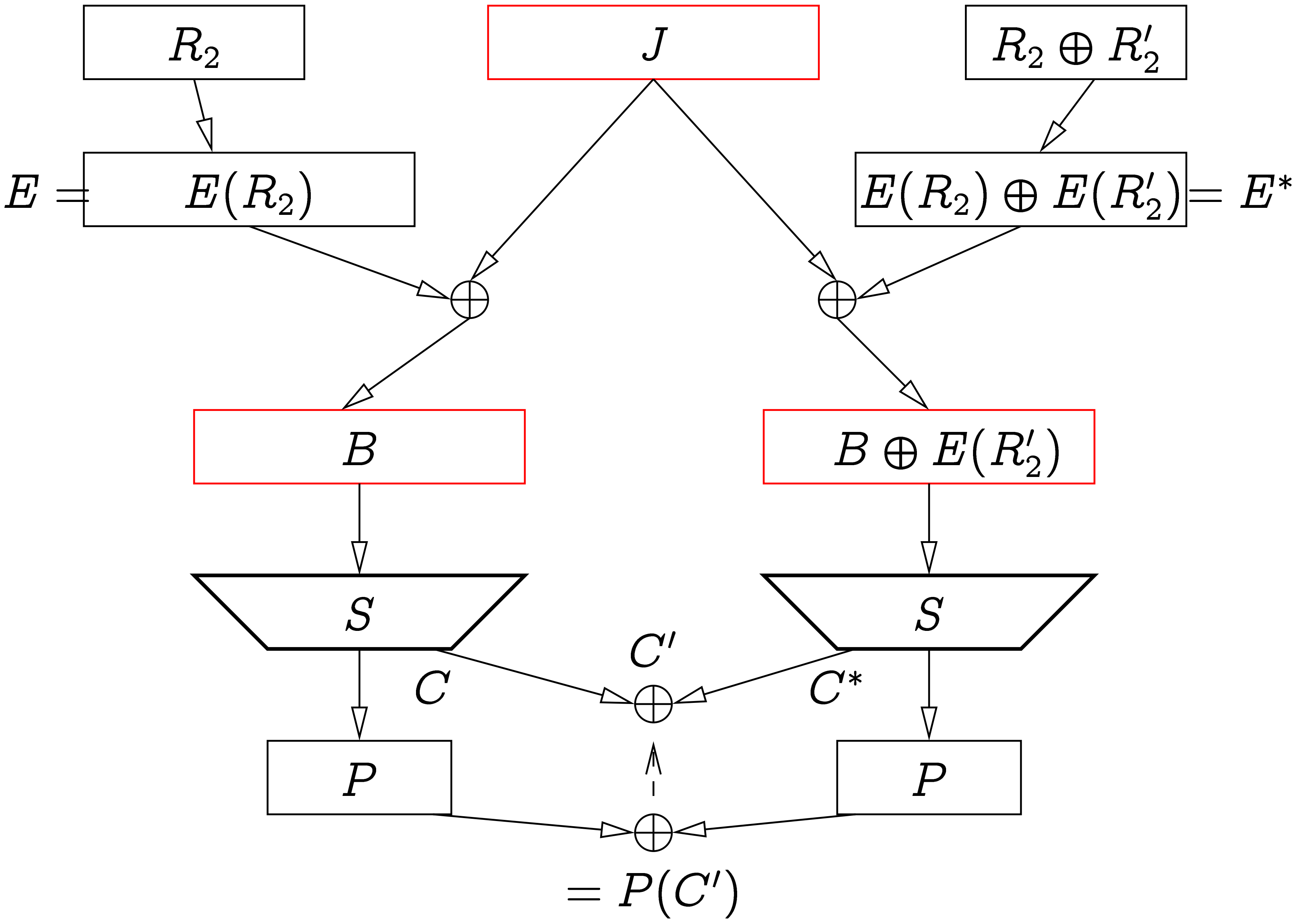
$$R_3' = L_0' \oplus f(R_2, K_3) \oplus f(R_2^*, K_3) \quad .$$

