Математические и компьютерные основы защиты информации

Лекция 4

Антон Николаевич Гайдук | УНИВЕР

vk.com/gaidukedu

02 марта 2023 г.

Содержание дисциплины

Раздел I Введение

- Тема 1. Введение. История. Основные понятия.

Раздел II Симметричная криптография

- Тема 2 Классические шифры.
- Тема 3 Поточные алгоритмы шифрования.
- Тема 4 Блочные алгоритмы шифрования.

- Тема 5 Функции хэширования.
- Тема 6 Математические методы криптоанализа.

Раздел III Асимметричная криптография

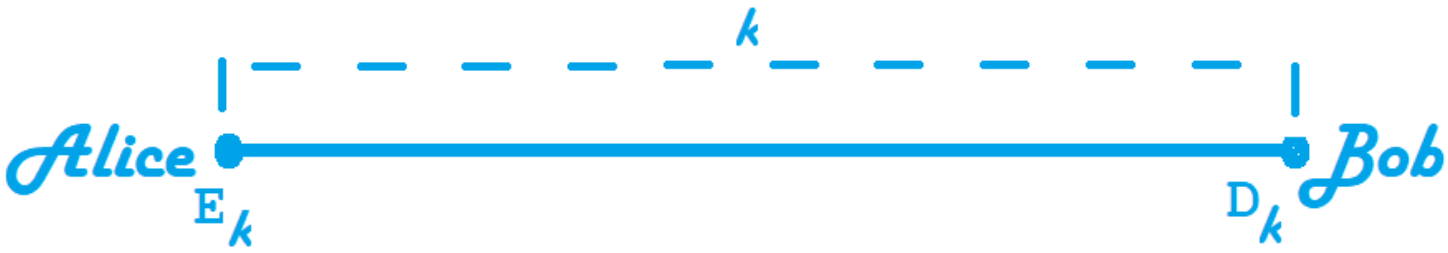
- Тема 7 Протокол Диффи-Хэллмана.
- Тема 8 Криптосистемы с открытым ключом.
- Тема 9 Электронная цифровая подпись.

Раздел II Симметричная криптография

Тема 4 Блочные алгоритмы шифрования.

- Понятие блочного алгоритма шифрования
- Примеры блочных алгоритмов шифрования
- Confusion and Diffusion
- Блочно-итерационные алгоритмы шифрования
- SP-подстановка
- SP-сеть
- Сеть Фейстеля
- Режимы шифрования

Симметричная криптография



Определение

Шифрсистемой называется пятерка $\{\mathcal{K}, \mathcal{P}, \mathcal{C}, E, D\}$, где
$\mathcal{K}$ — множество ключей (секретных параметров),
$\mathcal{P}$ — множество открытых текстов,
$\mathcal{C}$ — множество шифртекстов,
E — семейство преобразований зашифрования $E = \{E_k : \mathcal{P} \to \mathcal{C} | k \in \mathcal{K}\}$
D — семейство преобразований расшифрования $D = \{D_k : \mathcal{C} \to \mathcal{P} | k \in \mathcal{K}\}$
с ограничениями

- однозначность расшифрования: $D_k(E_k(p)) = p$ для $\forall p \in \mathcal{P}$;
- реализуемость всех шифртекстов: $\bigcup\limits_{k \in \mathcal{K}} \bigcup\limits_{p \in \mathcal{P}} E_k(p) = \mathcal{C}$, т.е.

  $\forall c \in \mathcal{C} \qquad \exists p \in \mathcal{P}, k \in \mathcal{K}$ такие, что $E_k(p) = c$.

Блочные алгоритмы шифрования

Шифрование осуществляется блоками длины n: $\mathcal{P} = \mathcal{C} = \mathbb{B}^n, \qquad \mathbb{B} = \{0, 1\}.$

$$p \to E_k(p) = c, \qquad p \in \mathbb{B}^n, c \in \mathbb{B}^n.$$

$E_k, D_k \in S(\mathbb{B}^n)$ — биекции, $E = \{E_k | k \in \mathcal{K}\} \subseteq S(\mathbb{B}^n)$.
$|\mathcal{K}| \ll |S(\mathbb{B}^n)|$ — шифрсистема состоит из малого подмножества допустимых подстановок.

Год	Алгоритм	Длина блока (бит)	Длина ключа (бит)
1971	Lucifer	48/32/128	48/64/128
1975	DES	64	56
1989 (1978)	ГОСТ 28147-89	64	256
1991	IDEA	64	128
1993	Blowfish	64	32—448
1998	AES	128	128/192/256
2007	BelT	128	256

Шэннон: Confusion and Diffusion

Confusion: преобразование усложнения (запутывание)

Задача: усложнить (скрыть) зависимость между ключом и шифртекстом.
S-box.

Diffusion: преобразование перемешивания (рассеивание)

Задача: усложнить (скрыть) зависимость между открытым текстом и шифртекстом.
P-box.

Шеннон предложил строить шифрсистемы как многократные композиции преобразований усложнения и перемешивания.

Лавинный эффект

Распространение «влияния» одного бита открытого текста (или ключа) на все остальные биты шифруемого блока за определенное количество раундов.

S-box и P-box

Пусть $\mathcal{A} = \{A, B, C, D\}$

Шифр подстановки

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

AAAA $\to$ CCCC

CCCD $\to$ AAAB

$\downarrow$

S-box

Шифр перестановки

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

AAAA $\to$ AAAA

CCCD $\to$ CDCC

$\downarrow$

P-box

S-box и P-box

$$\mathbb{B} = \{0, 1\}$$

S-блоком называется отображение $S(x) : \mathbb{B}^n \to \mathbb{B}^m$ сопоставляющее двоичному n-мерному вектору $x = (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$ двоичный m-мерный вектор $y = (y_1, y_2, \ldots, y_m) \in \mathbb{B}^m$ определяемый m координатными булевыми функциями от n переменных $y_i(x), i = 1, \ldots, m$ так, что

$$S(x) = (y_1(x), \ldots, y_m(x)).$$

P-блоком называется отображение $P(x) : \mathbb{B}^n \to \mathbb{B}^m$ сопоставляющее двоичному n-мерному вектору $x = (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$ двоичный m-мерный вектор $y = (y_1, y_2, \ldots, y_m) \in \mathbb{B}^m$ определяемый m координатными булевыми функциями от n переменных $y_i(x) = x_{\pi(i)}, i = 1, \ldots, m$ и отображением $\pi : \{1, \ldots, m\} \to \{1, \ldots, n\}$ так, что

$$P(x) = (x_{\pi(1)}, \ldots, x_{\pi(m)}).$$

S-box и P-box

$$\mathbb{B} = \{0, 1\}$$

S-box

$$S(x) : \mathbb{B}^n \to \mathbb{B}^m$$
$$x = (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$$
$$\downarrow$$
$$y = (y_1, y_2, \ldots, y_m) \in \mathbb{B}^m$$
$y_i(x)$ — произвольные

$$S(x) = (y_1(x), \ldots, y_m(x)).$$

P-box

$$P(x) : \mathbb{B}^n \to \mathbb{B}^m$$
$$x = (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$$
$$\downarrow$$
$$y = (y_1, y_2, \ldots, y_m) \in \mathbb{B}^m$$
$$y_i(x) = x_{\pi(i)},$$
$$\pi : \{1, \ldots, m\} \to \{1, \ldots, n\}$$

$$P(x) = (x_{\pi(1)}, \ldots, x_{\pi(m)}).$$

S-box и P-box

S-box

- Назначение заключается в нелинейном преобразовании, что препятствует проведению линейного (разностного) криптоанализа (усложнение).
- Одним из свойств хорошего S-блока является локальный лавинный эффект, то есть изменение одного бита на входе приводит к изменению половины бит на выходе.

P-box

- Назначение заключается в распределении выхода каждого S-блока между входами как можно большего числа других S-блоков (лавинный эффект).

Блочно-итерационные алгоритмы шифрования

Блочный алгоритм шифрования называется итерационным блочным алгоритмом шифрования, если преобразование зашифрования является композицией r раундовых функций зашифрования $\hat{E}_{k_i}^{(i)}(p)$, действие которых определяется раундовыми ключами k_i, $1 \leqslant i \leqslant r$.

Определяются следующими элементами

1. Количеством раундов (тактов, итераций): r.
2. Множеством раундовых ключей: $\hat{\mathcal{K}}$.
3. Отображением $\chi : \mathcal{K} \to \hat{\mathcal{K}}^r$, которое ставит в соответствие ключу $k \in \mathcal{K}$ набор тактовых ключей $(k_1, \ldots, k_r)$. Отображение называется **расписанием ключей**.
4. Семействами раундовых функций зашифрования $\{\hat{E}_{k'}^{(i)} | k' \in \hat{\mathcal{K}}\} \subseteq S(\mathbb{B}^n), i = \overline{1, r}$.

