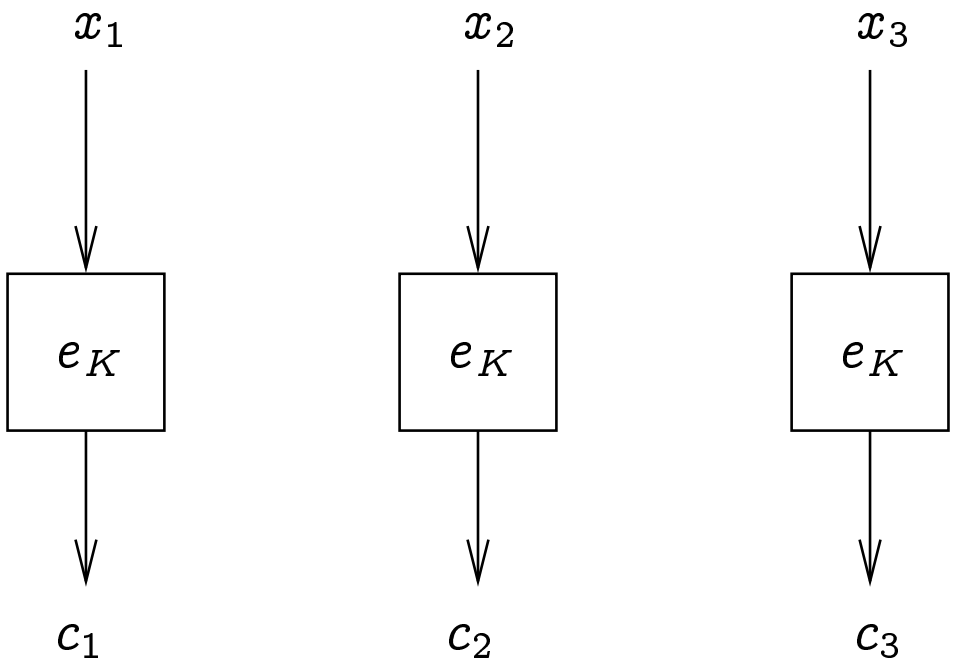
Block ciphers

- 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)



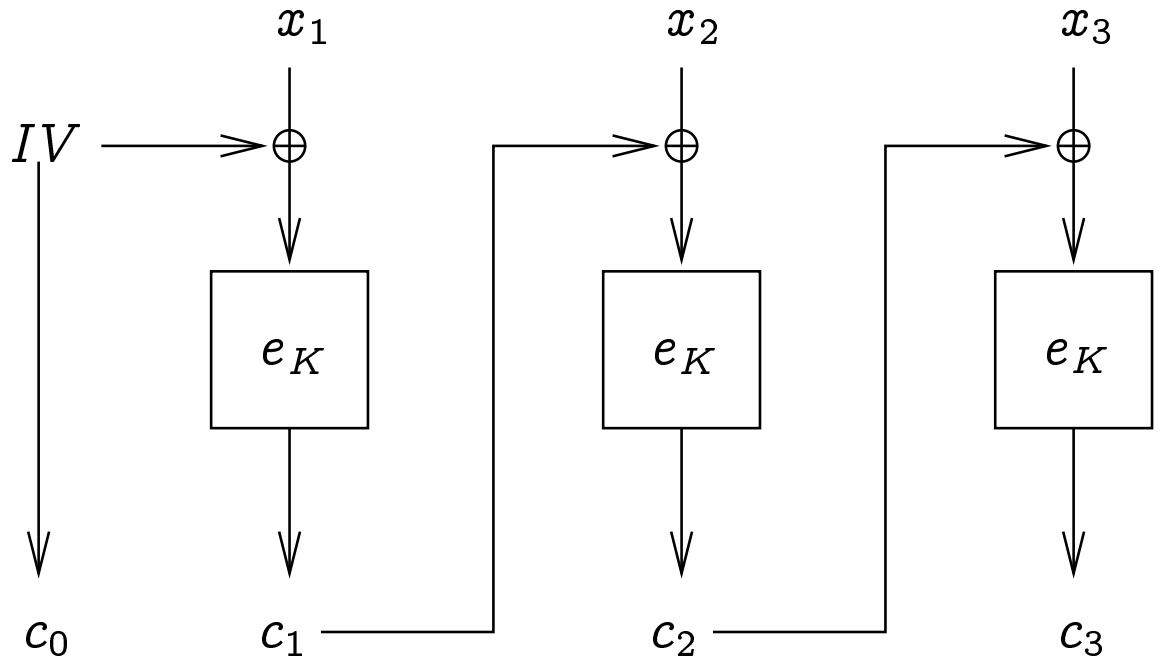
In our examples, this has been the mode we used.