We know L_0' and R_3'. Hence we can compute

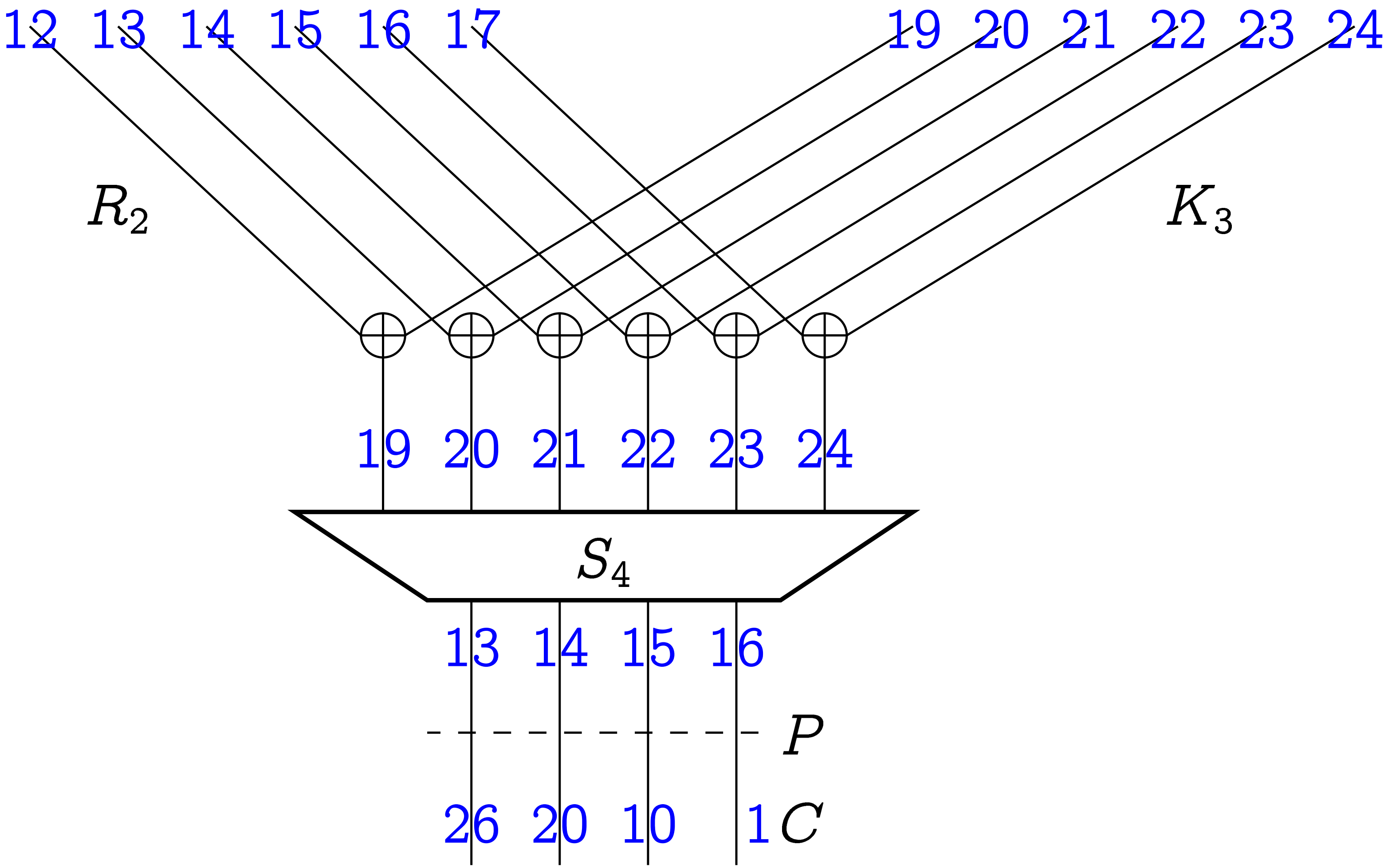
$$f(R_2, K_3) \oplus f(R_2^*, K_3) = R_3' \oplus L_0' \quad .$$

$f(R_2, K_3) = P(C)$ and $f(R_2^*, K_3) = P(C^*)$ for some S-box outputs C and C^*. We have $C' = C \oplus C^* = P^{-1}(R_3' \oplus L_0')$.

