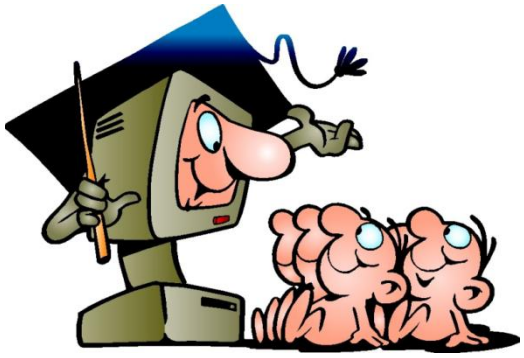
Кафедра № 12 Компьютерные системы и технологии
НИЯУ МИФИ

Защита информации

Иванов М.А.



Лекция № 3.
Основы криптологии

Москва, 2025

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Кодирование
- Шифрование

Это не синонимы !

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование

- Расшифрование
- Дешифрование

Это не синонимы !

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость
- Статистическая безопасность

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость
- Статистическая безопасность
- Рассеивание и перемешивание информации

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость
- Статистическая безопасность
- Рассеивание и перемешивание информации
- Статистическая безопасность последовательности используемых ключей

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость
- Статистическая безопасность
- Рассеивание и перемешивание информации
- Статистическая безопасность последовательности используемых ключей

Стойкость шифра

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость
- Статистическая безопасность
- Рассеивание и перемешивание информации
- Статистическая безопасность последовательности используемых ключей

Стойкость шифра

- Правило Керхгофса

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость
- Статистическая безопасность
- Рассеивание и перемешивание информации
- Статистическая безопасность последовательности используемых ключей

Стойкость шифра

- Правило Керхгофса
- Четыре подхода к анализу стойкости шифров

Криптология

- Криптография
- Криптоанализ

Термины и определения

- Шифр
- Ключ шифра
- Зашифрование
- Расшифрование
- Шифрование
- Дешифрование
- Стойкость шифра

Требования к шифру

- Непредсказуемость
- Статистическая безопасность
- Рассеивание и перемешивание информации
- Статистическая безопасность последовательности используемых ключей

Стойкость шифра

- Правило Керхгофса
- Четыре подхода к анализу стойкости шифров
- Два универсальных метода вскрытия шифров

Правило Керхгофса

Kerckhoffs' principle

- Auguste Kerckhoffs, 1883
  The design of a system should not require secrecy and compromise of the system should not inconvenience the correspondents

Правило Керхгофса

Kerckhoffs' principle

- Auguste Kerckhoffs, 1883
  The design of a system should not require secrecy and compromise of the system should not inconvenience the correspondents

What is it mean?

The security of any cryptosystem should depend only on the secrecy of the key !

Правило Керхгофса

Kerckhoffs' principle

- Auguste Kerckhoffs, 1883
  The design of a system should not require secrecy and compromise of the system should not inconvenience the correspondents

AES ← Rijndael
(Бельгия)

What is it mean?

The security of any cryptosystem should depend only on the secrecy of the key !

Правило Керхгофса

Kerckhoffs' principle

- Auguste Kerckhoffs, 1883
  The design of a system should not require secrecy and compromise of the system should not inconvenience the correspondents

What is it mean?

The security of any cryptosystem should depend only on the secrecy of the key !

AES ← Rijndael
(Бельгия)

Wep ← RC4
(Rivest Cipher № 4)
→ Allegedrcfour

Правило Керхгофса

Kerckhoffs' principle

- Auguste Kerckhoffs, 1883
  The design of a system should not require secrecy and compromise of the system should not inconvenience the correspondents

What is it mean?

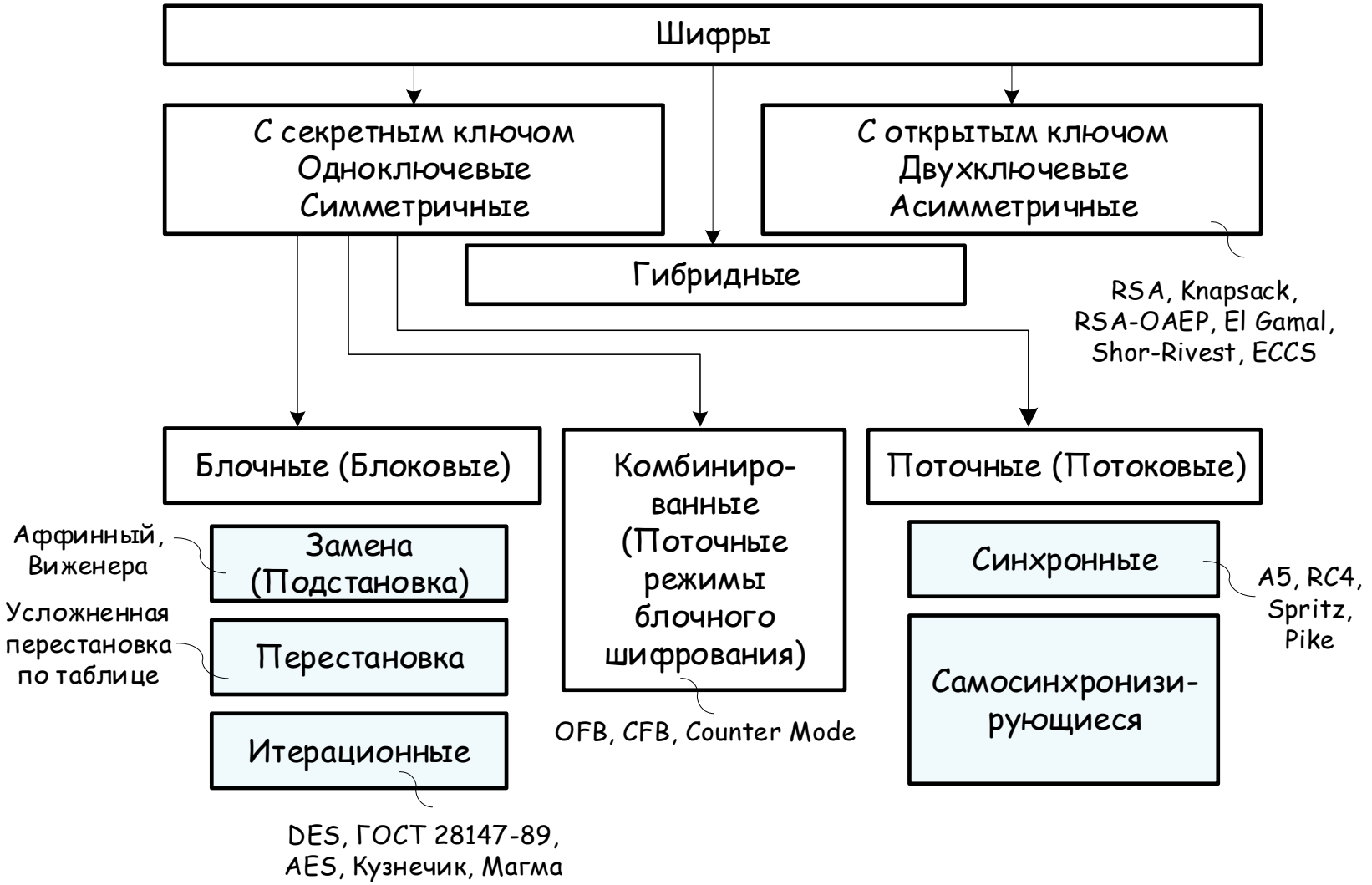
The security of any cryptosystem should depend only on the secrecy of the key !