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

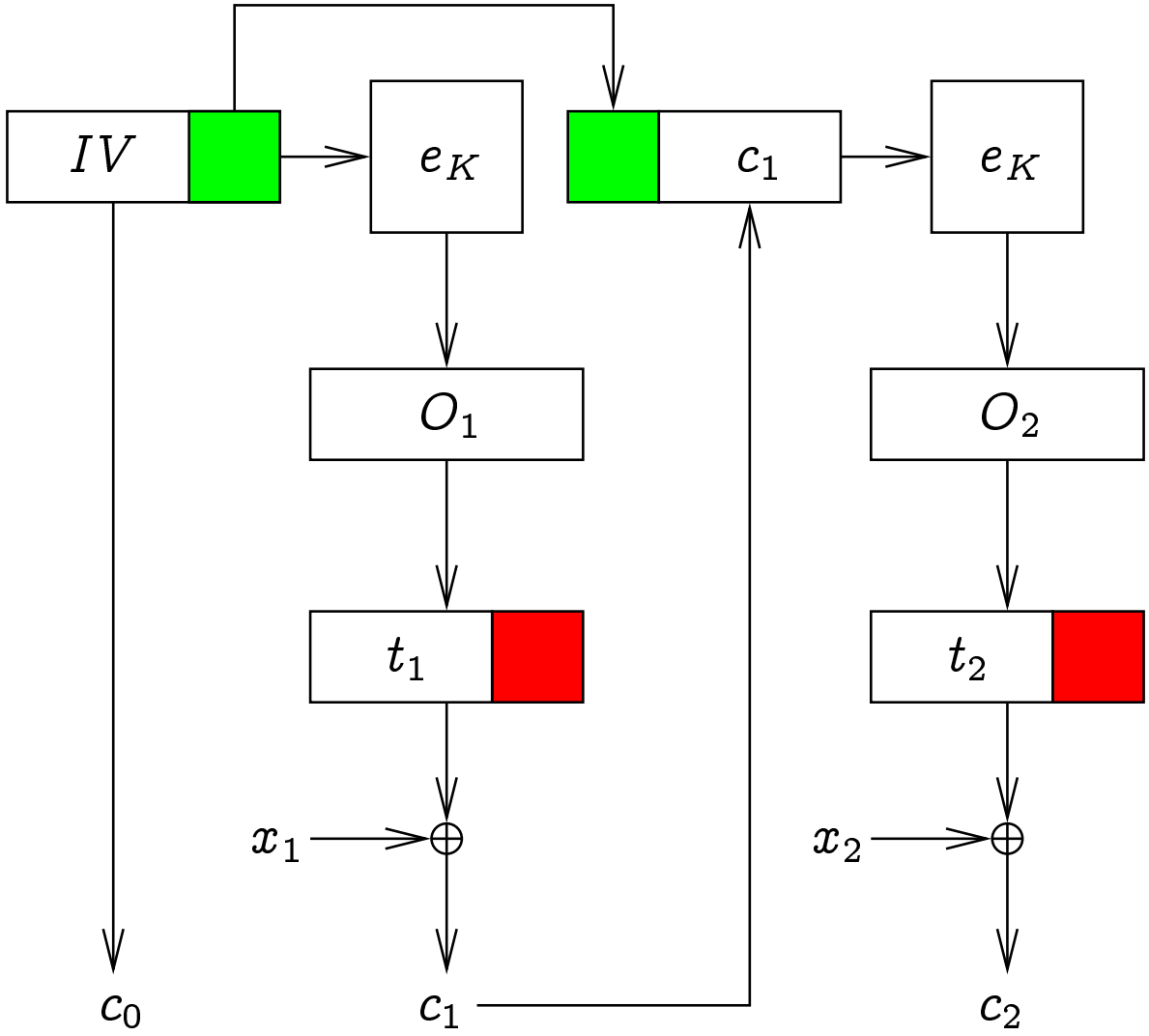
1. Encoding the same plaintext twice with different values of the IV yields different ciphertexts.
2. Reordering the blocks yields garbage as decoded plaintext after the point of reordering. Deleting a number of blocks from the end of the ciphertext does not yield garbage.
3. Bit errors in the i-th block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

Exercise: how parallelizable are encoding and decoding?

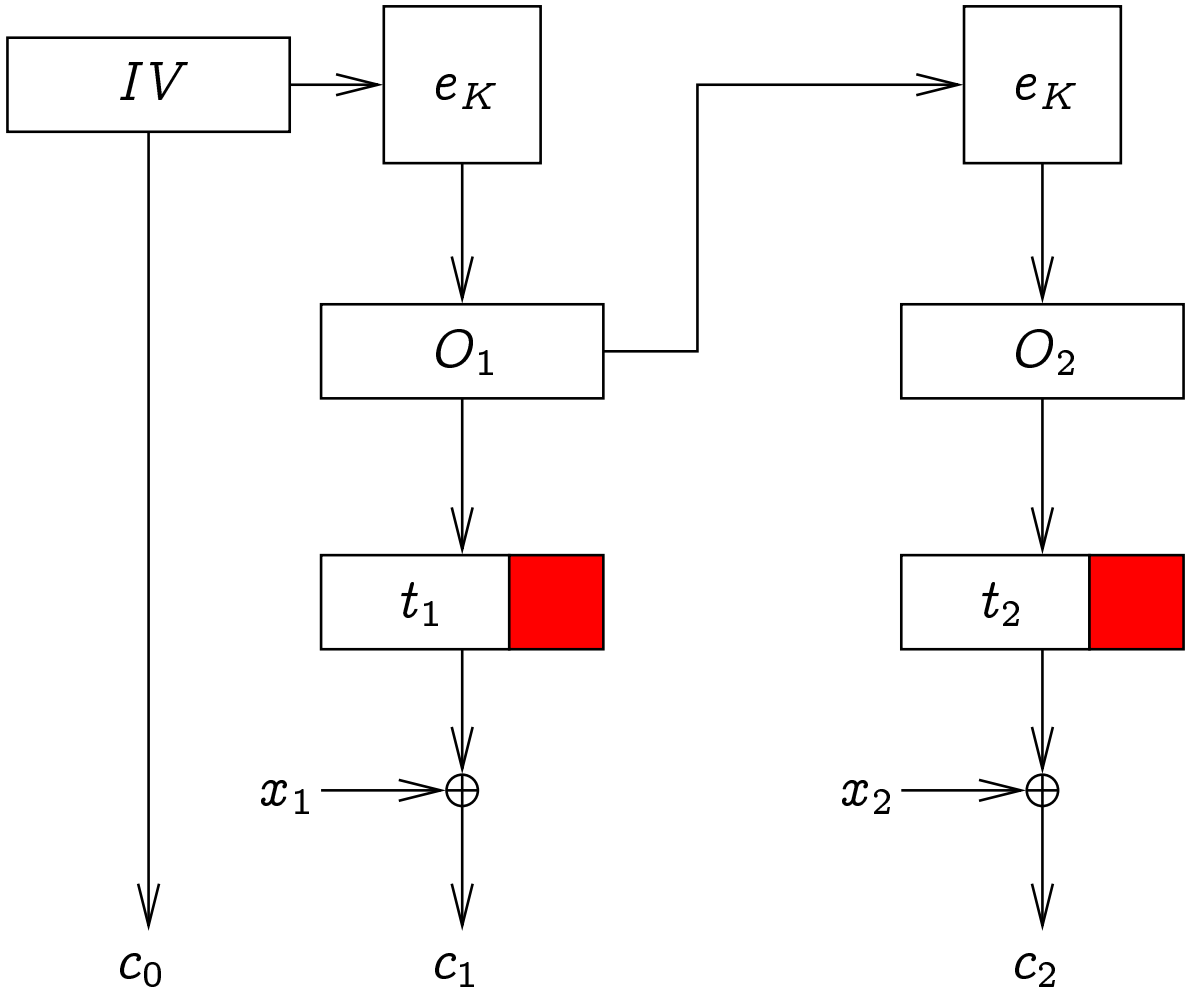
Exercise. Consider Vigenère cipher that has been employed in the CBC-mode. How to perform a ciphertext-only attack against it?