We know $R_2 = L_3$ and $R_2^* = L_3^*$. The inputs to the S-box are $E(R_2) \oplus K_3$ and $E(R_2^*) \oplus K_3$.


R_2
J
$R_2 \oplus R'_2$
$E =$
$E(R_2)$
$E(R_2) \oplus E(R'_2)$
$= E^*$
B
$B \oplus E(R'_2)$
S
S
C'
C
C^*
P
P
$= P(C')$

We know E, E^*, C' for the third round. Consider a single S-box, for example S_4.



- $R_2^4 := R_2[12, \ldots, 17]$; $R_2^{*4} := R_2^*[12, \ldots, 17]$
- $K_3^4 := K_3[19, \ldots, 24]$
- $C'^4 := C'[26, 20, 10, 1]$

K_3^4 must be such that $S_4(R_2^4 \oplus K_3^4) \oplus S_4(R_2^{*4} \oplus K_3^4) = C'^4$.

$test_i(E^i, E^{*i}, C'^i) := \{K^i \in \{0,1\}^6 \mid S_i(E^i \oplus K^i) \oplus S_i(E^{*i} \oplus K^i) = C'^i\}$

All such sets $test_i(E^i, E^{*i}, C'^i)$ will be precomputed.

Exercise. How many such sets are there? How much memory will they need?

Exercise. If $K^i \in test_i(E^i, E^{*i}, C'^i)$ then a certain $\bar{K}^i$ is definitely also a member of $test_i(E^i, E^{*i}, C'^i)$. Which one?

We have excluded certain 6-bit strings from the values of K_3^i for $i \in \{1, \ldots, 8\}$.

By considering more pairs L_0R_0 and $L_0^*R_0^*$ we'll exclude more. Eventually we'll converge on a single value.

The subkey K_3 consists of 48 bits. We'll brute-force the remaining 8.

We chose L_0R_0 and $L_0^*R_0^*$ so, that $R_0 \oplus R_0^* = 00000000_{16}$.

What if we had chosen differently, say $R_0 \oplus R_0^* = 20000000_{16}$?

$$R_3' = L_0' \oplus f(R_0, K_1) \oplus f(R_0^*, K_1) \oplus f(R_2, K_3) \oplus f(R_2^*, K_3)$$

Before we had $f(R_0, K_1) \oplus f(R_0^*, K_1) = 00000000_{16}$. What is its value now?

Only the inputs to the first S-box are different. Only the outputs of the first S-box are different, too.

The permutation P maps 4 first bits to positions $[9, 17, 23, 31]$.

$$f(R_0, K_1) \oplus f(R_0^*, K_1) = 00000000?0000000?00000?0000000?0_2$$

$P(C') = f(R_2, K_3) \oplus f(R_2^*, K_3)$ still equals $R_3' \oplus L_0'$, except for bits $9, 17, 23, 31$.

C' still equals $P^{-1}(R_3' \oplus L_0')$, except for bits $1, 2, 3, 4$.

We cannot argue about K_3^1. We still can argue about $K_3^2, \ldots, K_3^8$.

Example: six-round DES.

$$R_6 = R_4 \oplus f(R_5, K_6) = L_3 \oplus f(R_3, K_4) \oplus f(R_5, K_6)$$

$$R'_6 = L'_3 \oplus f(R_3, K_4) \oplus f(R^*_3, K_4) \oplus f(R_5, K_6) \oplus f(R^*_5, K_6)$$

We try to find K_6.

We do not know L'_3 nor R'_3. But we can choose $L'_0 R'_0$ so that certain values are highly likely.