Зашифрование

$$E_k(p) = \hat{E}_{k_r}^{(r)} \circ \cdots \circ \hat{E}_{k_1}^{(1)}(p).$$

Расшифрование

$$D_k(c) = \hat{E}_{k_1}^{(1)^{-1}} \circ \cdots \circ \hat{E}_{k_r}^{(r)^{-1}}(c).$$

Блочно-итерационные алгоритмы шифрования

Раундовые функции зашифрования $\hat{E}_{k_i}^{(i)}(p)$ имеют, как правило, простое строение и состоят в замене и перестановке символов подлежащего преобразованию слова. Однако многократная композиция таких преобразований определяет сложную зависимость между открытым текстом, шифртекстом и ключом.

Зашифрование

Вход: p, k.
Выход: c.
Шаги:

1. $(k_1, \ldots, k_r) \leftarrow \chi(k)$.
2. $c^{(0)} = p$.
3. Для $i = 1, \ldots, r$:

$$c^{(i)} = \hat{E}_{k_i}^{(i)}(c^{(i-1)}).$$

4. Вернуть $c = c^{(r)}$.

Расшифрование

Вход: c, k.
Выход: p.
Шаги:

1. $(k_1, \ldots, k_r) \leftarrow \chi(k)$.
2. $c^{(r)} = c$.
3. Для $i = r, \ldots, 1$:

$$c^{(i-1)} = \hat{E}_{k_i}^{(i)^{-1}}(c^{(i)}).$$

4. Вернуть $p = c^{(0)}$.

Блочно-итерационные алгоритмы шифрования

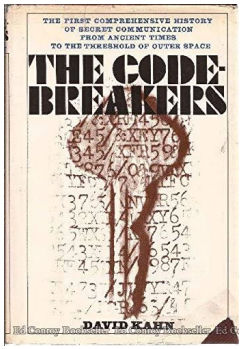
Модификации:

1. **Дополнительные преобразования (DES)**. Используются дополнительные бесключевые подстановки $\tau_1, \tau_2 \in S(\mathbb{B}^n)$, которые применяются перед первым раундом и после последнего:

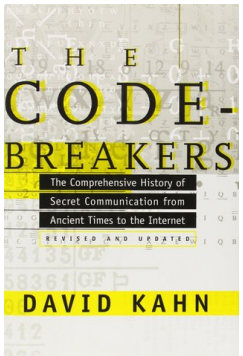
$$E_k(p) = \tau_1 \hat{E}_{k_r}^{(r)} \circ \cdots \circ \hat{E}_{k_1}^{(1)}(p)\tau_2.$$

2. **Отбеливание (Blowfish)**. По k строится дополнительный ключ $k_{r+1} \in \mathbb{B}^n$, который добавляется к результату r-раундового зашифрования: $c^{(r+1)} = c^{(r)} \oplus k_{r+1}$.
3. **Однородные раунды**. $\hat{E}_{k_i}^{(i)} = E_{k_i}, i = \overline{1, r}$.

THE CODE-BREAKERS



Книга Дэвида Кана, фундаментальный труд по истории криптографии. Книга вышла в 1967 году, не содержала новых открытий в области криптографии, но подробно описывала имеющиеся на тот момент результаты в области криптографии, включала большой исторический материал.



Книга имела заметный коммерческий успех и познакомила с криптографией десятки тысяч людей. С этого момента в открытой печати постепенно стали появляться другие работы по криптографии.

Книга была переиздана в 1996 году. В новое издание была добавлена глава, описывающая события, прошедшие с момента первой публикации.

Lucifer

United States Patent [19] [11] **3,798,359**
Feistel [45] **Mar. 19, 1974**

[54] **BLOCK CIPHER CRYPTOGRAPHIC SYSTEM**

[75] Inventor: **Horst Feistel,** Mount Kisco, N.Y.

[73] Assignee: **International Business Machines Corporation,** Armonk, N.Y.

[22] Filed: **June 30, 1971**

[21] Appl. No.: **158,360**

[52] **U.S. Cl.** **178/22,** 340/172.5, 340/348
[51] **Int. Cl.** **H04l 9/00**
[58] **Field of Search** 178/22; 340/172.5, 348

[56] **References Cited**

UNITED STATES PATENTS

3,657,699	4/1972	Rocher	178/22
2,984,700	5/1961	Small	178/22
3,170,033	2/1965	Vasseur	178/22
2,995,624	8/1961	Watters	178/22
2,917,579	12/1959	Hagelin	178/22

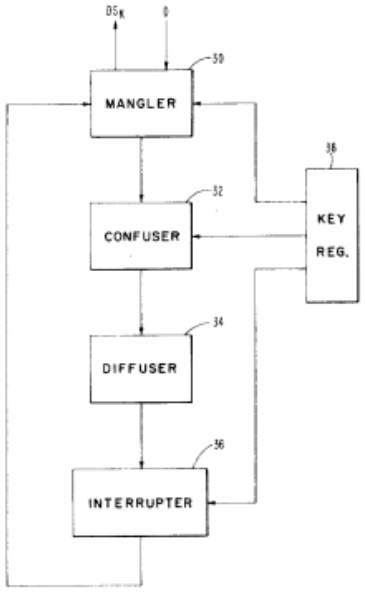
Primary Examiner—Benjamin A. Borchelt
Assistant Examiner—H. A. Birmiel
Attorney, Agent, or Firm—Victor Siber

[57] **ABSTRACT**

A cryptographic system for encrypting a block of binary data under the control of a key consisting of a set of binary symbols. The cryptographic system is utilized within a data processing environment to ensure complete privacy of data and information that is stored or processed within a computing system. All authorized subscribers who are permitted access to data within the network are assigned a unique key consisting of a combination of binary symbols. The central processing unit within the computing network contains a complete listing of all distributed authorized subscriber keys. All communications transmitted from terminal input are encrypted into a block cipher by use of the cryptographic system operating under the control of the subscriber key which is inputed to the terminal device. At the receiving station or central processing unit, an identical subscriber key which is obtained from internal tables stored within the computing system is used to decipher all received ciphered communications.

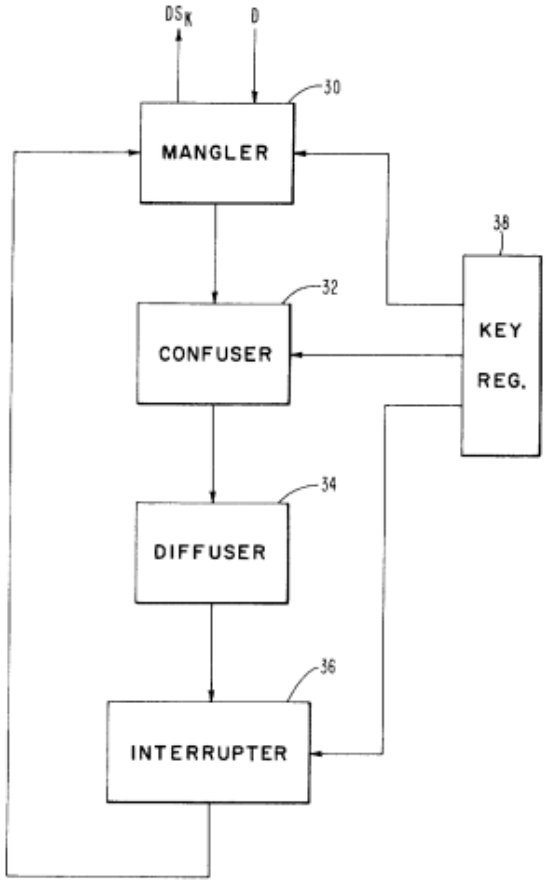
The cryptographic system develops a product cipher which is a combination of linear and nonlinear transformations of the clear message, the transformation being a function of the binary values that appear in the subscriber key. In addition to the transformation, the key controls various register substitutions and modulo-2 additions of partially ciphered data within the cryptographic system.