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

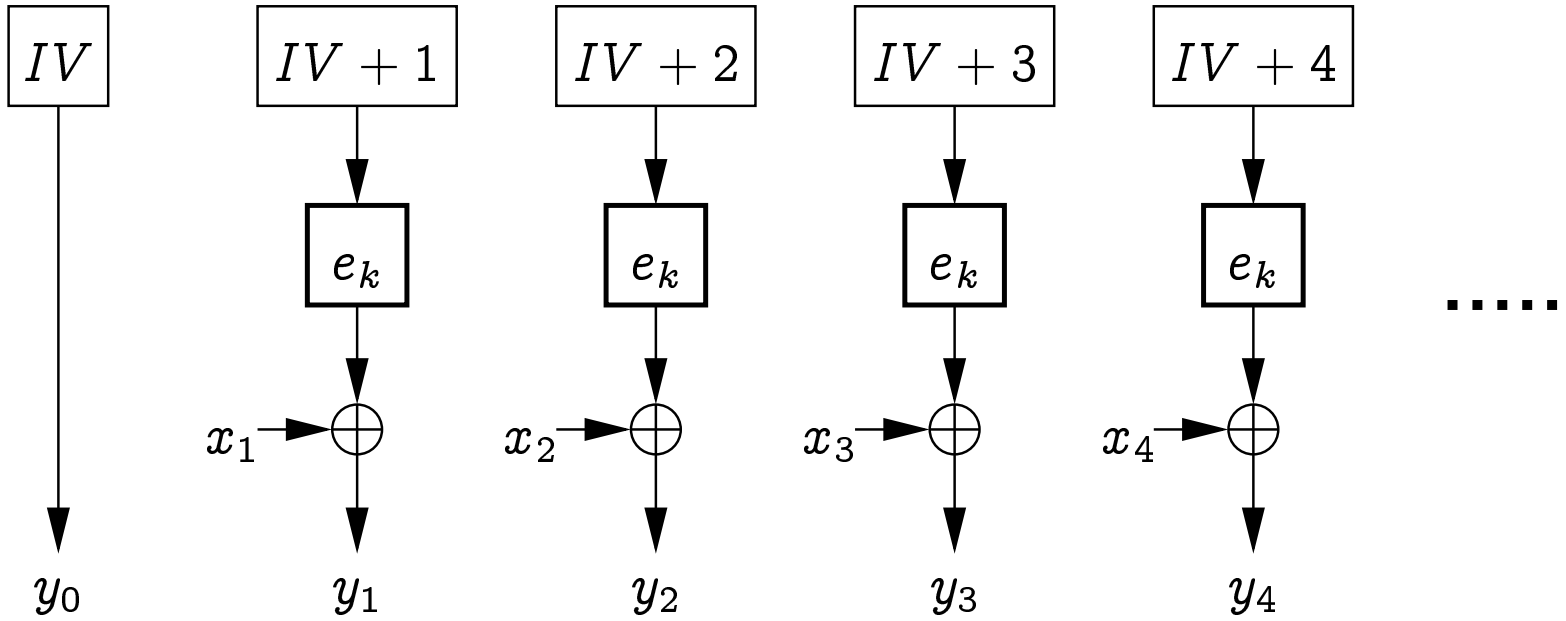
Cipher Feedback (CFB) mode



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

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

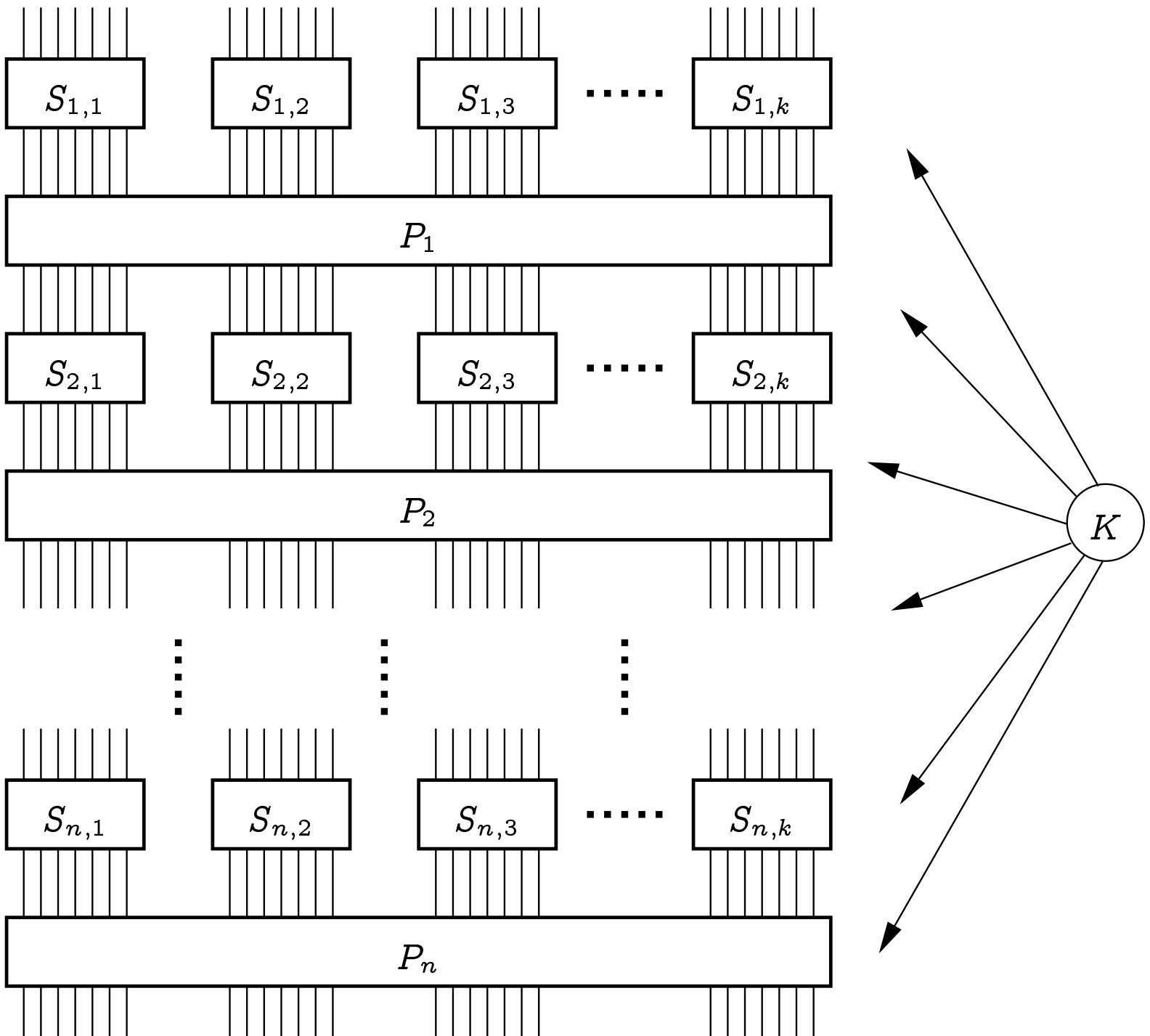
Let $\mathbf{V}_n$ be the Vigenère cipher with the key length n. What can be said about