We try to make so, that this highly likely value for R'_3 has just a few bits equal to 1.

A one-round characteristic is a quantity

$$L_0' R_0' \overset{p_1}{\to} L_1' R_1'$$

where

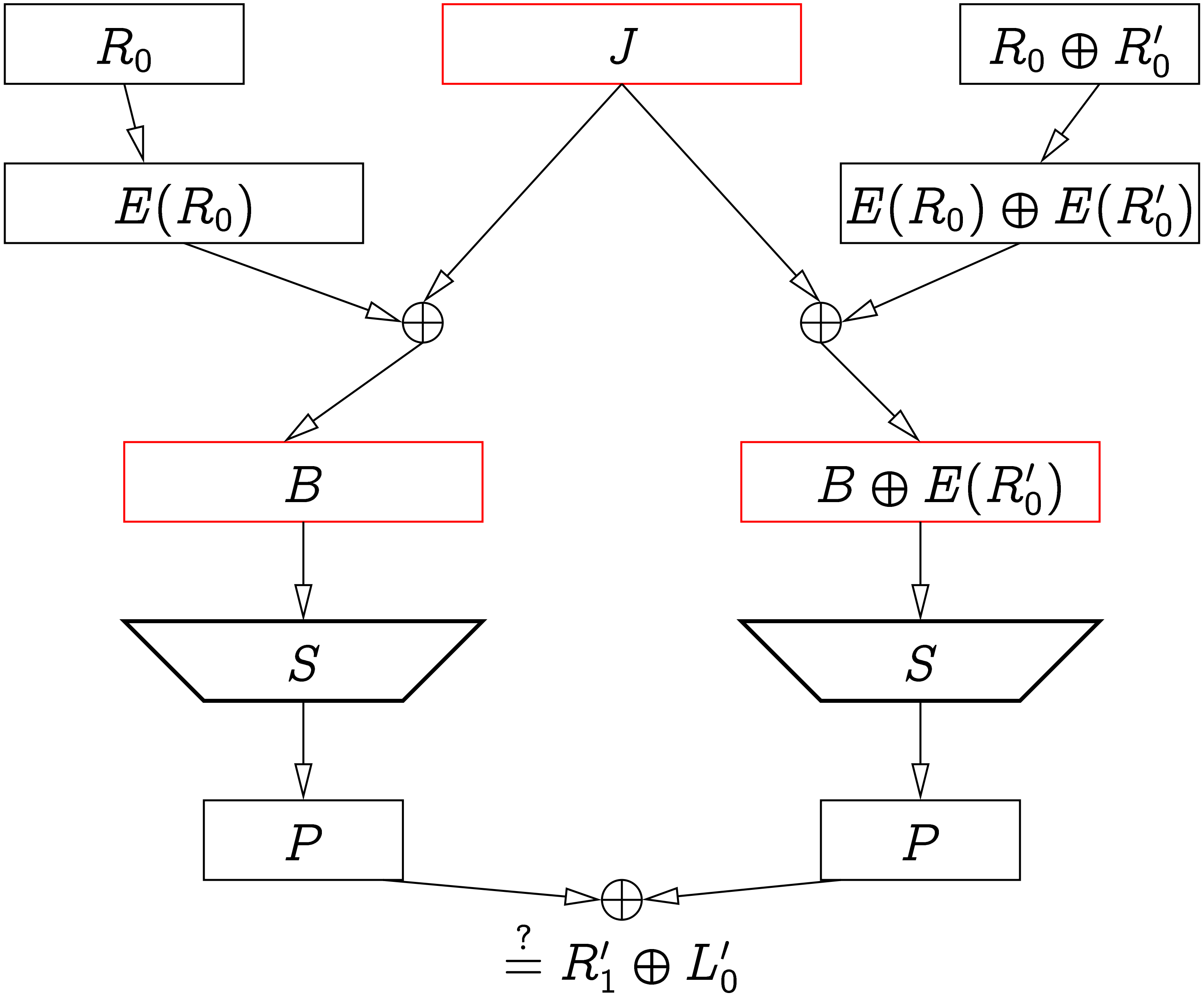
- $L_1' = R_0'$;
- For any choice of L_0, R_0, the quantity p_1 is the probability that (taken over uniformly chosen $J \in \{0,1\}^{48}$)