13 Claims, 31 Drawing Figures



Lucifer

FIG. 3

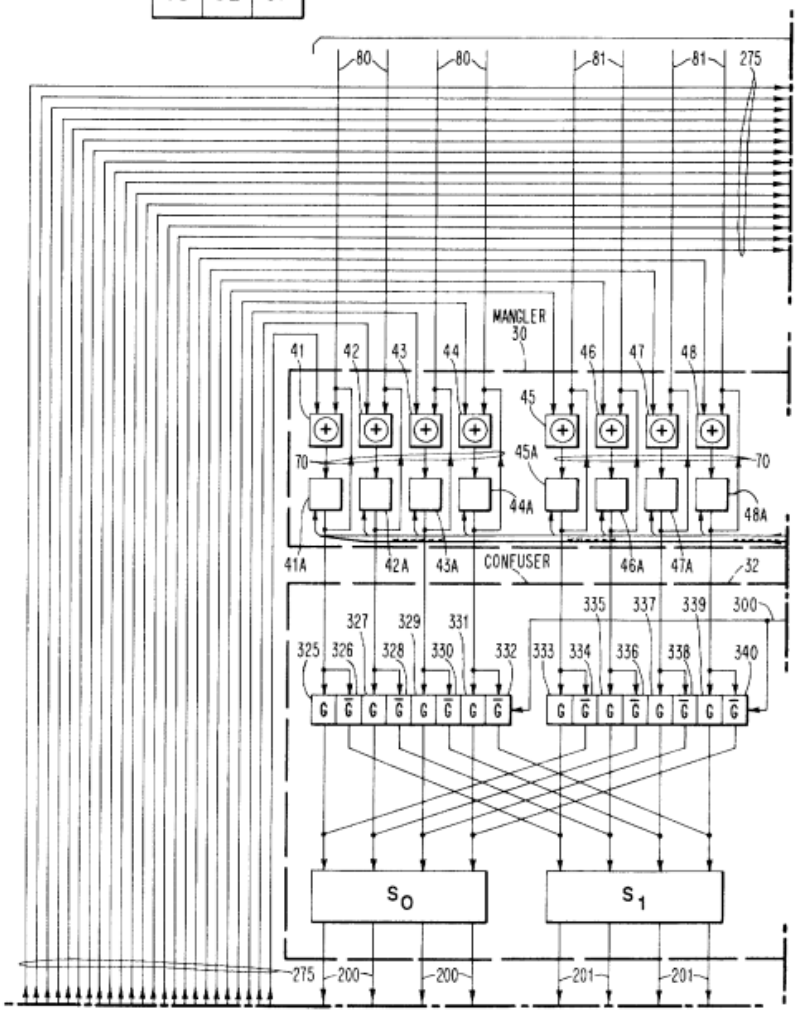


Lucifer

FIG. 6

FIG. 6A	FIG. 6B	FIG. 6C
FIG. 6D	FIG. 6E	FIG. 6F

FIG. 6A



Lucifer

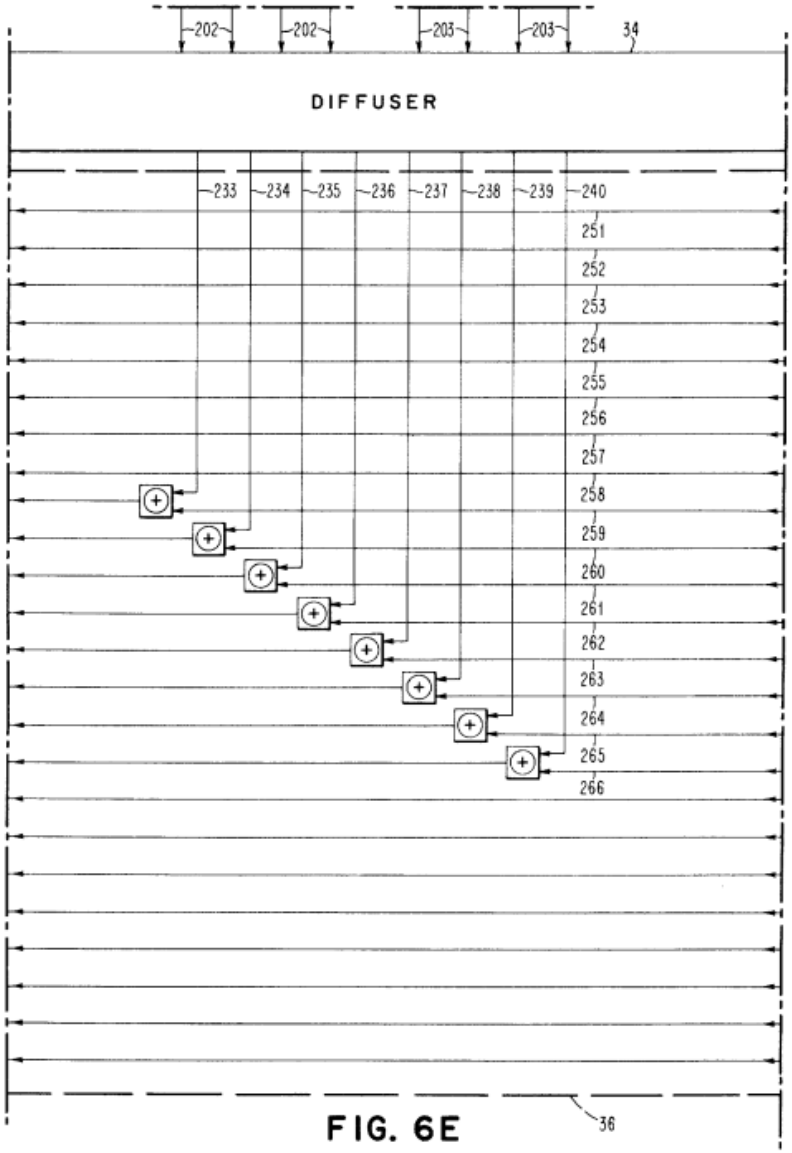
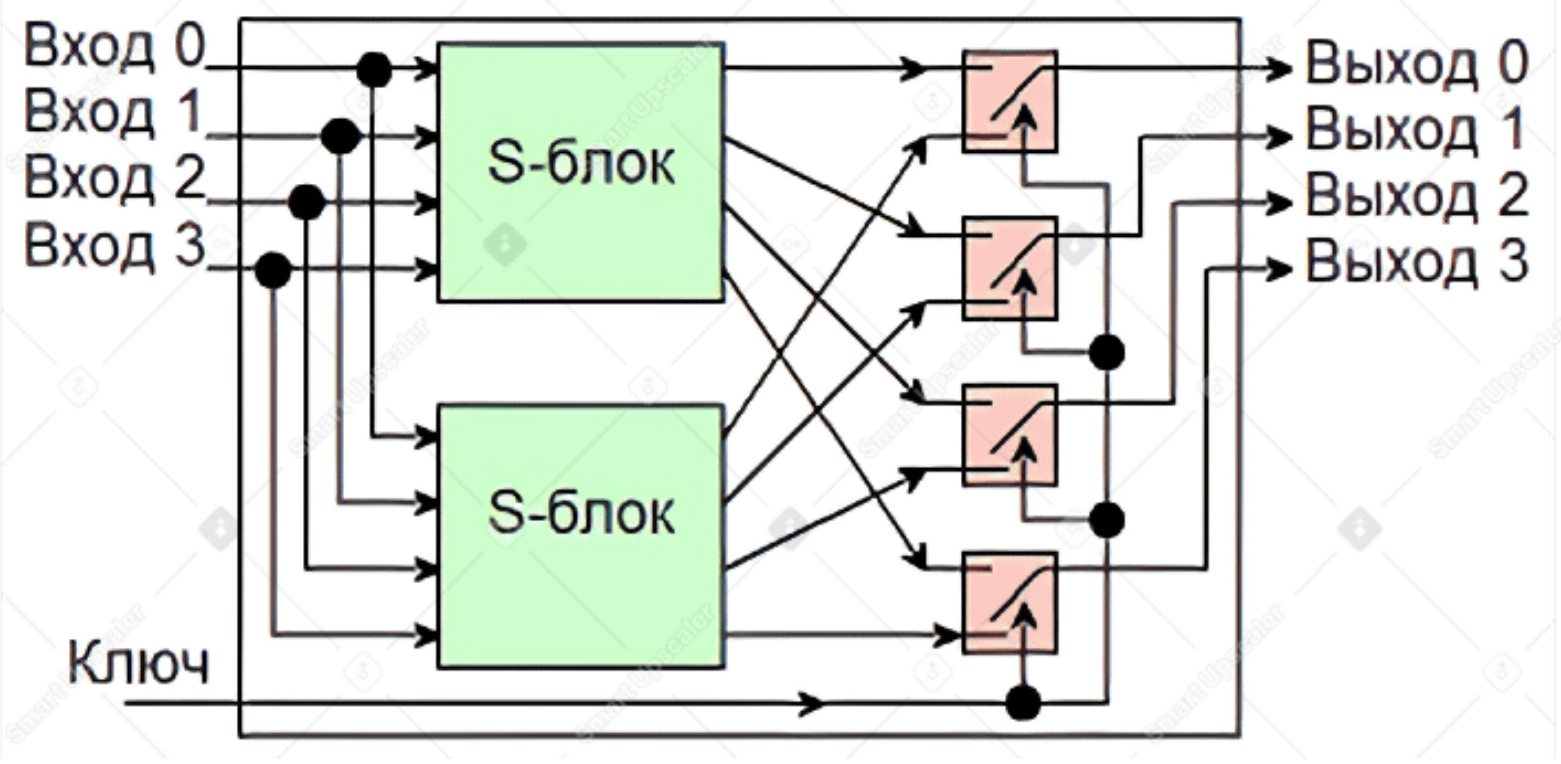
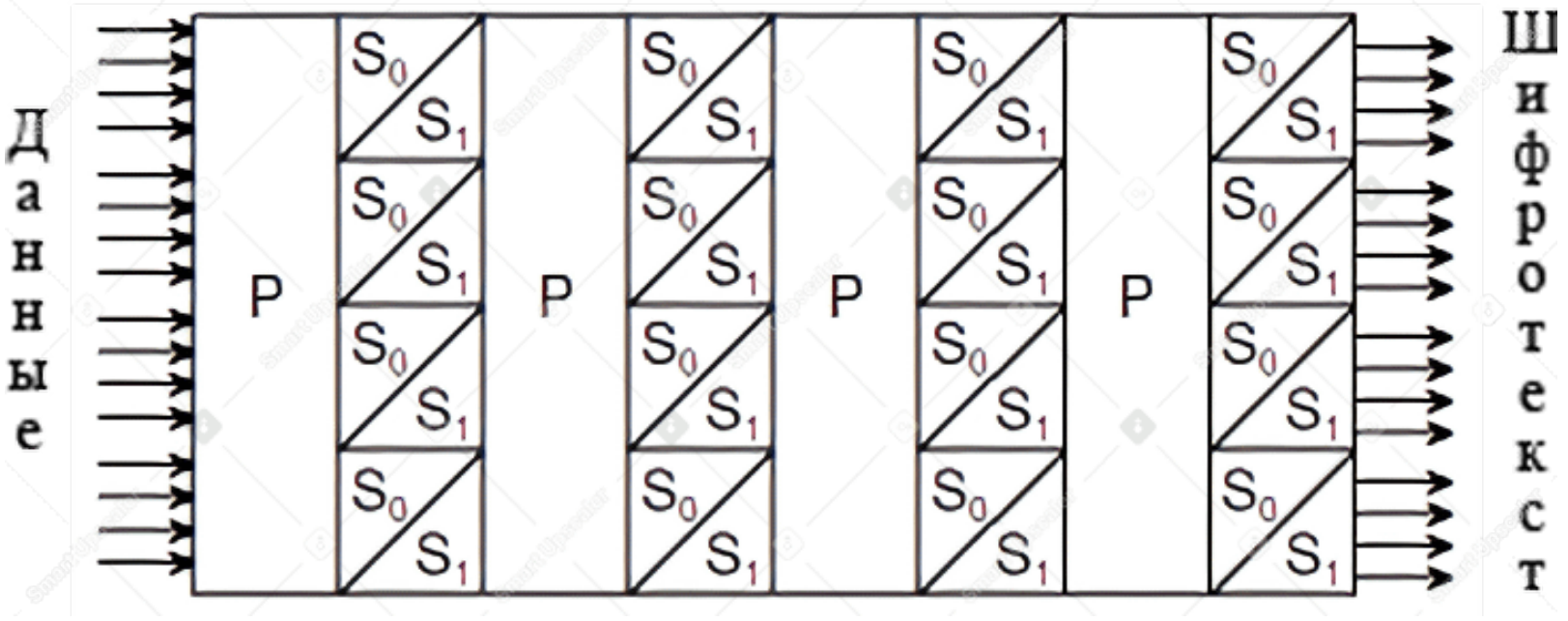