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

More exercises

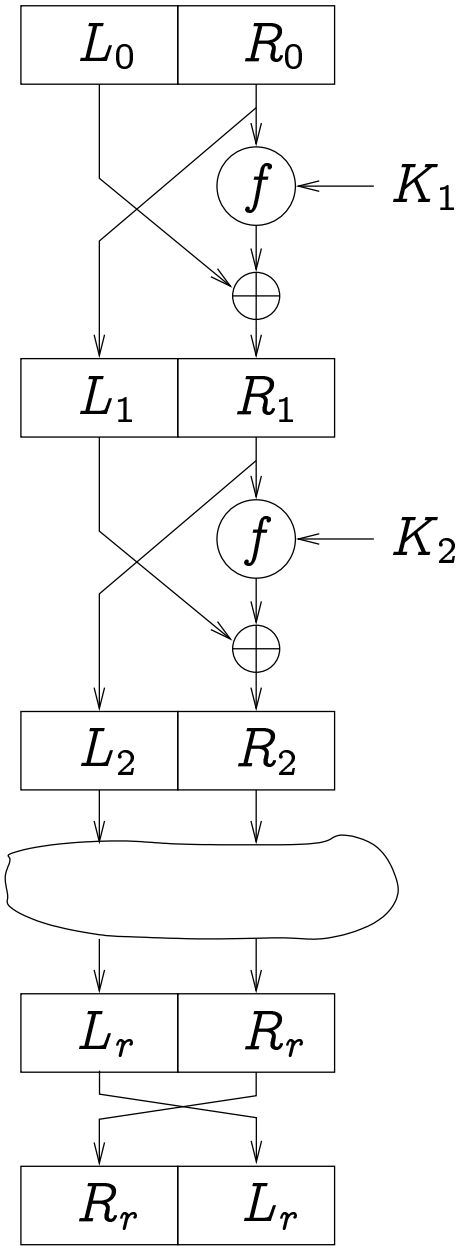
- Let $\mathbf{N}'$ be shift cipher with some skewed distribution of keys. What is $\mathbf{N} \times \mathbf{N}'$?
- Let G be group and g a uniformly chosen element of g. Show that
  - g^{-1} is uniformly distributed;
  - for a random $h \in G$ (with any distribution), $g \cdot h$ is uniformly distributed.
- 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^*?

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).

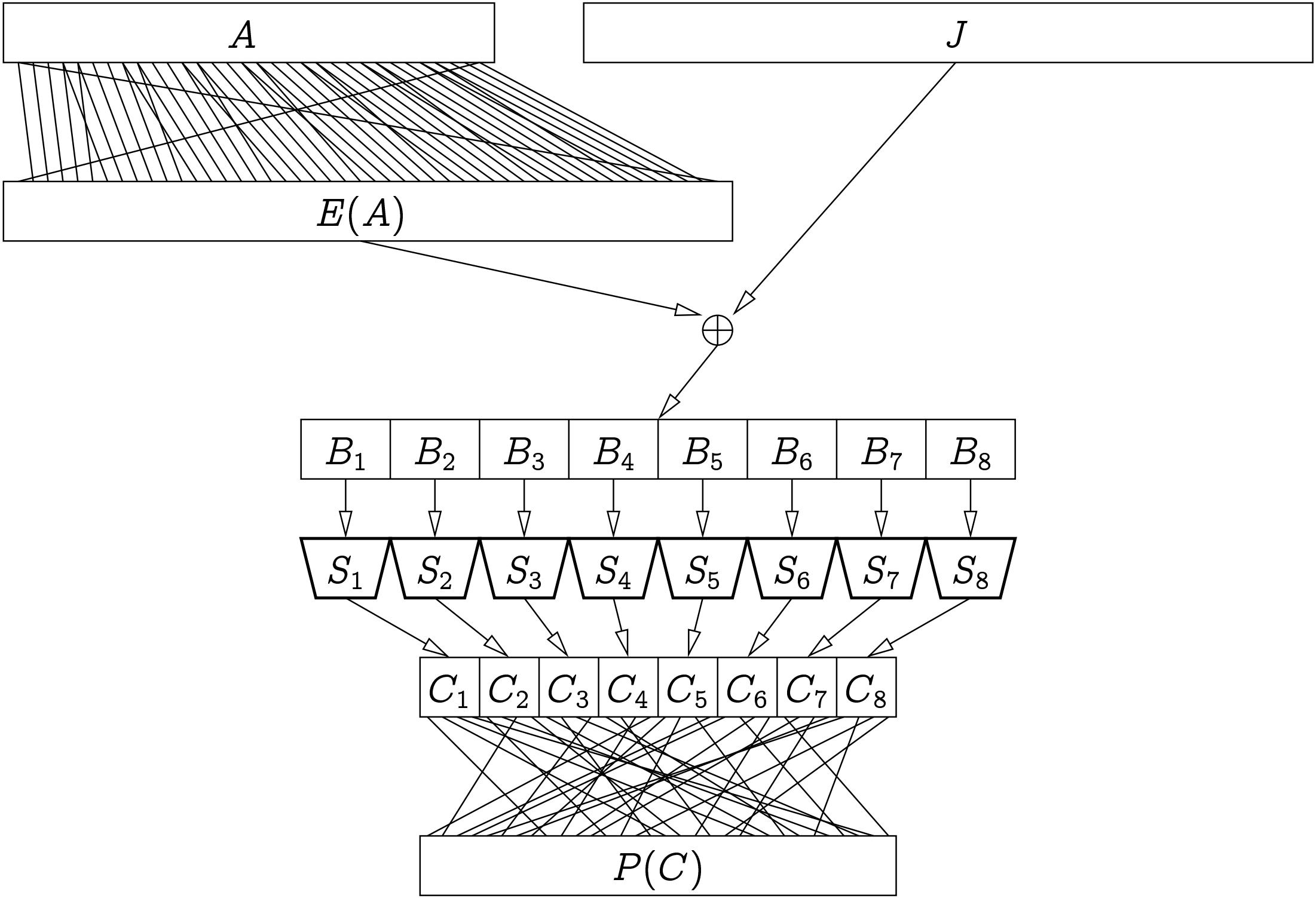
- $\mathcal{P} = \mathcal{C} = \{0,1\}^{64}$.
- $\mathcal{K} = \{0,1\}^{56}$.
- Encoding bit-string x with the key K:
  1. Let $x_0 = IP(x)$, where IP is a certain permutation of bits. Let L_0 [R_0] be the first [last] 32 bits of x.
  2. 16 rounds of Feistel construction:

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

     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 $S\text{-}box$)
4. return $P(C_1 \cdots C_8)$ where P is a certain permutation of bits.