AES ← Rijndael
(Бельгия)

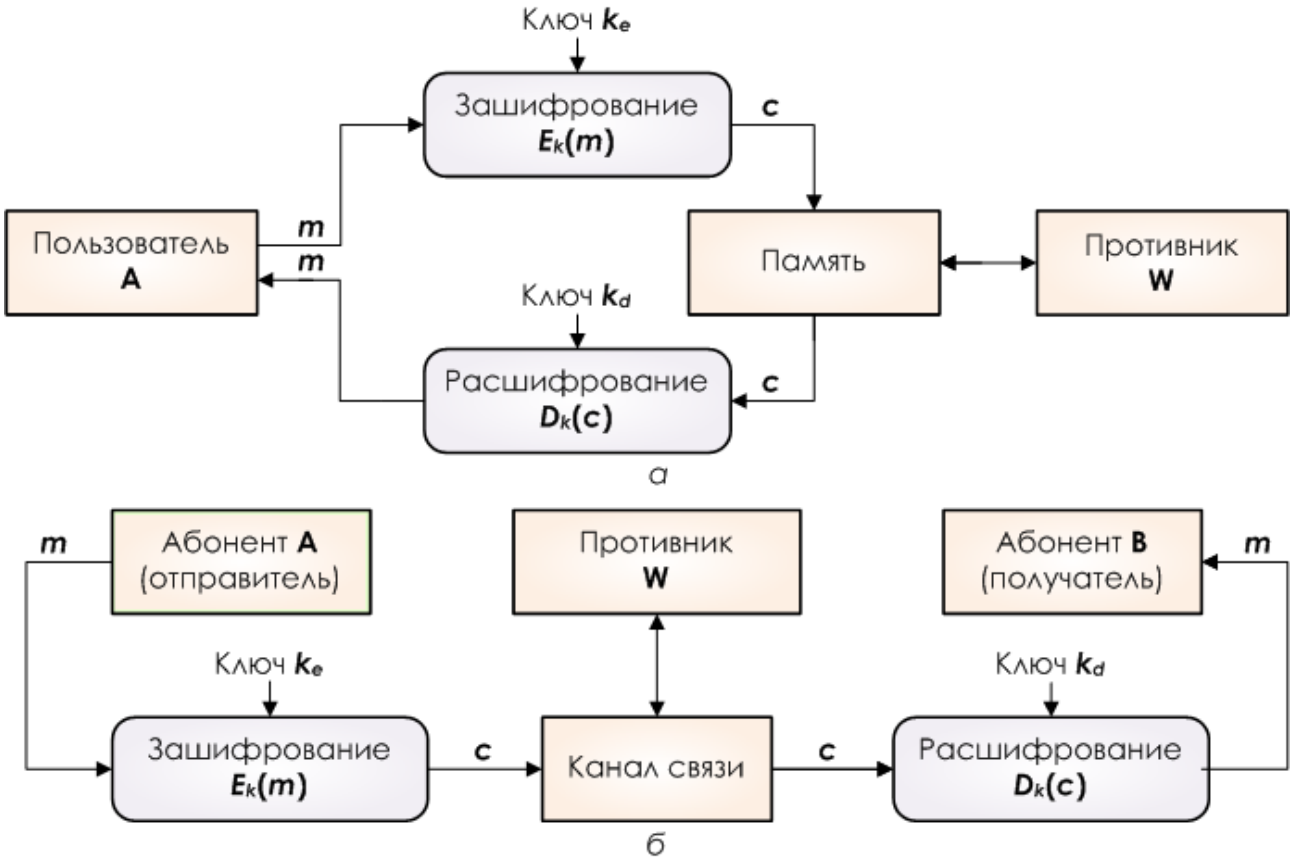
Wep ← RC4
(Rivest Cipher № 4)
→ Allegedrcfour