FIG. 6E

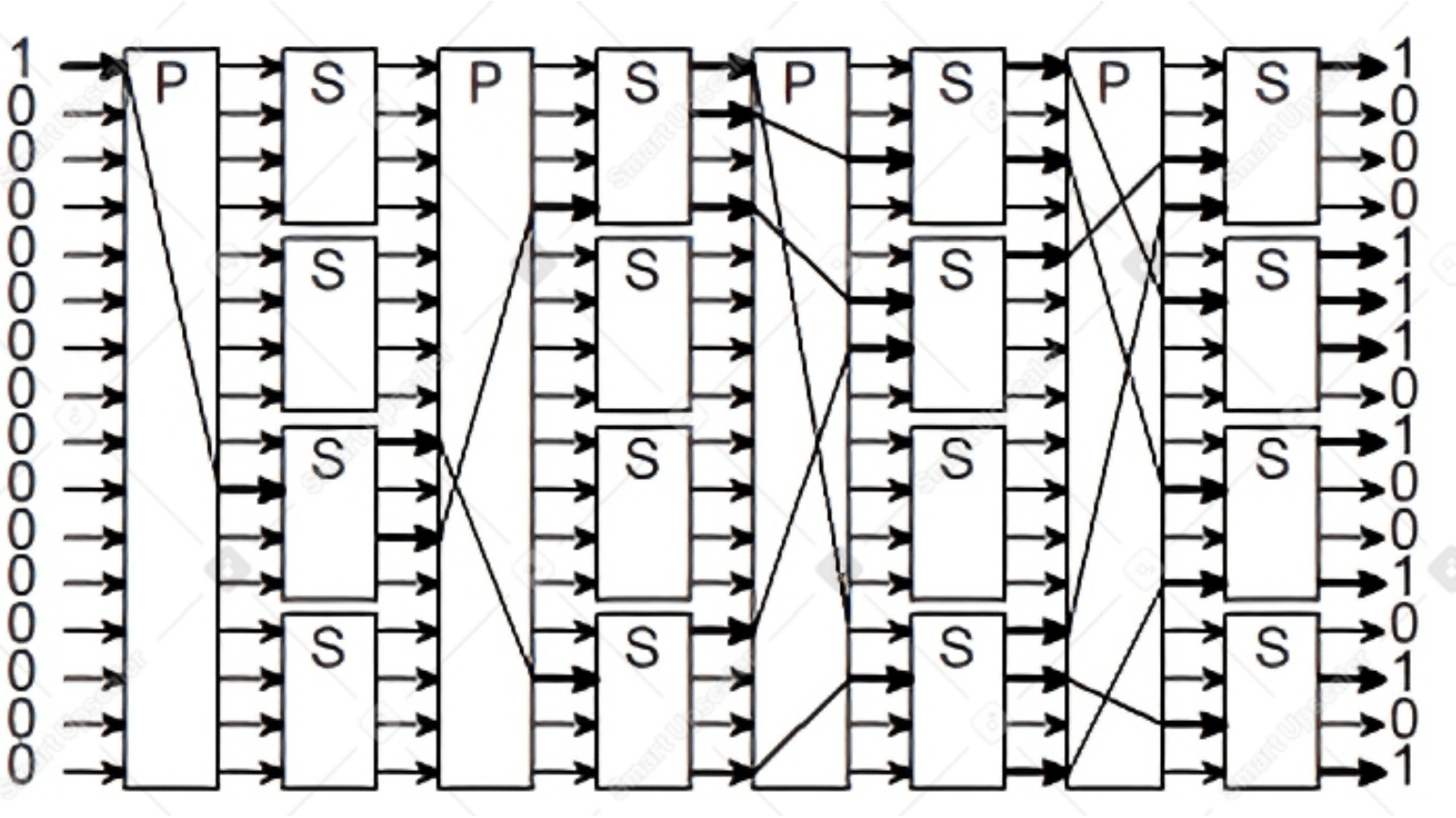
Lucifer


Вход 0
Вход 1
Вход 2
Вход 3
S-блок
S-блок
Ключ
Выход 0
Выход 1
Выход 2
Выход 3

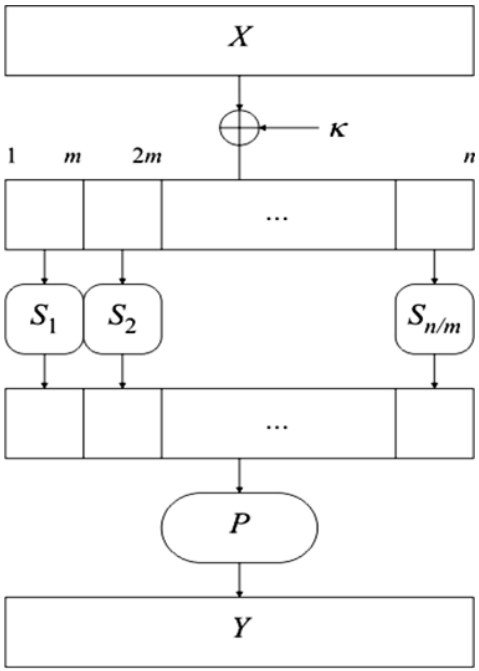
Lucifer



Lucifer

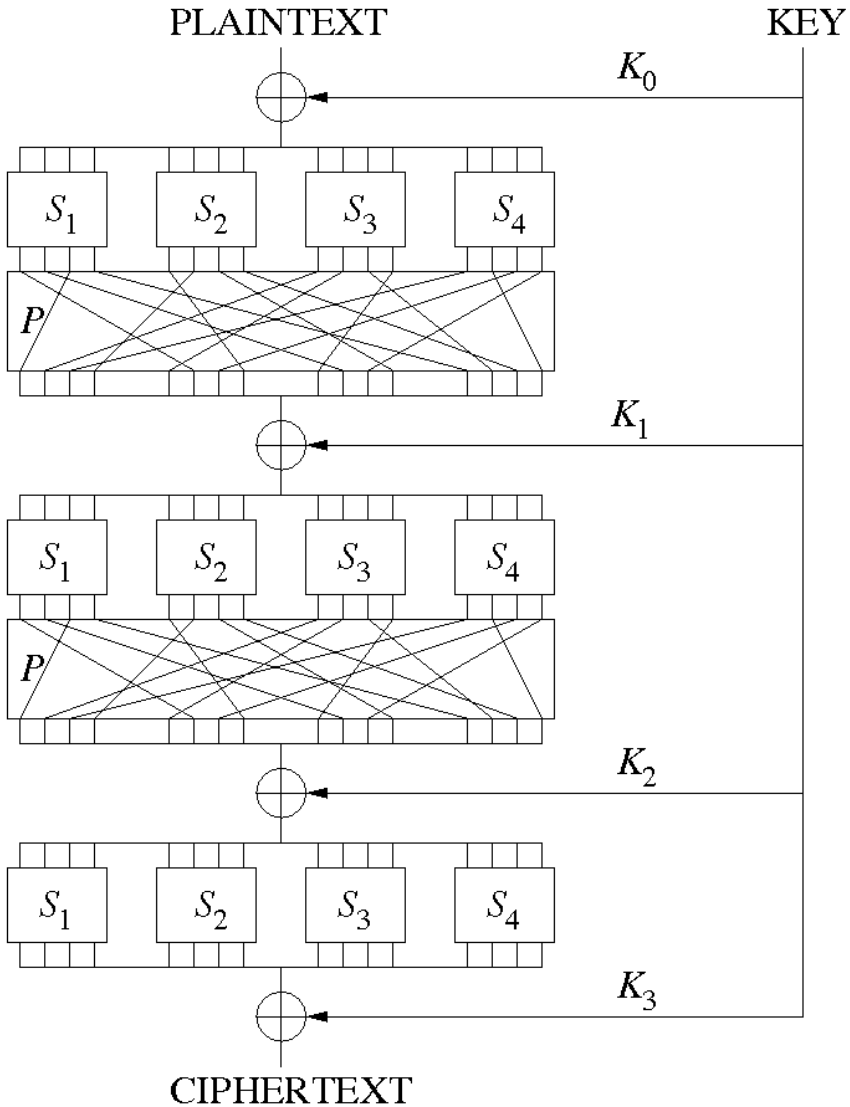

1
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
P
S
S
S
S
P
S
S
S
S
P
S
S
S
S
P
S
S
S
S
1
0
0
0
1
1
1
0
1
0
0
1
0
1
0
1

SP-подстановка



1. Входные данные $x \in \mathbb{B}^n, n = lm$ суммируются с ключом $\hat{k} \in \hat{\mathcal{K}} = \mathbb{B}^n$ ($\oplus$ или другая групповая операция).
2. Последовательные m-фрагменты результата суммирования подвергаются преобразованиям $S_1, \ldots, S_m \in S(\mathbb{B}^m)$.
3. Выполняется преобразование перестановки P объединенных фрагментов.

SP-сеть


PLAINTEXT
KEY
K_0
S_1
S_2
S_3
S_4
P
K_1
S_1
S_2
S_3
S_4
P
K_2
S_1
S_2
S_3
S_4
K_3
CIPHERTEXT

Инволютивные подстановки

Подстановка τ называется инволютивной, если τ^2 — тождественная подстановка.

Пусть τ и σ — подстановки, которые действуют на одном и том же множестве. Подстановку σ назовем τ-инволютивной, если $\sigma\tau\sigma = \tau$.

Теорема о использовании τ-инволютивности для расшифрования

Пусть преобразование зашифрования блочно-итерационной алгоритма шифрования имеют вид

$$E_k(p) = \tau\hat{E}_{k_r} \circ \cdots \circ \hat{E}_{k_1}(p),$$

где $\tau \in S(\mathbb{B}^n)$—инволютивна, а раундовые функции зашифрования $\hat{E}_{\hat{k}} \in S(\mathbb{B}^n)$ — τ-инволютивны при любом $\hat{k} \in \hat{\mathcal{K}}$. Тогда

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \hat{E}_{k_r}(c).$$

Доказательство.

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \ \hat{E}_{k_r}\tau\hat{E}_{k_r} \ \circ \cdots \circ \hat{E}_{k_1}(p)$$

Инволютивные подстановки

Подстановка τ называется инволютивной, если τ^2 — тождественная подстановка.

Пусть τ и σ — подстановки, которые действуют на одном и том же множестве. Подстановку σ назовем τ-инволютивной, если $\sigma\tau\sigma = \tau$.

Теорема о использовании τ-инволютивности для расшифрования

Пусть преобразование зашифрования блочно-итерационной алгоритма шифрования имеют вид

$$E_k(p) = \tau\hat{E}_{k_r} \circ \cdots \circ \hat{E}_{k_1}(p),$$

где $\tau \in S(\mathbb{B}^n)$—инволютивна, а раундовые функции зашифрования $\hat{E}_{\hat{k}} \in S(\mathbb{B}^n)$ — τ-инволютивны при любом $\hat{k} \in \hat{\mathcal{K}}$. Тогда

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \hat{E}_{k_r}(c).$$

Доказательство.

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \underbrace{(\hat{E}_{k_r}\tau\hat{E}_{k_r})}_{\tau} \circ \cdots \circ \hat{E}_{k_1}(p)$$

Инволютивные подстановки