A
J
E(A)
B1
B2
B3
B4
B5
B6
B7
B8
S1
S2
S3
S4
S5
S6
S7
S8
C1
C2
C3
C4
C5
C6
C7
C8
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

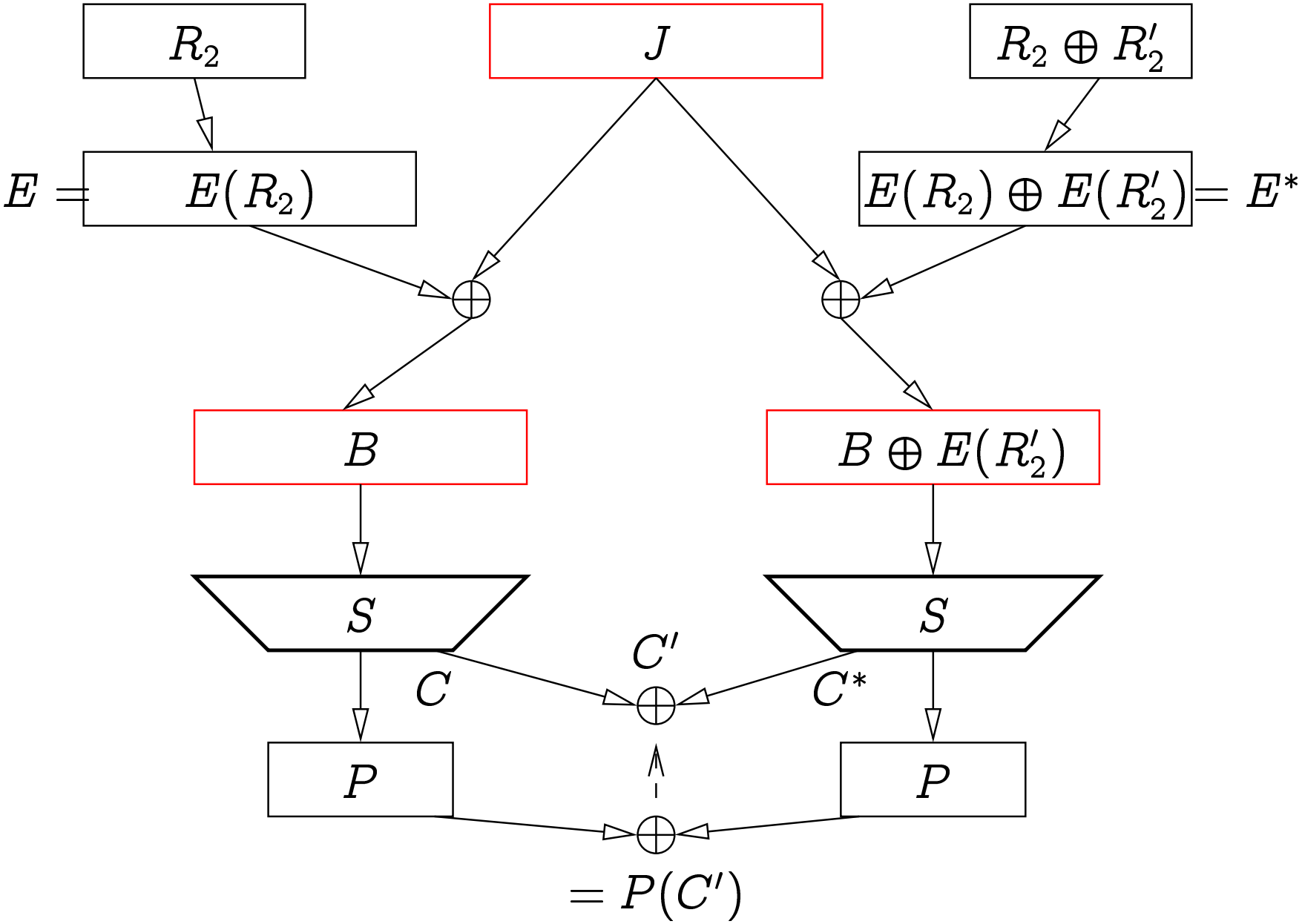
$$R_3' = L_0' \oplus f(R_2, K_3) \oplus f(R_2^*, K_3) \ .$$