GSM ←A5

Классификация шифров

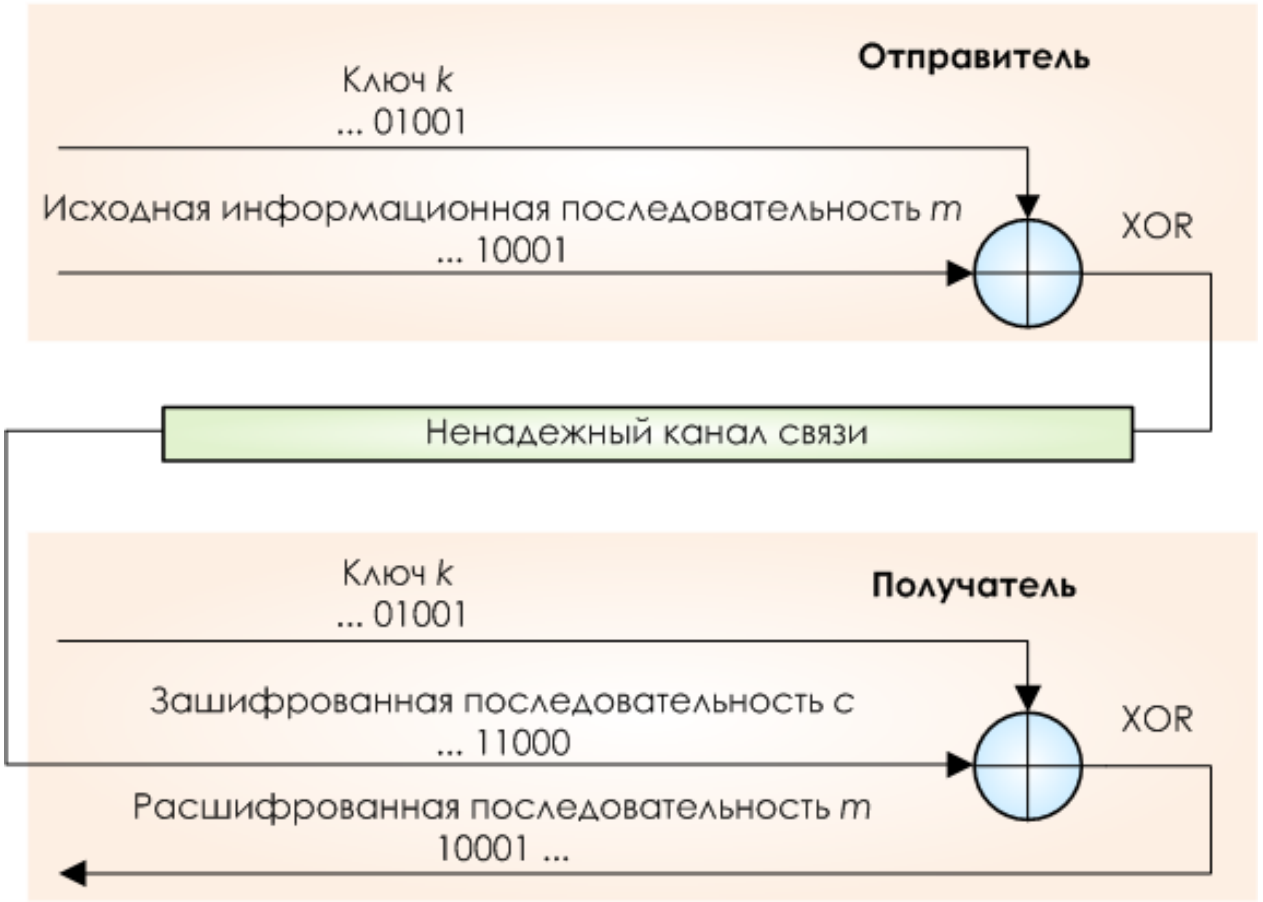


Криптозащита: *а* – при хранении, *б* – при передаче данных

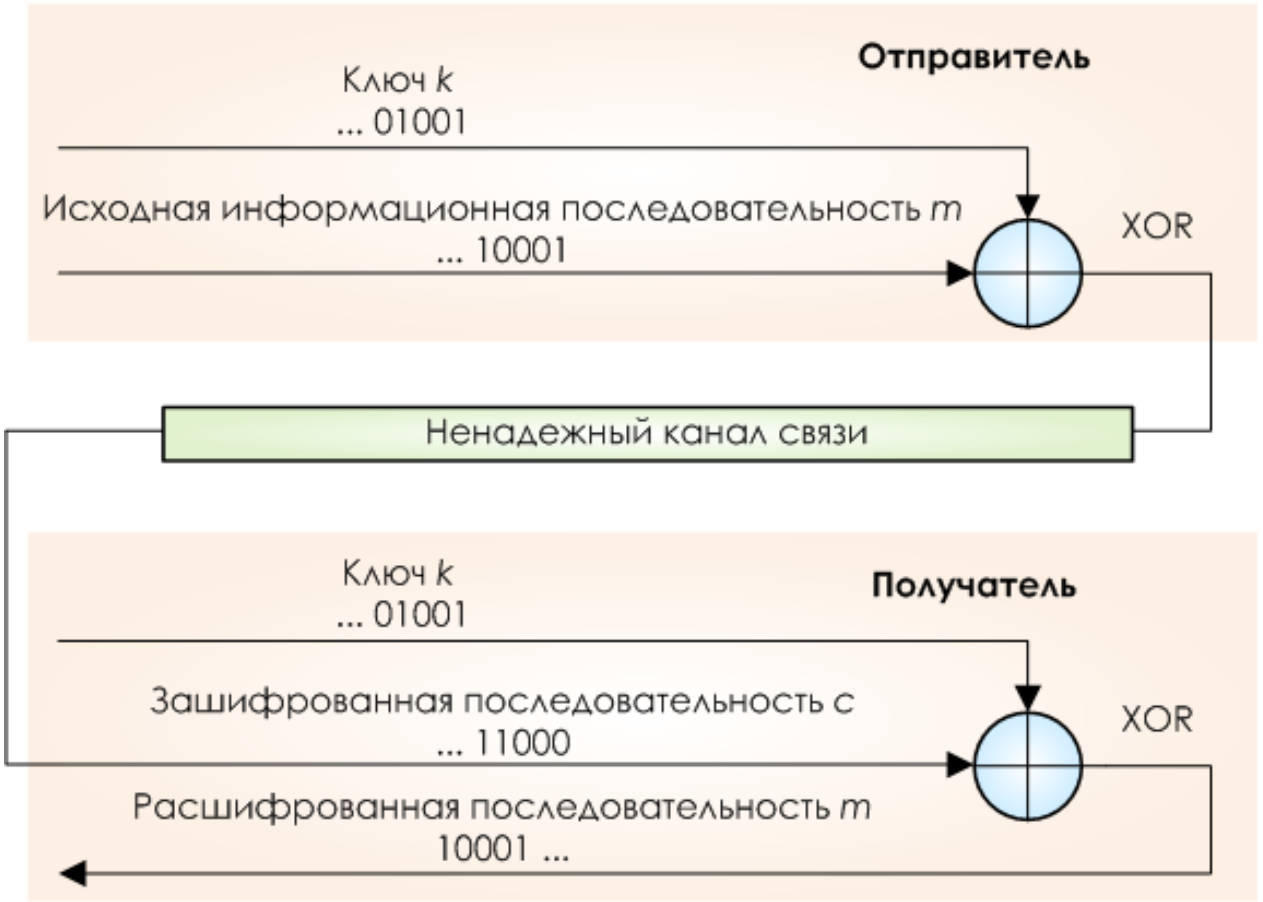


$c = E_k(m)$ – зашифрование, $m = D_k(c)$ – расшифрование
m – сообщение или документ, c – криптограмма
E_k, D_k – соответственно функции за- и расшифрования

Абсолютно стойкий шифр (Совершенно секретный шифр)