Подстановка τ называется инволютивной, если τ^2 — тождественная подстановка.

Пусть τ и σ — подстановки, которые действуют на одном и том же множестве. Подстановку σ назовем τ-инволютивной, если $\sigma\tau\sigma = \tau$.

Теорема о использовании τ-инволютивности для расшифрования

Пусть преобразование зашифрования блочно-итерационной алгоритма шифрования имеют вид

$$E_k(p) = \tau\hat{E}_{k_r} \circ \cdots \circ \hat{E}_{k_1}(p),$$

где $\tau \in S(\mathbb{B}^n)$—инволютивна, а раундовые функции зашифрования $\hat{E}_{\hat{k}} \in S(\mathbb{B}^n)$ — τ-инволютивны при любом $\hat{k} \in \hat{\mathcal{K}}$. Тогда

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \hat{E}_{k_r}(c).$$

Доказательство.

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \underbrace{(\hat{E}_{k_{r-1}}\tau\hat{E}_{k_{r-1}})}_{\tau} \circ \cdots \circ \hat{E}_{k_1}(p)$$

Инволютивные подстановки

Подстановка τ называется инволютивной, если τ^2 — тождественная подстановка.

Пусть τ и σ — подстановки, которые действуют на одном и том же множестве. Подстановку σ назовем τ-инволютивной, если $\sigma\tau\sigma = \tau$.

Теорема о использовании τ-инволютивности для расшифрования

Пусть преобразование зашифрования блочно-итерационной алгоритма шифрования имеют вид

$$E_k(p) = \tau\hat{E}_{k_r} \circ \cdots \circ \hat{E}_{k_1}(p),$$

где $\tau \in S(\mathbb{B}^n)$—инволютивна, а раундовые функции зашифрования $\hat{E}_{\hat{k}} \in S(\mathbb{B}^n)$ — τ-инволютивны при любом $\hat{k} \in \hat{\mathcal{K}}$. Тогда

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \hat{E}_{k_r}(c).$$

Доказательство.

$$D_k(c) = \tau\tau(p) = p.$$

Инволютивные подстановки

Подстановка τ называется инволютивной, если τ^2 — тождественная подстановка.

Пусть τ и σ — подстановки, которые действуют на одном и том же множестве. Подстановку σ назовем τ-инволютивной, если $\sigma\tau\sigma = \tau$.

Теорема о использовании τ-инволютивности для расшифрования

Пусть преобразование зашифрования блочно-итерационной алгоритма шифрования имеют вид

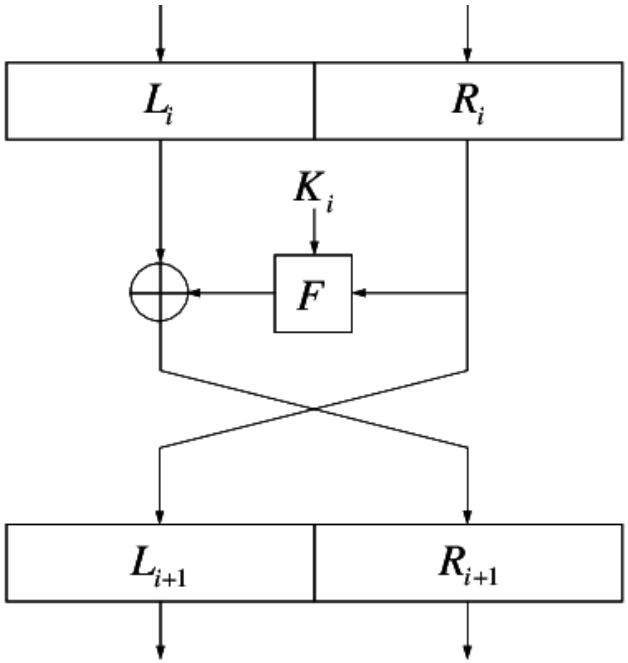
$$E_k(p) = \tau\hat{E}_{k_r} \circ \cdots \circ \hat{E}_{k_1}(p),$$

где $\tau \in S(\mathbb{B}^n)$—инволютивна, а раундовые функции зашифрования $\hat{E}_{\hat{k}} \in S(\mathbb{B}^n)$ — τ-инволютивны при любом $\hat{k} \in \hat{\mathcal{K}}$. Тогда

$$D_k(c) = \tau\hat{E}_{k_1} \circ \cdots \circ \hat{E}_{k_r}(c).$$

Теорема означает, что с использованием τ-инволютивных подстановок можно строить блочно-итерационные алгоритмы, в которых направление «зашифрование — расшифрование» изменяется только порядком следования раундовых ключей.