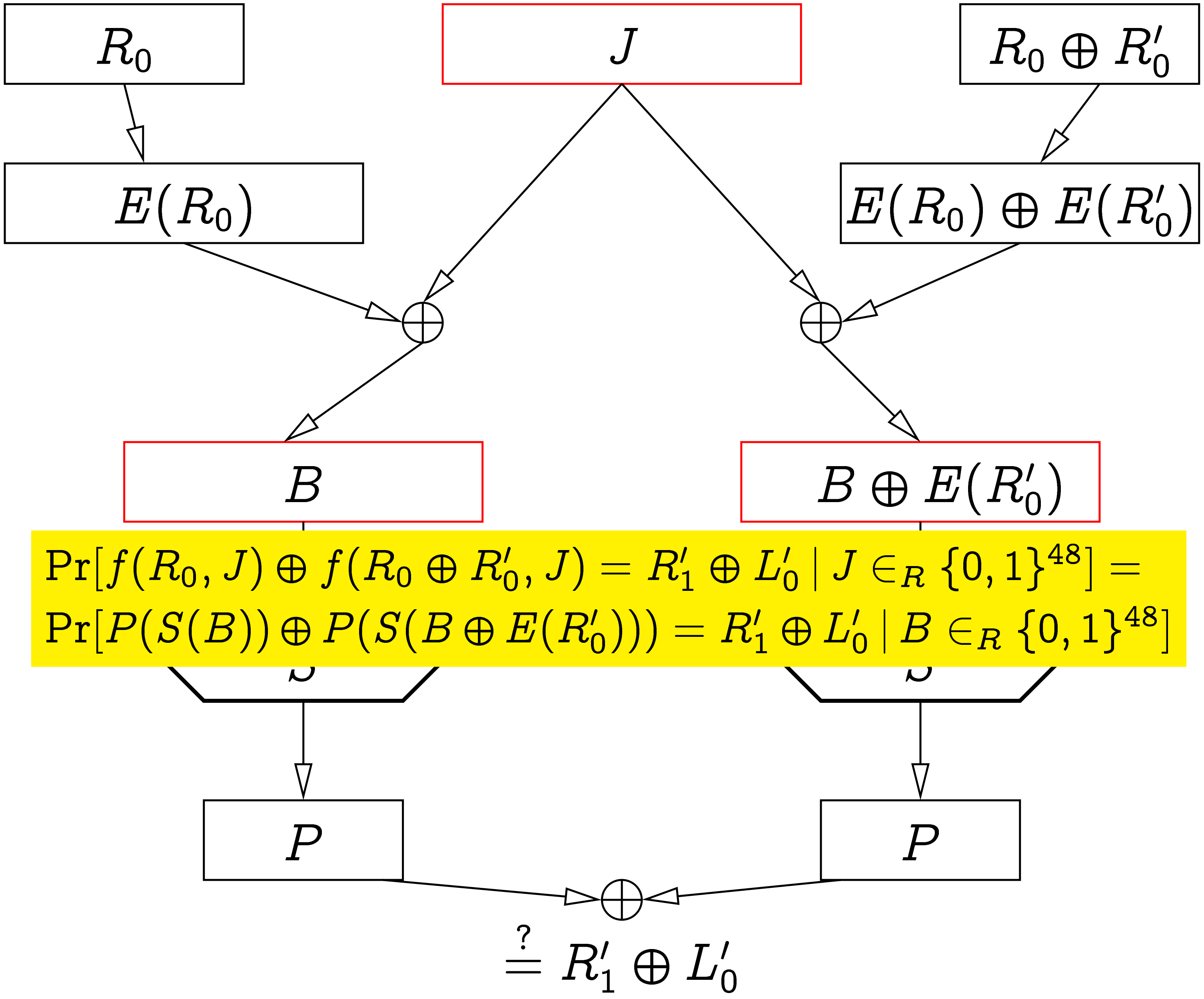
  $$\big(L_0 \oplus f(R_0, J)\big) \oplus \big((L_0 \oplus L_0') \oplus f(R_0 \oplus R_0', J)\big) = R_1'$$