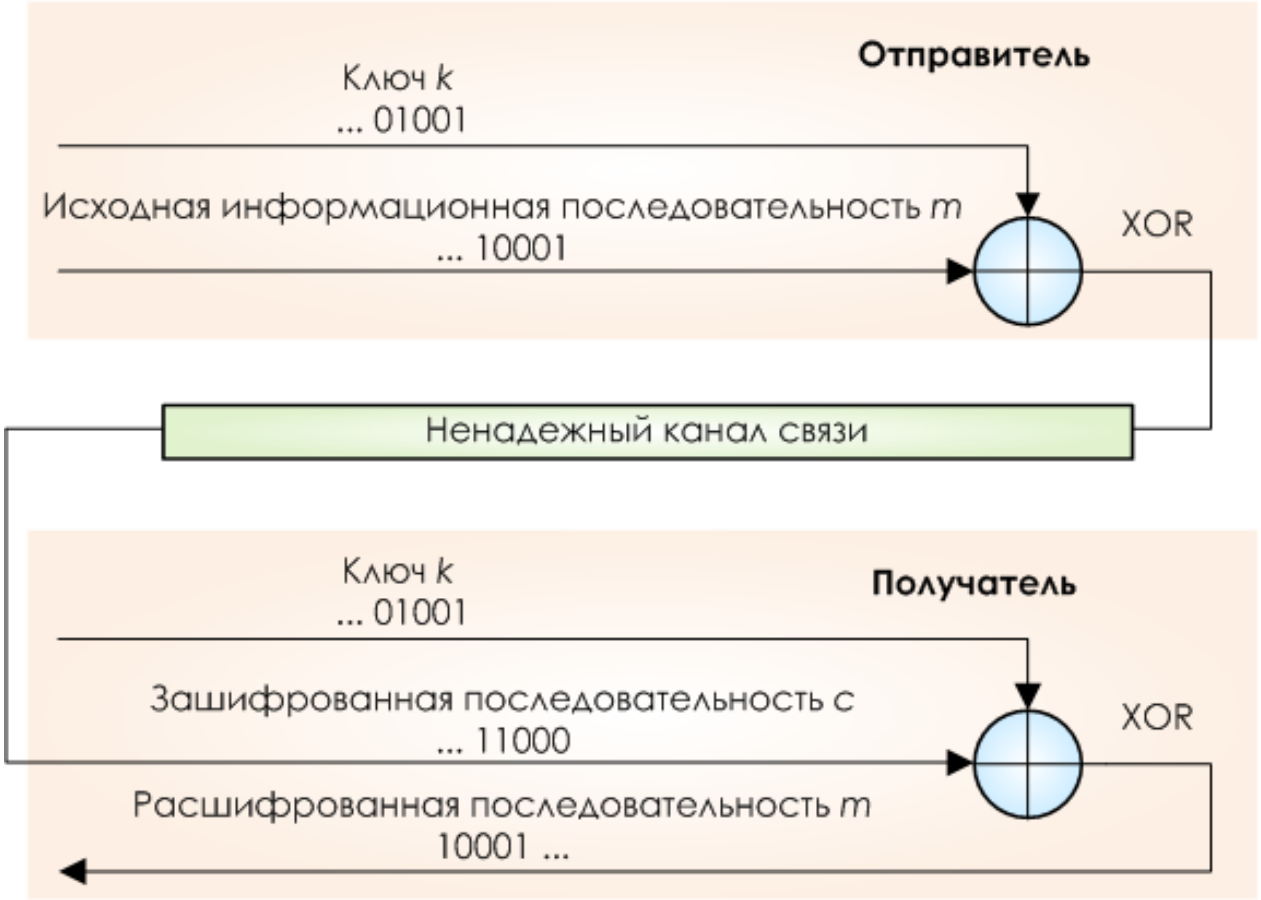
Абсолютно стойкий шифр (Совершенно секретный шифр)



1929 г.
Г.С. Вернам

Абсолютно стойкий шифр (Совершенно секретный шифр)

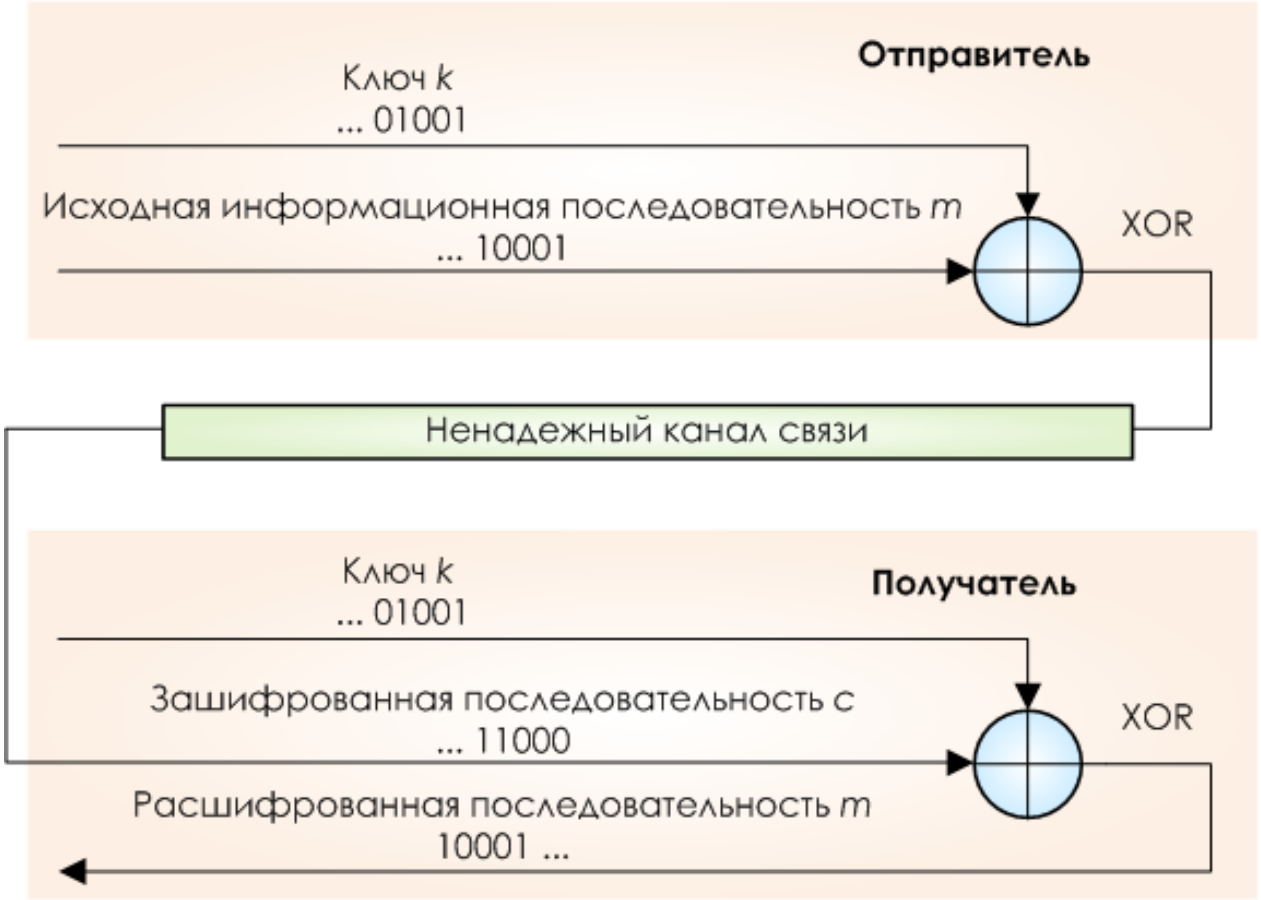
- Разрядность ключа k равна разрядности открытого текста ($|k| = |m|$)