Сеть Фейстеля



Блок открытого текста делится на две равные части: (L_0, R_0).

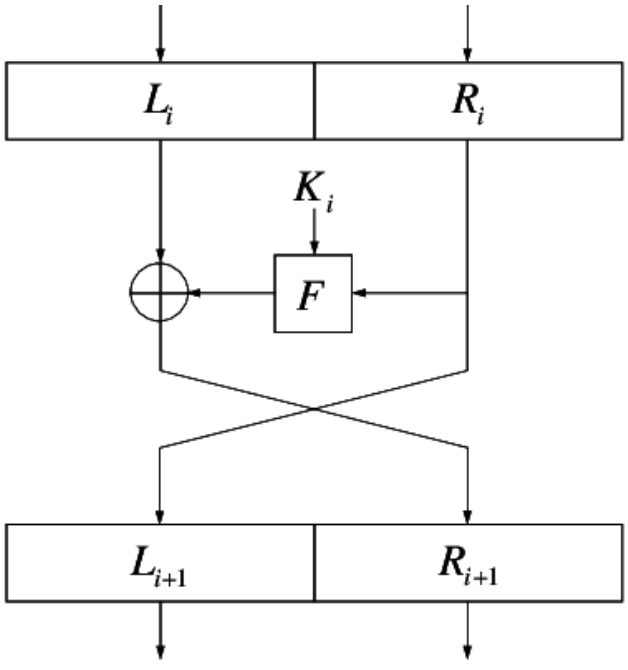
В каждом раунде вычисляются $(i = \overline{0, r-2})$:

$$L_{i+1} = R_i,$$
$$R_{i+1} = L_i \oplus F_{k_{i+1}}(R_i).$$

Последний раунд:

$$L_r = L_{r-1} \oplus F_{k_r}(R_{r-1})$$
$$R_r = R_{r-1}.$$

Сеть Фейстеля



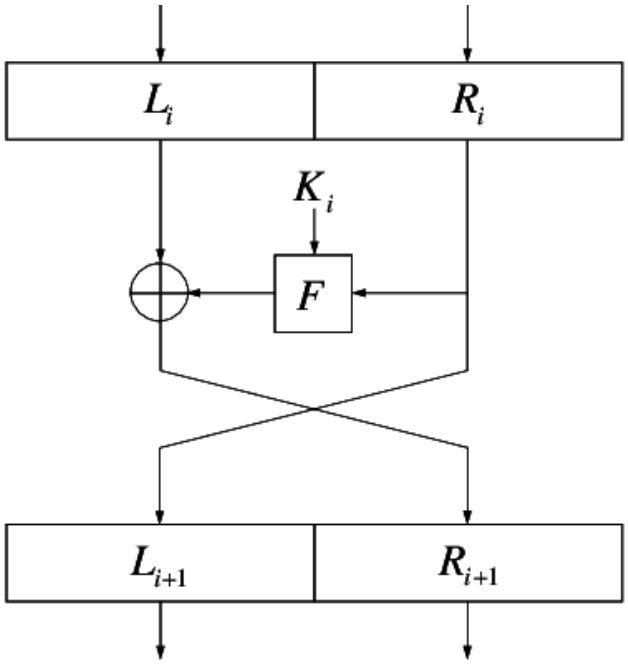
Подстановка Фейстеля:

$$E_{\hat{k}}(L\|R) = R\|(L \oplus F_{\hat{k}}(R)).$$

Подстановка τ:

$$\tau(L\|R) = R\|L.$$

Сеть Фейстеля



Подстановка Фейстеля:

$$E_{\hat{k}}(L\|R) = R\|(L \oplus F_{\hat{k}}(R)).$$

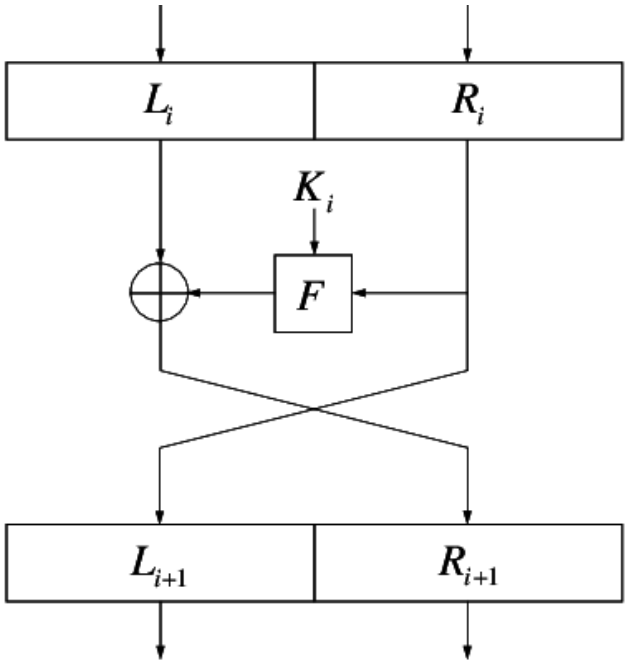
Подстановка τ:

$$\tau(L\|R) = R\|L.$$

Тогда $E_{\hat{k}}$ — является τ-инволютивной подстановкой:

$$E_{\hat{k}}\tau E_{\hat{k}}(L\|R) = E_{\hat{k}}\tau(R\|L \oplus F_{\hat{k}}(R)) =$$
$$= E_{\hat{k}}(L \oplus F_{\hat{k}}(R)\|R) =$$
$$= (R\|L \oplus \cancel{F_{\hat{k}}(R)} \oplus \cancel{F_{\hat{k}}(R)}) = (R\|L) = \tau(L\|R).$$

Сеть Фейстеля



Подстановка Фейстеля:

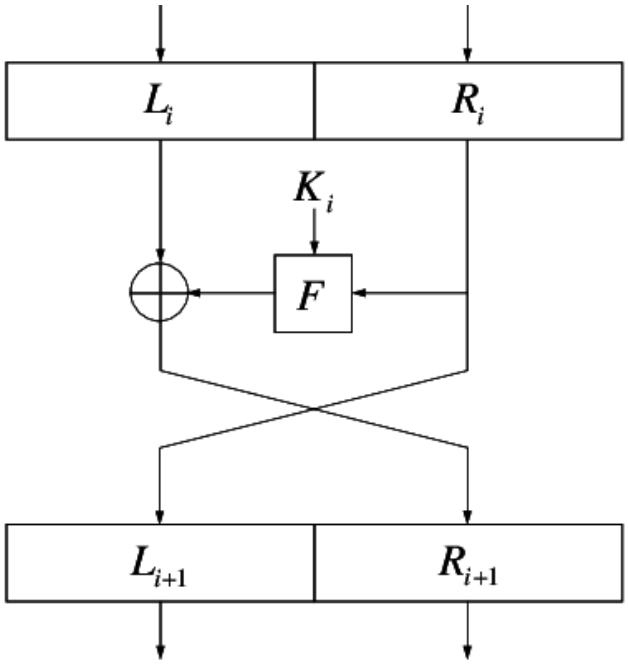
$$E_{\hat{k}}(L\|R) = R\|(L \oplus F_{\hat{k}}(R)) = \tau((L \oplus F_{\hat{k}}(R))\|R).$$

Подстановка τ:

$$\tau(L\|R) = R\|L.$$

Тогда зашифрование является многократной композицией преобразовний усложнения и перемешивания.

Сеть Фейстеля



Подстановка Фейстеля:

$$E_{\hat{k}}(L\|R) = R\|(L \oplus F_{\hat{k}}(R)) = \tau((L \oplus F_{\hat{k}}(R))\|R).$$

Подстановка τ:

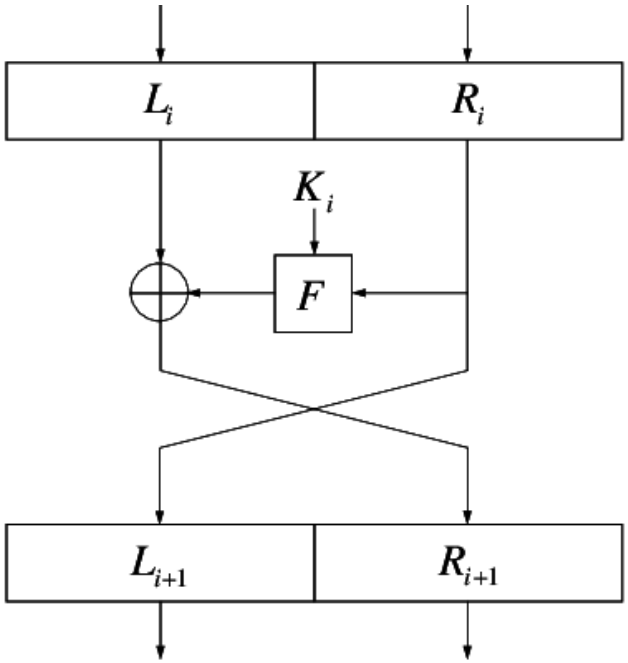
$$\tau(L\|R) = R\|L.$$

Тогда зашифрование является многократной композицией преобразовний усложнения и перемешивания.