We know L'_0 and R'_3. Hence we can compute

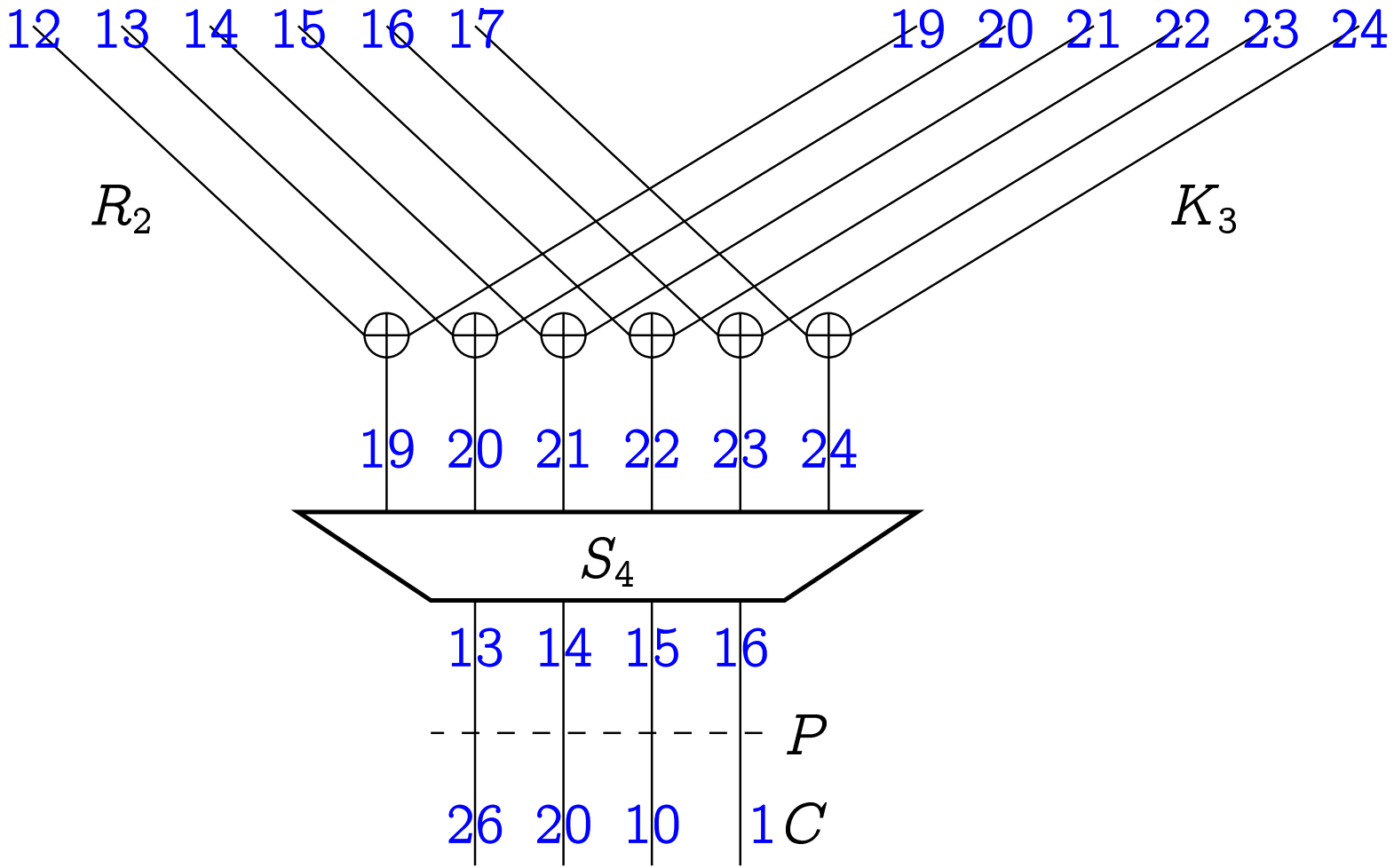
$$f(R_2, K_3) \oplus f(R^*_2, K_3) = R'_3 \oplus L'_0 \ .$$

$f(R_2, K_3) = P(C)$ 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 $S_4(R_2^4 \oplus K_3^4) \oplus S_4(R_2^{*4} \oplus K_3^4) = C'^4$.

$test_i(E^i, E^{*i}, C'^i) := \{K^i \in \{0,1\}^6 \mid S_4(E^i \oplus K^i) \oplus S_4(E^{*i} \oplus K^i) = C'^i\}$

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 $L_0 R_0$ 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 $L_0 R_0$ 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

$$L'_0 R'_0 \xrightarrow{p_1} L'_1 R'_1$$

where

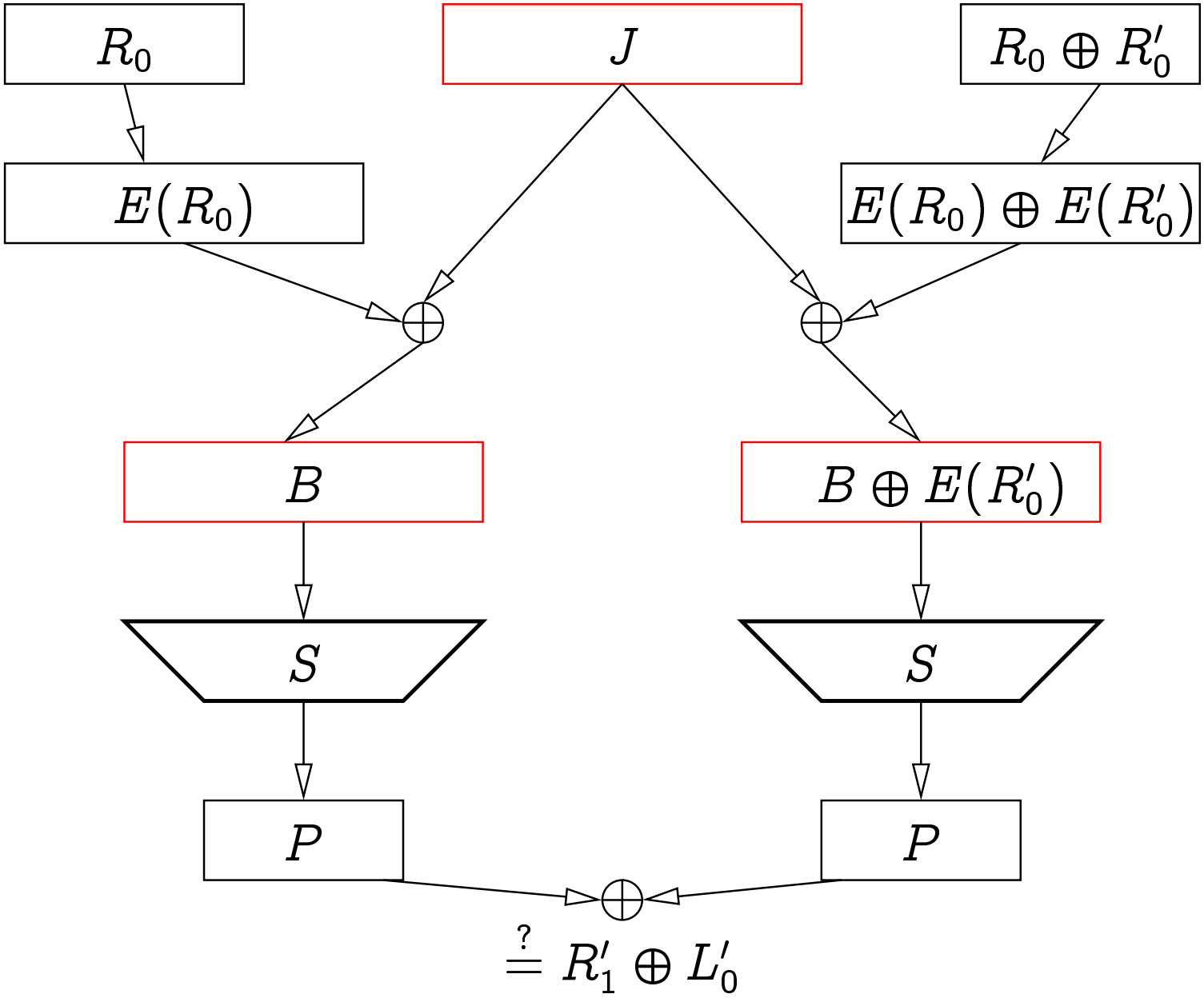
- $L'_1 = R'_0$;
- For any choice of L_0, R_0, the quantity p_1 is the probability that (taken over uniformly chosen $J \in \{0,1\}^{48}$)