1929 г.
Г.С. Вернам

Абсолютно стойкий шифр (Совершенно секретный шифр)

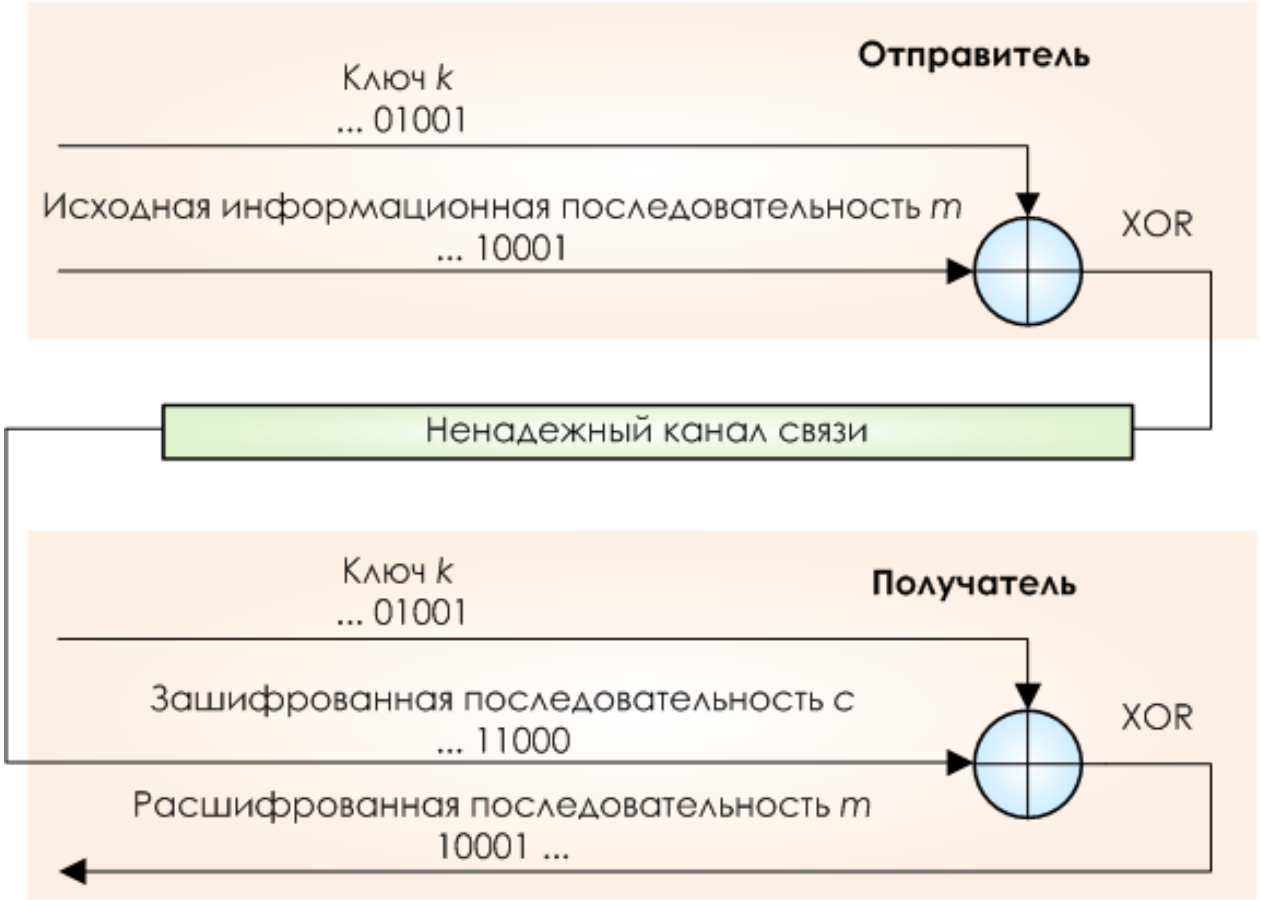
- Разрядность ключа k равна разрядности открытого текста ($|k| = |m|$)
- Ключ k используется только один раз