  or that

  $$f(R_0, J) \oplus f(R_0 \oplus R_0', J) = R_1' \oplus L_0' \enspace .$$

That probability does not depend on R_0 either.


R_0
J
$R_0 \oplus R'_0$
$E(R_0)$
$E(R_0) \oplus E(R'_0)$
B
$B \oplus E(R'_0)$
S
S
P
P
$\overset{?}{=} R'_1 \oplus L'_0$



$$\Pr[f(R_0, J) \oplus f(R_0 \oplus R_0', J) = R_1' \oplus L_0' \mid J \in_R \{0,1\}^{48}] =$$
$$\Pr[P(S(B)) \oplus P(S(B \oplus E(R_0'))) = R_1' \oplus L_0' \mid B \in_R \{0,1\}^{48}]$$

An n-round characteristic is

$$L'_0 R'_0 \xrightarrow{p_1} L'_1 R'_1 \xrightarrow{p_2} \cdots \xrightarrow{p_n} L'_n R'_n$$

where each $L'_{i-1} R'_{i-1} \xrightarrow{p_i} L'_i R'_i$ is a one-round characteristic.

The probability of such a characteristic is $p_1 \cdots p_n$.

Some one-round characteristics:

$$\begin{array}{ccc} xxxxxxxx_{16}|00000000_{16} & \overset{1}{\to} & 00000000_{16}|xxxxxxxx_{16} \\ 00000000_{16}|60000000_{16} & \overset{14/64}{\to} & 60000000_{16}|00808200_{16} \end{array}$$

Second example: $E(R'_0) = 001100\cdots0_2$. Hence the inputs to S-boxes $S_2,\ldots,S_8$ are equal, but the inputs to S_1 differ by 001100.

The probability that the outputs to S_1 differ by $x \in \{0,1\}^4$ is

$$\frac{|\{B \in \{0,1\}^6 \mid S_1(B) \oplus S_1(B \oplus 001100_2) = x\}|}{64} \enspace .$$

If $x = 1110_2$ then this quantity equals $14/64$.

The output difference of S-boxes is $111000\cdots0_2$ with probability $14/64$. The bit-permutation P brings those three 1-s to the positions shown above.

Example: six-round DES.

$$R_6 = R_4 \oplus f(R_5, K_6) = L_3 \oplus f(R_3, K_4) \oplus f(R_5, K_6)$$

$$R_6' = L_3' \oplus f(R_3, K_4) \oplus f(R_3^*, K_4) \oplus f(R_5, K_6) \oplus f(R_5^*, K_6)$$

We try to find K_6.

A three-round characteristic:

$$40080000_{16}|04000000_{16} \overset{1/4}{\rightarrow} 04000000_{16}|00000000_{16} \overset{1}{\rightarrow}$$

$$00000000_{16}|04000000_{16} \overset{1/4}{\rightarrow} 04000000_{16}|40080000_{16}$$

If $L_0'R_0' = 40080000_{16}|04000000_{16}$ then
$L_3'R_3' = 04000000_{16}|40080000_{16}$ with probability $1/16$.

Assume that this happens, i.e. we know L_3' and R_3'. We also know R_6' and $R_5' = L_6'$.