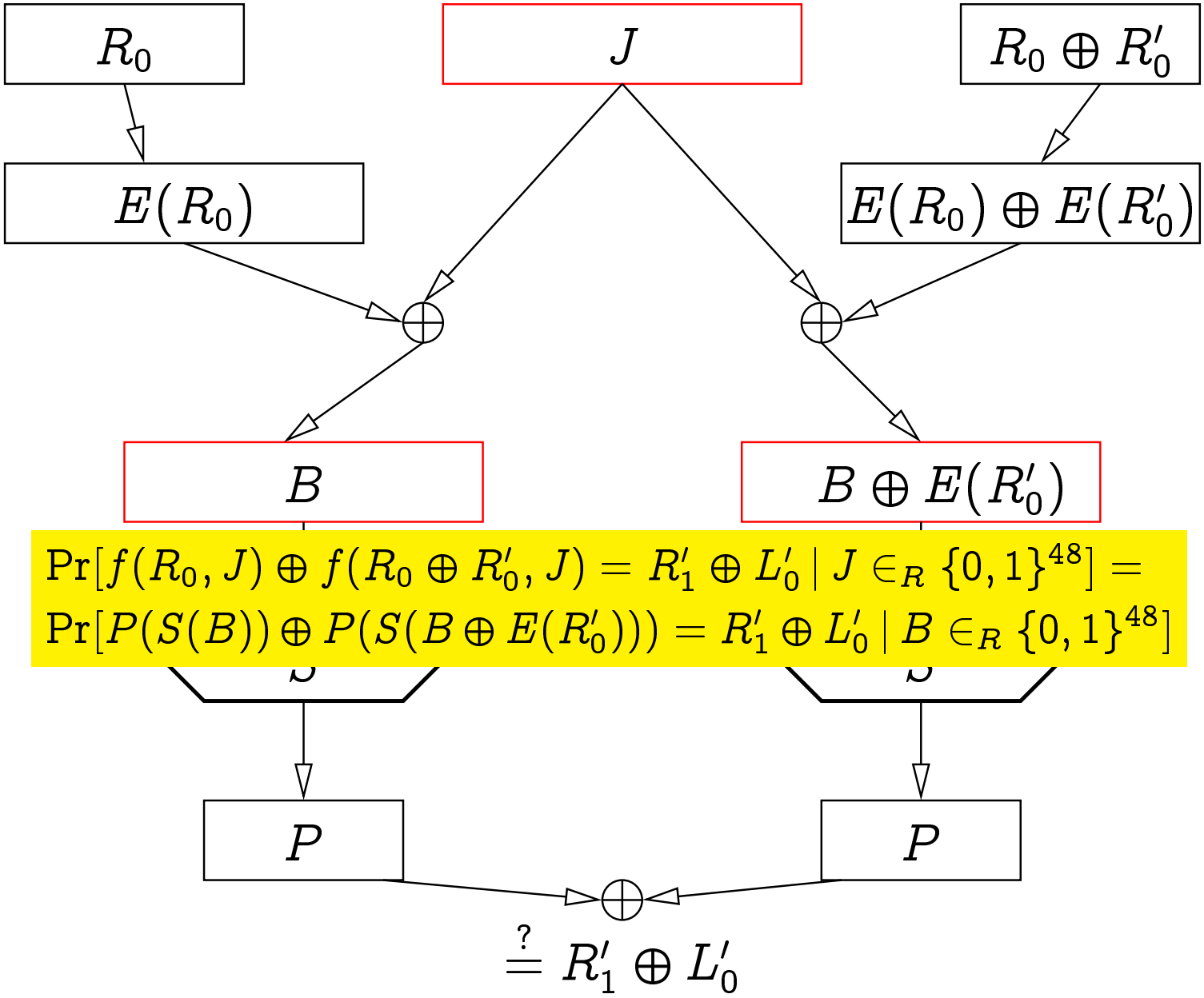
  $$\big(L_0 \oplus f(R_0, J)\big) \oplus \big((L_0 \oplus L'_0) \oplus f(R_0 \oplus R'_0, J)\big) = R'_1$$

  or that

  $$f(R_0, J) \oplus f(R_0 \oplus R'_0, J) = R'_1 \oplus L'_0 \ .$$

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
$\stackrel{?}{=} R'_1 \oplus L'_0$


R_0
J
$R_0 \oplus R'_0$
$E(R_0)$
$E(R_0) \oplus E(R'_0)$
B
$B \oplus E(R'_0)$
$\Pr[f(R_0, J) \oplus f(R_0 \oplus R'_0, J) = R'_1 \oplus L'_0 \mid J \in_R \{0,1\}^{48}] =$
$\Pr[P(S(B)) \oplus P(S(B \oplus E(R'_0))) = R'_1 \oplus L'_0 \mid B \in_R \{0,1\}^{48}]$
P
P
$\stackrel{?}{=} R'_1 \oplus L'_0$

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:

$$\begin{array}{lcl} xxxxxxxx_{16}|00000000_{16} & \stackrel{1}{\longrightarrow} & 00000000_{16}|xxxxxxxx_{16} \\ 00000000_{16}|60000000_{16} & \stackrel{14/64}{\longrightarrow} & 60000000_{16}|00808200_{16} \end{array}$$

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

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

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:

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

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

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 $R'_5 = L'_6$.

$E(R'_3) = 001000|000000|000001|010000|0 \cdots 0$. 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

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

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

We have found 30 bits of the key. The characteristic

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

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.

Some bits of number theory

(not contained in the book for the "Elements of Discrete Mathematics" course)

Euclidean algorithm for finding $\gcd(a, b)$, where $a, b \in \mathbb{N} \backslash \{0\}$:

Assume $a \geq b$. Let $a_0 = a$ and $a_1 = b$. For all $n \geq 1$ let $a_{n+1} = a_{n-1} \bmod a_n$, if $a_n \neq 0$. Then $\gcd(a, b)$ is equal to the last non-zero element in the sequence (a_n).