1929 г.
Г.С. Вернам

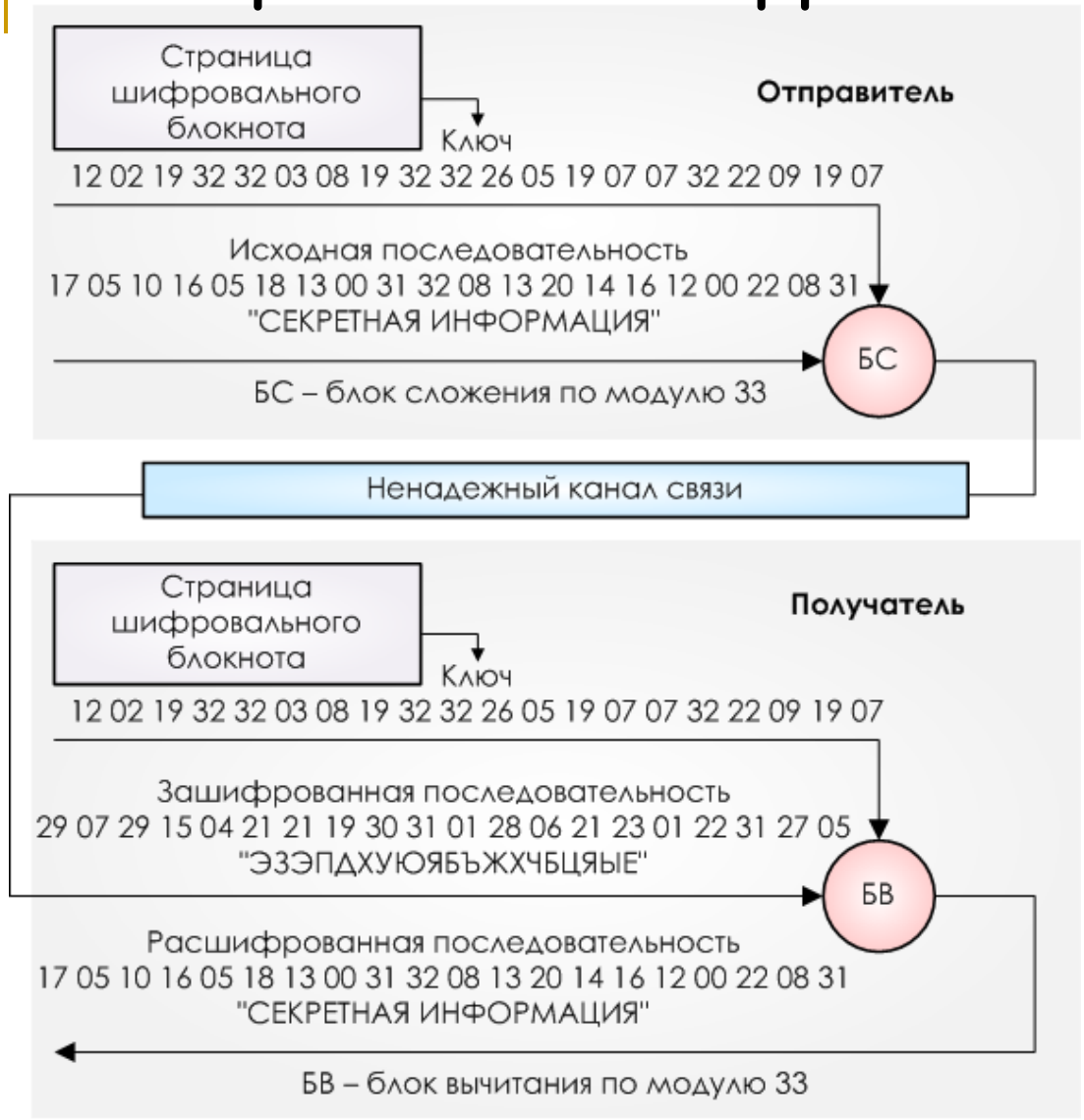
Абсолютно стойкий шифр (Совершенно секретный шифр)

- Разрядность ключа k равна разрядности открытого текста ($|k| = |m|$)
- Ключ k используется только один раз
- Ключ k формируется случайным образом