Определяется

- Расписанием ключей χ.
- Раундовой вспомогательной функцией F.

Сеть Фейстеля



Подстановка Фейстеля:

$$E_{\hat{k}}(L\|R) = R\|(L \oplus F_{\hat{k}}(R)) = \tau((L \oplus F_{\hat{k}}(R))\|R).$$

Подстановка τ:

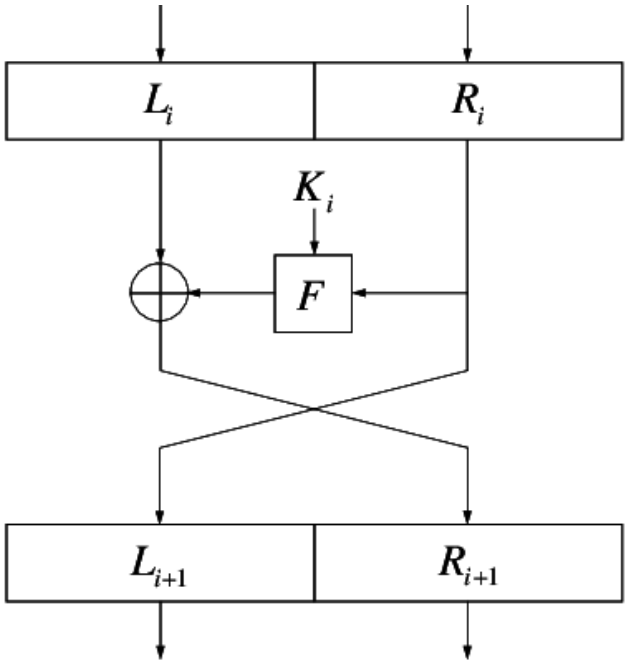
$$\tau(L\|R) = R\|L.$$

Тогда зашифрование является многократной композицией преобразовний усложнения и перемешивания.

Требования к F

- Её работа должна приводить к лавинному эффекту.
- Должна быть нелинейна по отношению к операции $\bigoplus$.

Сеть Фейстеля



Подстановка Фейстеля:

$$E_{\hat{k}}(L\|R) = R\|(L \oplus F_{\hat{k}}(R)) = \tau((L \oplus F_{\hat{k}}(R))\|R).$$

Подстановка τ:

$$\tau(L\|R) = R\|L.$$

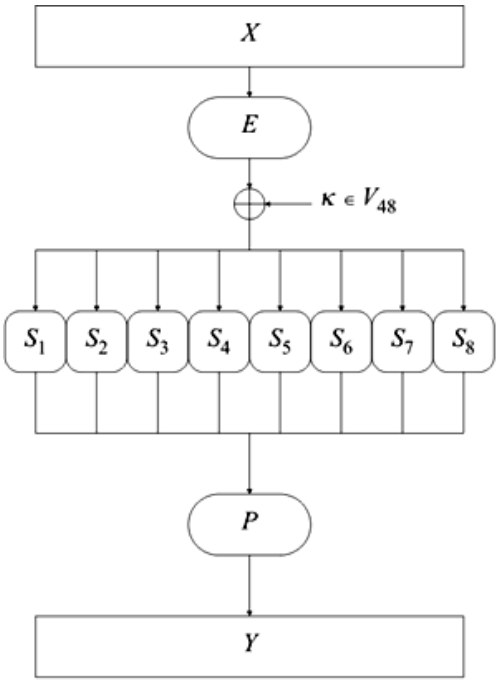
Тогда зашифрование является многократной композицией преобразовний усложнения и перемешивания.

Достоинства:

- обратимость алгоритма независимо от используемой функции F;
- возможность выбора сколь угодно сложной функции F.

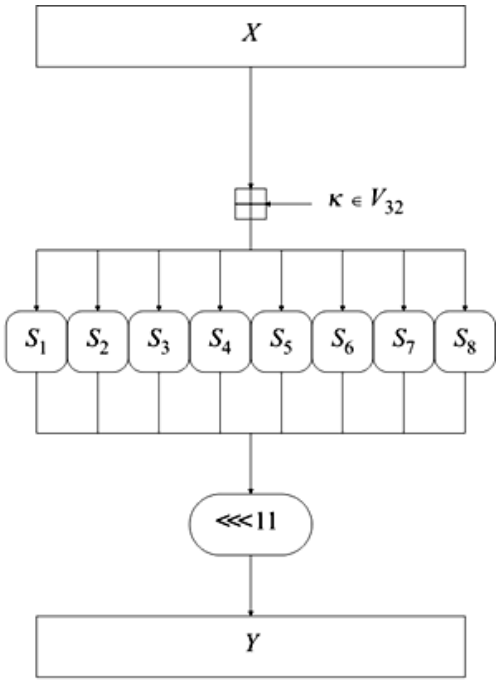
Примеры вспомогательного преобразования Фейстеля

DES



а

ГСОТ 28147-89



б

Алгоритм	L	$\mathcal{K}$	r	$\hat{\mathcal{K}}$	S-блок
DES	64	$\mathbb{B}^{56}$	16	$\mathbb{B}^{48}$	$S_i : \mathbb{B}^6 \to \mathbb{B}^4$ (постоянные)
ГОСТ 28147-89	64	$\mathbb{B}^{256}$	32	$\mathbb{B}^{32}$	$S_i : \mathbb{B}^4 \to \mathbb{B}^4$ (долговременный ключ)

$\oplus$ (mod 2)

$$\begin{array}{cccccccc} & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ \oplus & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}$$

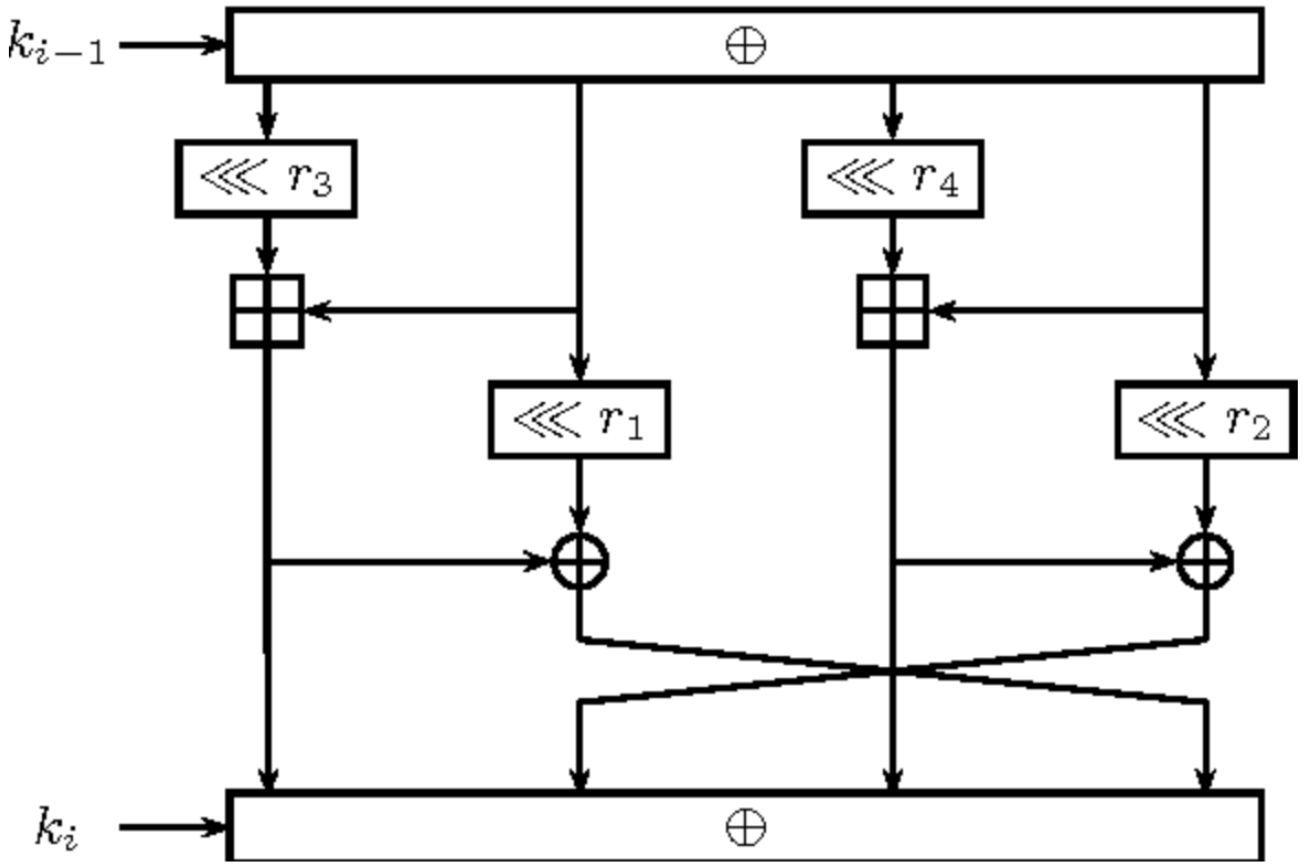
$\boxplus$ (mod 2^n)

$$\begin{array}{cccccccc} & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ \boxplus & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{array}$$

$$(x_{n-1}, x_{n-2}, \ldots, x_1, x_0) \overset{\ggg k}{\to} (x_{k-1}, x_{k-2}, \ldots, x_1, x_0, x_{n-1}, x_{n-2}, \ldots, x_k).$$

$$(x_{n-1}, x_{n-2}, \ldots, x_1, x_0) \overset{\lll k}{\to} (x_{n-1-k}, x_{n-2-k}, \ldots, x_1, x_0, x_{n-1}, x_{n-2}, \ldots, x_{n-1-k+1}).$$

ARX шифры



Режимы шифрования
(Block cipher modes of operation)

Режимы шифрования

Когда блочный алгоритм шифрования используется в определенном режиме работы, полученная конструкция обозначается именем блочного алгоритма, аббревиатурой блочного режима и размером ключа. Примеры:

- AES-256-GCM — алгоритм AES с 256 битным ключом в режиме GCM
- AES-128-CTR — алгоритм AES с 128 битным ключом в режиме CTR
- BF-128-CBC — алгоритм BlowFish с 128 битным ключом в режиме CBC

Основная идея, лежащая в основе режимов блочного шифрования (таких как CBC, CFB, OFB, CTR, EAX, CCM, GCM и др.), заключается в возможности обработке данных, длина которых превышает один блок.