$E(R_3') = 001000|000000|000001|010000|0\cdots0$. I.e. the input (and also output) xor-s to S_2, S_5, S_6, S_7, S_8 in the fourth round are zero. We try to find the corresponding 30 bits of K_6.

$$R_6' = L_3' \oplus f(R_3, K_4) \oplus f(R_3^*, K_4) \oplus f(R_5, K_6) \oplus f(R_5^*, K_6)$$

and certain 20 bits of $f(R_3, K_4)$ and $f(R_3^*, K_4)$ are equal. These 20 bits in $f(R_5, K_6) \oplus f(R_5^*, K_6)$ are equal to the same bits in R_6'.

We know the output xor-s of S_2, S_5, S_6, S_7, S_8 in the sixth round. We also know the inputs to these S-boxes (as we know $R_5 = L_6$ and $R_5^* = L_6^*$).

We know the triples E_i, E_i^*, C_i' for the sixth round, where $i \in \{2, 5, 6, 7, 8\}$. We can compute the sets $test_i$ and find the candidate keys.

We also get noise (because our certainty in $L_3'R_3'$ was only $1/16$), but the right key should stick out.

To find the right key more quickly:

We have the plaintext pairs $(x_1, x_1^*), \ldots, (x_N, x_N^*)$ with $x_i \oplus x_i^* = L_0'R_0'$.

Each of these pairs defines a quintuple of sets $(test_2^{(i)}, test_5^{(i)}, test_6^{(i)}, test_7^{(i)}, test_8^{(i)})$.

For each i: if this quintuple of sets contains the empty set, then discard it.

A set $\{i_1, \ldots, i_n\} \subseteq \{1, \ldots, N\}$ is allowable if

$$\bigcap_{k=1}^{n} test_j^{(i_k)} \neq \emptyset \text{ for all } j \in \{2, 5, 6, 7, 8\} \quad .$$

We search for an allowable set of maximum cardinality (using backtracking).

We have found 30 bits of the key. The characteristic

$$00200008_{16}|00000400_{16} \overset{1/4}{\to} 00000400_{16}|00000000_{16} \overset{1}{\to} 00000000_{16}|00000400_{16} \overset{1/4}{\to} 00000400_{16}|00200008_{16}$$

allows us to find further 12 (those corresponding to the inputs of S_1 and S_4). The remaining 14 bits can be brute-forced.

A two-round characteristic:

$$19600000_{16}|00000000_{16} \xrightarrow{1} 00000000_{16}|19600000_{16}$$
$$\xrightarrow{14 \cdot 8 \cdot 10/(64)^3} 19600000_{16}|00000000_{16}$$

The second fraction is about $1/234$. Iterating this characteristic 6.5 times gives a 13-round characteristic of probability $1/234^6$. This is the best-known characteristic for cryptanalysing full 16-round DES.

Linear cryptanalysis.

Let the key K be fixed. What is the probability p of

$$P_{i_1} \oplus \cdots \oplus P_{i_r} \oplus C_{j_1} \oplus \cdots \oplus C_{j_s} \oplus K_{k_1} \oplus \cdots \oplus K_{k_t} = 1$$

where P and C are the plaintext and ciphertext and X_i is the i-th bit of X? The indices $i_\star, j_\star, k_\star$ are fixed. The plaintext P is uniformly distributed.

- For an "ideal" cipher: $1/2$.
- If (say) $p > 1/2$, then there is a known-plaintext attack:
  - Obtain sufficiently many pairs (P, C).
  - Compute $P_{i_1} \oplus \cdots \oplus P_{i_r} \oplus C_{j_1} \oplus \cdots \oplus C_{j_s}$.
  - If the computed bit is 1 for more than half of pairs (P, C), then $K_{k_1} \oplus \cdots \oplus K_{k_t} = 0$. Otherwise $K_{k_1} \oplus \cdots \oplus K_{k_t} = 1$.

- From the construction of the cipher we find the indices $i_1, \ldots, i_r, j_1, \ldots, j_s, k_1, \ldots, k_t$ for which the probability p is as far from $1/2$ as possible.
- We need several such tuples to determine several bits of the key.
- To break the cipher, we need $O(|p - 1/2|^2)$ plaintext-ciphertext pairs.