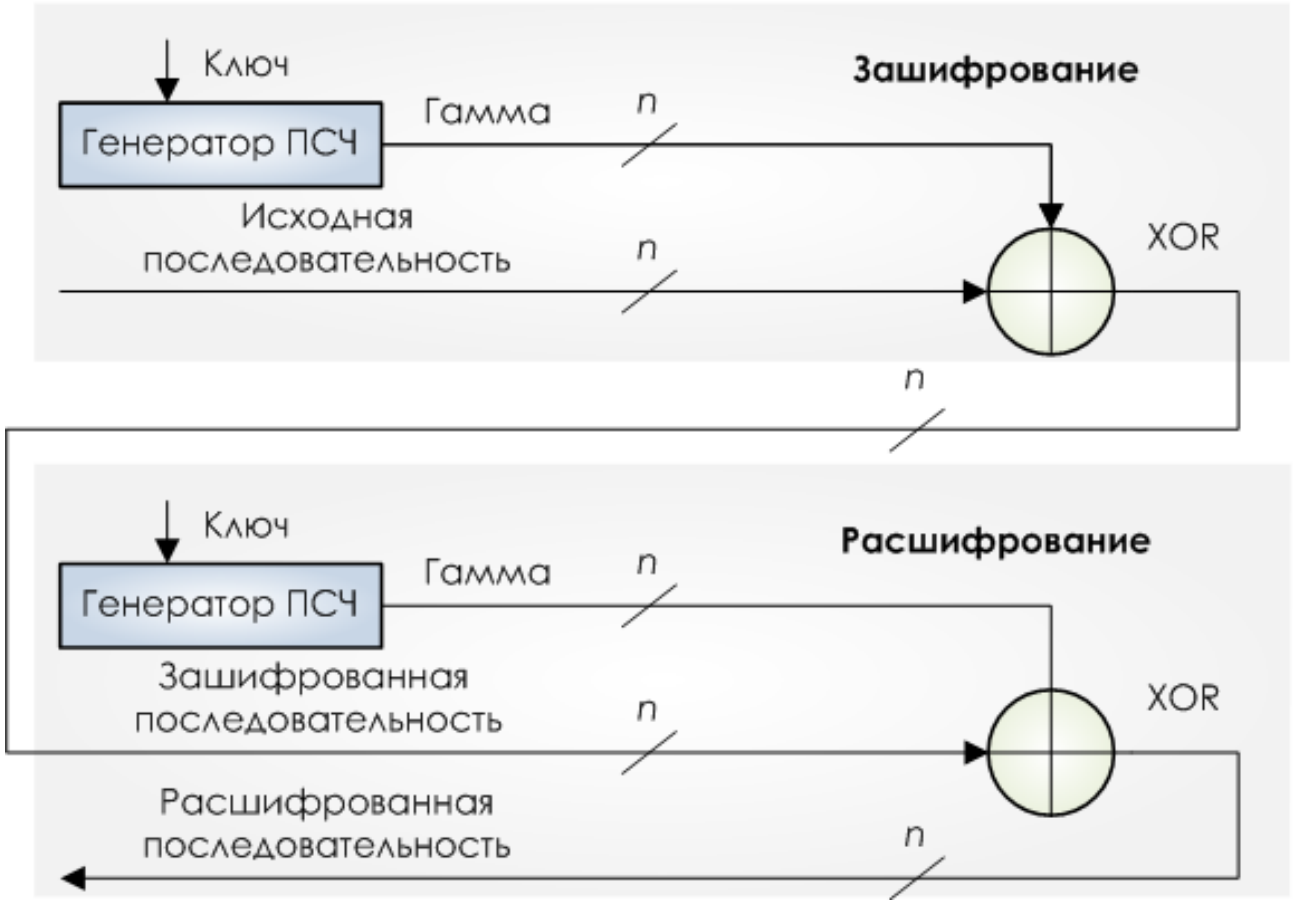
1929 г.
Г.С. Вернам

Одноразовый шифрблокнот

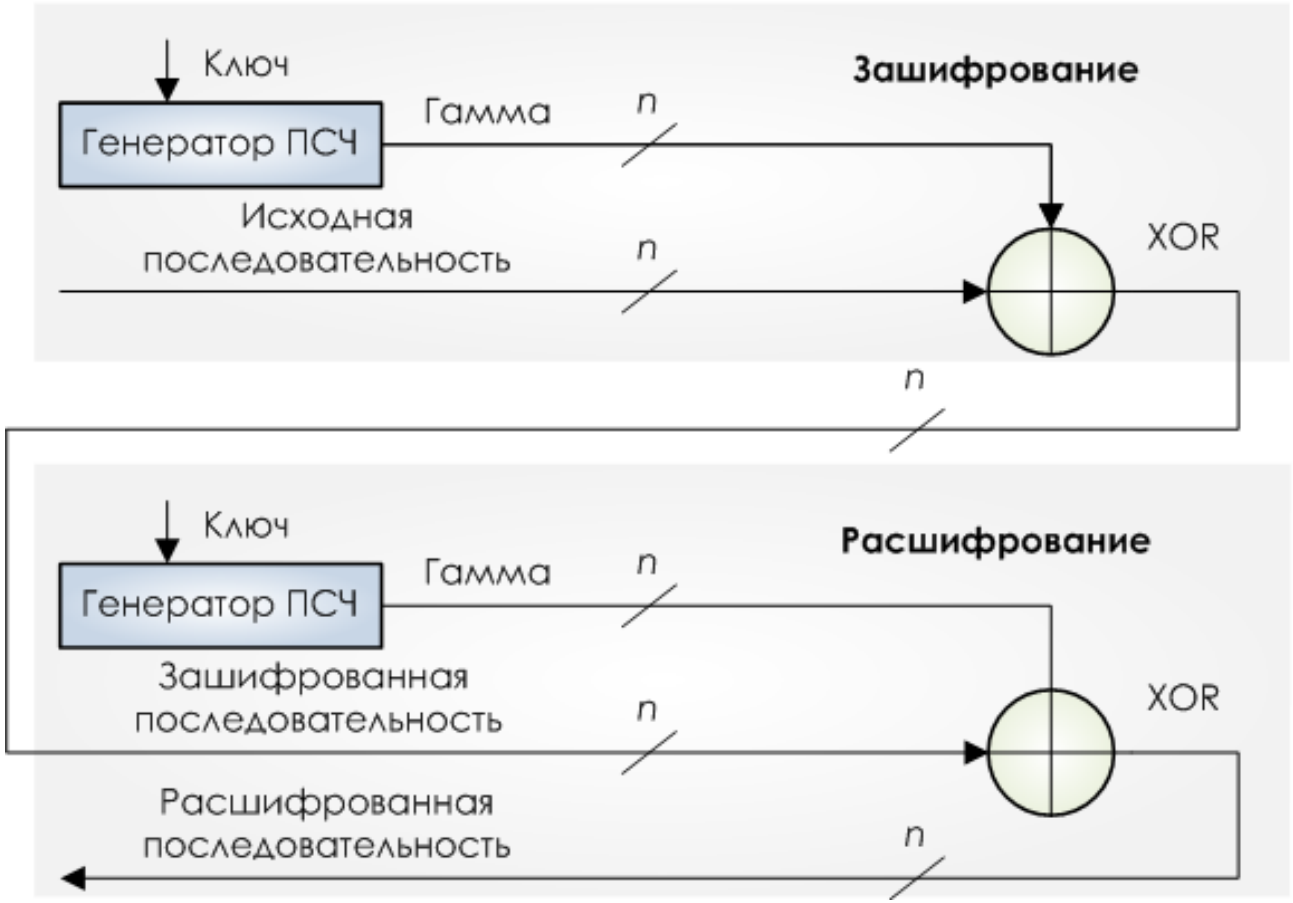


Буква	А	Б	В	Г	Д	Е	Ж	З
Код	0	1	2	3	4	5	6	7
Буква	И	Й	К	Л	М	Н	О	П
Код	8	9	10	11	12	13	14	15
Буква	Р	С	Т	У	Ф	Х	Ц	Ч
Код	16	17	18	19	20	21	22	23
Буква	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	
Код	24	25	26	27	28	29	30	31	32