Конфиденциальность

- ECB (Electronic codebook)
- CBC (Cipher block chaining)
- OFB (Output feedback)
- CFB (Cipher feedback)
- CTR (Counter)

Дополнение последнего неполного блока (Padding)

Схемы дополнения

- ANSI X.923
- ISO 10126
- PKCS#7
- ISO/IEC 7816-4

PKCS#7

Дополнение в целых байтах. Значение каждого байта равно числу добавленных байтов, то есть добавляется N байт со значением N. Число добавленных байтов зависит от границы блока, до которого необходимо расширить сообщение. Дополнение будет одним из:

```
01
02 02
03 03 03
04 04 04 04
05 05 05 05 05
...
```

```
... | DD DD DD DD DD DD DD DD | DD DD DD DD 04 04 04 04 |
```

ECB (Electronic codebook)

Великий шифр: середина XVII в. — начало XIX в.

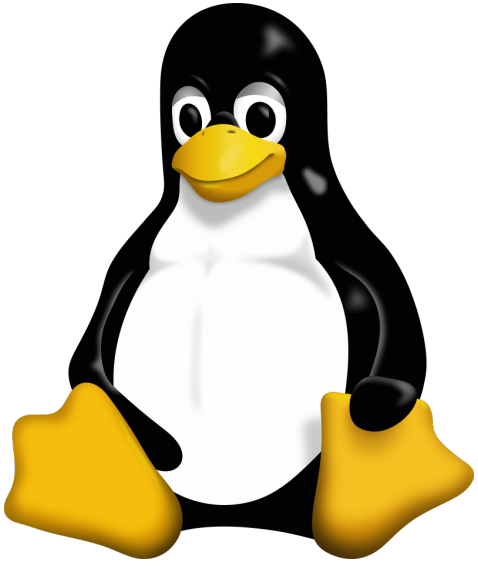
N	O	P	Q	R	S	T	V	X	Y	Z	&
811	117 238	219	407	511	355	340	141 163	205	518	820	279 448
702	359 500	338	595	733	527	618	284 164	436	639		615 827

genera,l,ux.	35	lieu, x	668	Ob	19	presque	801
gens	55	limites	708	obei	59	preten,dre,tion	30
ger	575 95	livre	728	objet, s.	69	pretexte	841
ges	115	le Roy de	758	oblig er, ation	89	pri	881
gla	135	le Prince, de	798	observ, er, ation	129	principa,l,ux	52
gle	215	le Duc de	838	obstacle, s.	179	prisonnier, s.	132
gli	275	le Marquis de	858	obtenir	225	pro	162
glo, ire	355	le Baron de	898	oc, casion	249	prochain	252
gna	375	le Sieur de	69	ocup, er	289	profit, er	262
gne 845	435	loin	79	of	349	projet, s.	282
gni	485	lon	139	office, ier, s	429	propos, ition, s.	282
gno	505	lors	189	offre, s	449	provision, s.	422
gouvern, er, ment	16	luy 848	239	oient	499	prouv	442
gra, æ	405			oir	529	pru	462
grand	525	Ma 868	298	oire	559	publi, er, c	512
gre	585	me 779	339	oit	629	puis, sance	572
gri	625	mi	379	ol	669		
gro	665	mo	439	om	729	Qu	662
gua	695	mu	489	on, s	759	qua	672
gue	735	magasin, s	519	ont,	789	qualite	722
guerre	825	main, s	549	op, pose, ition	819	quand	742
gui, de, s	895	mais 159	579	or	849	quantite	762
		maitre, s	609	ordinaire, s	899	quarente	782
Ba	26	mal, ade, s, je, s,	659	ordonn, er	20	quart, ier, s.	822
be	56	mand, er	679	ordre, s	60	quatre	842
bi	156	maniere, s	719	or, s, t	100	que	862
bo	216	manque, r	739	os, t	130	quel, le, s	882
bu	266	marche, s	769	ou, r	160	question, s.	23
baut	326	marqu, e, r	799	outre	210	qui 50	53
babi, t, le, tant	486	marecha, l, ux	829	ouvr	240	qu'il	73
beur, e, s	656	mauvais	859			quinze	153
bier	796	meilleur	879	La	270	quo, n 190	183

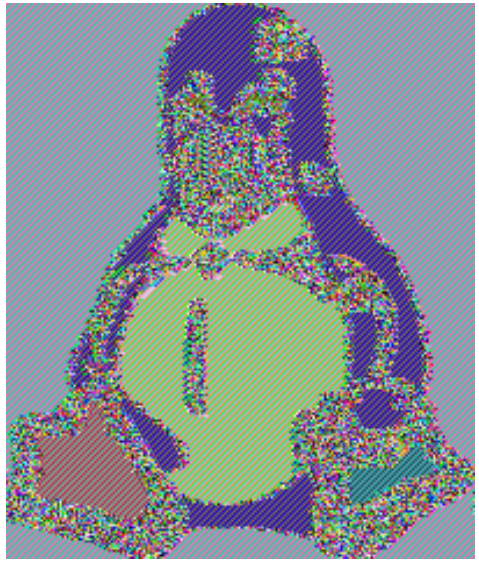
шифр, разработанный Антуаном Россиньолем и его сыном Бонавентуром Россиньолем. Великий Шифр получил такое название из-за своей стойкости и репутации невзламываемого. Модифицированные формы использовались французской армией до лета 1811 года.

ECB

$$p = P_1 \| P_2 \| \ldots \| P_t$$
$$\downarrow$$
$$c = E_k(P_1) \| E_k(P_2) \| \ldots \| E_k(P_t)$$



Оригинал



Режим ECB

Другие режимы

Microsoft Office 365 Message Encryption (OME)

WithSecure, 14.10.2022:

- "(OME) utilitises Electronic Codebook (ECB) mode of operation"

Microsoft:

- "Legacy versions of Office (2010) require AES 128 ECB, and Office docs are still protected in this manner by Office apps."

CBC (Cipher Block Chaining)

CBC

$$p = P_1 \| P_2 \| \dots \| P_t$$
$$\downarrow$$
$$c = C_1 \| C_2 \| \dots \| C_t$$

$$C_i = E_k(P_i \oplus C_{i-1}), \qquad i = \overline{1, t}$$

$$c = E_k(P_1 \oplus C_0) \| E_k(P_2 \oplus C_1) \| \dots \| E_k(P_t \oplus C_{t-1})$$

$C_0 = IV$ — синхропосылка

Синхропосылка обеспечивает уникальность результатов криптографического преобразования на одном и том же ключе. Синхропосылка является **несекретным** параметром и может передаваться вместе с зашифрованными данными.

OFB (Output feedback)
CTR (Counter)

OFB и CTR

$$p = P_1 \| P_2 \| \dots \| P_t$$
$$E_k \to \gamma = \Gamma_1 \| \Gamma_2 \| \dots \| \Gamma_t$$
$$\downarrow$$
$$c = C_1 \| C_2 \| \dots \| C_t$$

$$c = P_1 \oplus \Gamma_1 \| P_2 \oplus \Gamma_2 \| \dots \| P_t \oplus \Gamma_t$$

$$C_i = P_i \oplus \Gamma_i$$

$$\begin{array}{lrcl} \text{OFB}: & \Gamma_i & = & E_k(\Gamma_{i-i}) \\ \text{CTR}: & \Gamma_i & = & E_k(S_i), \quad S_i = \phi(S_{i-1}), \qquad i = \overline{1,t}. \end{array}$$

Γ_0, S_0 — синхропосылка

Сравнение режимов

Свойство	ECB	CBC	OFB	CTR
зависимость от $P_1, \ldots, P_{t-1}$	-	+	-	-
распараллеливание	+	-	-	+
уникальность синхропосылки	не исп.	+	+	+
необходимость E_k^{-1}	+	+	-	-