Lemma. Euclidean algorithm is correct.

Proof. Induction over the length of (a_n).

Base: $a_2 = 0$. Then $b \mid a$ and $\gcd(a, b) = b = a_1$.

Step: We show that $\gcd(a, b) = \gcd(b, a \bmod b)$.

I) Let $d \mid a$ and $d \mid b$. Then $a \bmod b = a - b \cdot \lfloor a/b \rfloor = d\big((a/d) - (b/d) \cdot \lfloor a/b \rfloor\big)$.

II) Let $d \mid b$ and $d \mid (a \bmod b)$. Then $a = b \cdot \lfloor a/b \rfloor + (a \bmod b) = d\big((b/d) \cdot \lfloor a/b \rfloor + (a \bmod b)/d\big)$.

Lemma. Let (a_n) be the sequence that is obtained while we use the Euclidean algorithm to find $\gcd(a, b)$. Then for each n there exist $u_n, v_n \in \mathbb{Z}$, such that $u_n a + v_n b = a_n$.

Proof. $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$.

In the sequence (a_n), the following holds:

$$a_{n+1} = a_{n-1} - a_n \cdot \lfloor a_{n-1}/a_n \rfloor \ .$$

Hence we'll define

$$\begin{aligned} u_{n+1} &= u_{n-1} - u_n \cdot \lfloor a_{n-1}/a_n \rfloor \\ v_{n+1} &= v_{n-1} - v_n \cdot \lfloor a_{n-1}/a_n \rfloor \ . \end{aligned}$$

If $\gcd(a, n) = 1$, then there exist $u, v \in \mathbb{Z}$ such that $ua + vn = 1$. In the ring $\mathbb{Z}_n$ we have $ua = 1$, i.e. $u = a^{-1} \pmod{n}$.

Set $\mathbb{Z}_n^*$

. . . is the set of all invertible elements of the structure $(\mathbb{Z}_n, \cdot)$:

$$\begin{aligned} \mathbb{Z}_n^* &= \{x \in \mathbb{Z}_n : \exists x' \in \mathbb{Z}_n, x \cdot x' = 1\} = \\ &= \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}. \end{aligned}$$

Theorem. The structure $(\mathbb{Z}_n^*, \cdot)$ is a group.

Which pairs (k, a) are a suitable key for the affine cipher

$$\mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto k \cdot x + a \mod n,$$

such that decoding were always possible? Obviously

$$(k, a) \in \mathbb{Z}_n^* \times \mathbb{Z}_n.$$

How large is the key space?

$$|\mathbb{Z}_n^* \times \mathbb{Z}_n| = |\mathbb{Z}_n^*| \cdot |\mathbb{Z}_n| = |\mathbb{Z}_n^*| \cdot n.$$

Euler's totient function φ

. . . is defined as

$$\varphi(n) := |\mathbb{Z}_n^*| = |\{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}|.$$

Theorem. If $p \in \mathbb{P}$ and $e \in \mathbb{N}$, then

$$\varphi(p^e) = p^e - p^{e-1}.$$

What is $\varphi(n)$ for any $n \in \mathbb{N}$? Any n can be uniquely represented as the product of powers of its prime factors:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}.$$

Theorem.

$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdot \ldots \cdot (p_r^{e_r} - p_r^{e_r-1}).$$

This follows from the next lemma

Lemma. If $\gcd(m, n) = 1$, then

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$: example

Consider juhtu $n = 72$.

$$\begin{aligned} \varphi(72) &= \varphi(8 \cdot 9) = \varphi(8) \cdot \varphi(9) = \\ &= \varphi(2^3) \cdot \varphi(3^2) = (2^3 - 2^2) \cdot (3^2 - 3^1) = \\ &= (8 - 4) \cdot (9 - 3) = 4 \cdot 6 = 24. \end{aligned}$$

	0	1	2	3	4	5	6	7	8
0	0	64	56	48	40	32	24	16	8
1	9	1	65	57	49	41	33	25	17
2	18	10	2	66	58	50	42	34	26
3	27	19	11	3	67	59	51	43	35
4	36	28	20	12	4	68	60	52	44
5	45	37	29	21	13	5	69	61	53
6	54	46	38	30	22	14	6	70	62
7	63	55	47	39	31	23	15	7	71

Proof sketch (I)

If $\gcd(m, n) = 1$, then the mapping

$$CRT : \mathbb{Z}_{m \cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n : x \mapsto (x \mod m, x \mod n)$$

is a bijection. This claim is equivalent to the *Chinese remainder theorem*.

Theorem. If $\gcd(m, n) = 1$, then the system of congruences

$$\begin{aligned} x &= a \mod m, \\ x &= b \mod n \end{aligned}$$

has exactly one solution *modulo* $m \cdot n$.

Chinese remainder theorem (general form)

Theorem. Let $m_1, m_2, \ldots, m_r$ be pairwise coprime natural numbers and $a_1, a_2, \ldots, a_r$ some integers. The system of congruences

$$\begin{aligned} x &= a_1 \bmod m_1 \\ x &= a_2 \bmod m_2 \\ &\ldots \\ x &= a_r \bmod m_r \end{aligned}$$

has exactly one solution *modulo* $m_1 \cdot m_2 \cdot \ldots \cdot m_r$.

Proof. We'll find x as follows. Define

- $M = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.
- $M_i = M/m_i$, $1 \leq i \leq r$.
- $M_i' = M_i^{-1} \pmod{m_i}$.
- $x = (M_1 M_1' a_1 + M_2 M_2' a_2 + \ldots + M_r M_r' a_r) \bmod M$.

Then $x \equiv M_i M_i' a_i \equiv a_i \pmod{m_i}$, because $M_j \equiv 0 \pmod{m_i}$, when $i \neq j$.

We showed that there exists at least one solution. Thus the mapping CRT is surjective. The injectivity follows from the equality of the cardinalities of the domain and codomain (and from their finiteness).

Proof sketch (II)

To prove the claim

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

or

$$|\mathbb{Z}^*_{m \cdot n}| = |\mathbb{Z}^*_m| \cdot |\mathbb{Z}^*_n| (= |\mathbb{Z}^*_m \times \mathbb{Z}^*_n|),$$

it is sufficient to prove that

$$x \in \mathbb{Z}^*_{m \cdot m} \Leftrightarrow CRT(x) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n.$$

This should not pose any difficulties.