Гаммирование

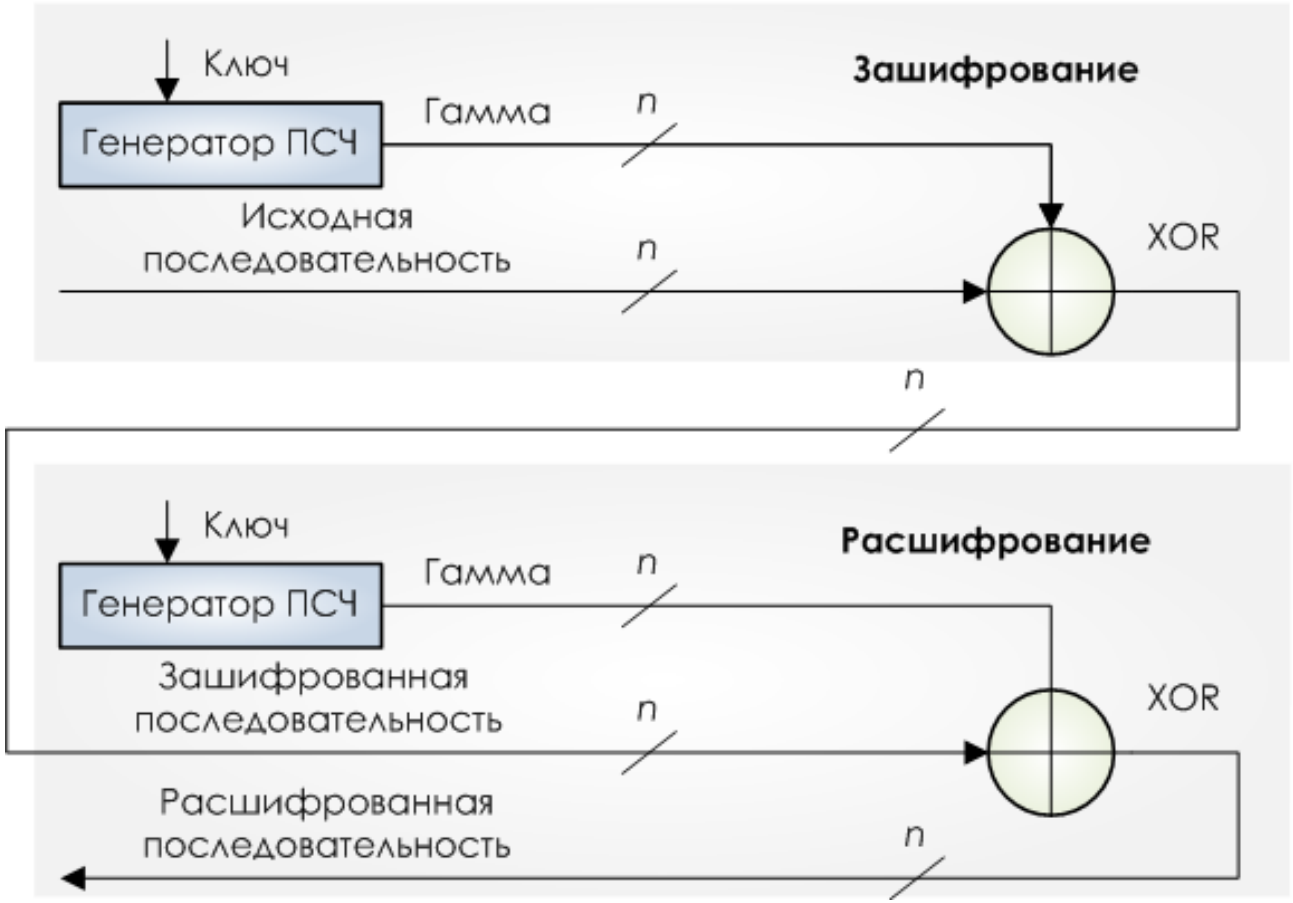


Гаммирование



Свойства

Гаммирование



Свойства

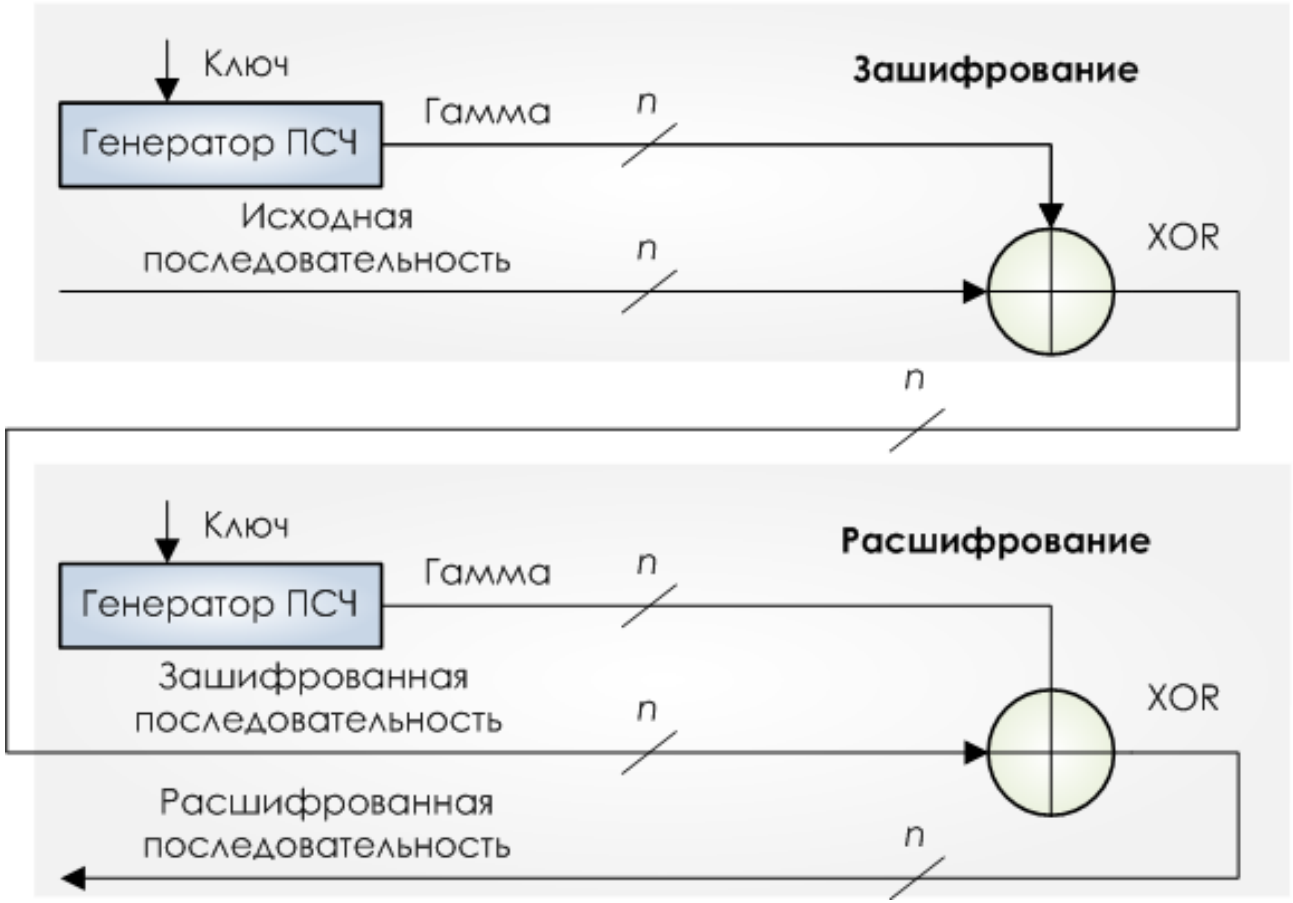
- Противник, не знающий ключа, всегда может вносить предсказуемые изменения в зашифрованный текст

Пусть n = 8, M – “Выдать мистеру Смиту 100$”

$M = M_1 M_2 \ldots$ – исходное сообщение
$C = C_1 C_2 \ldots$ – криптограмма, полученная методом гаммирования
$G = G_1 G_2 \ldots$ – гамма шифра
A_1 - ASCII код “1”, A_9 - ASCII код “9”

- ✓ $M_{22} = A_1 \rightarrow C_{22} = M_{22} \oplus G_{22}$
- ✓ $C_{22}' = C_{22} \oplus A_1 \oplus A_9 = M_{22} \oplus G_{22} \oplus A_1 \oplus A_9 =$
  $= A_1 \oplus G_{22} \oplus A_1 \oplus A_9 = G_{22} \oplus A_9$
- ✓ В расшифрованном сообщении вместо “1” получатель увидит “9”

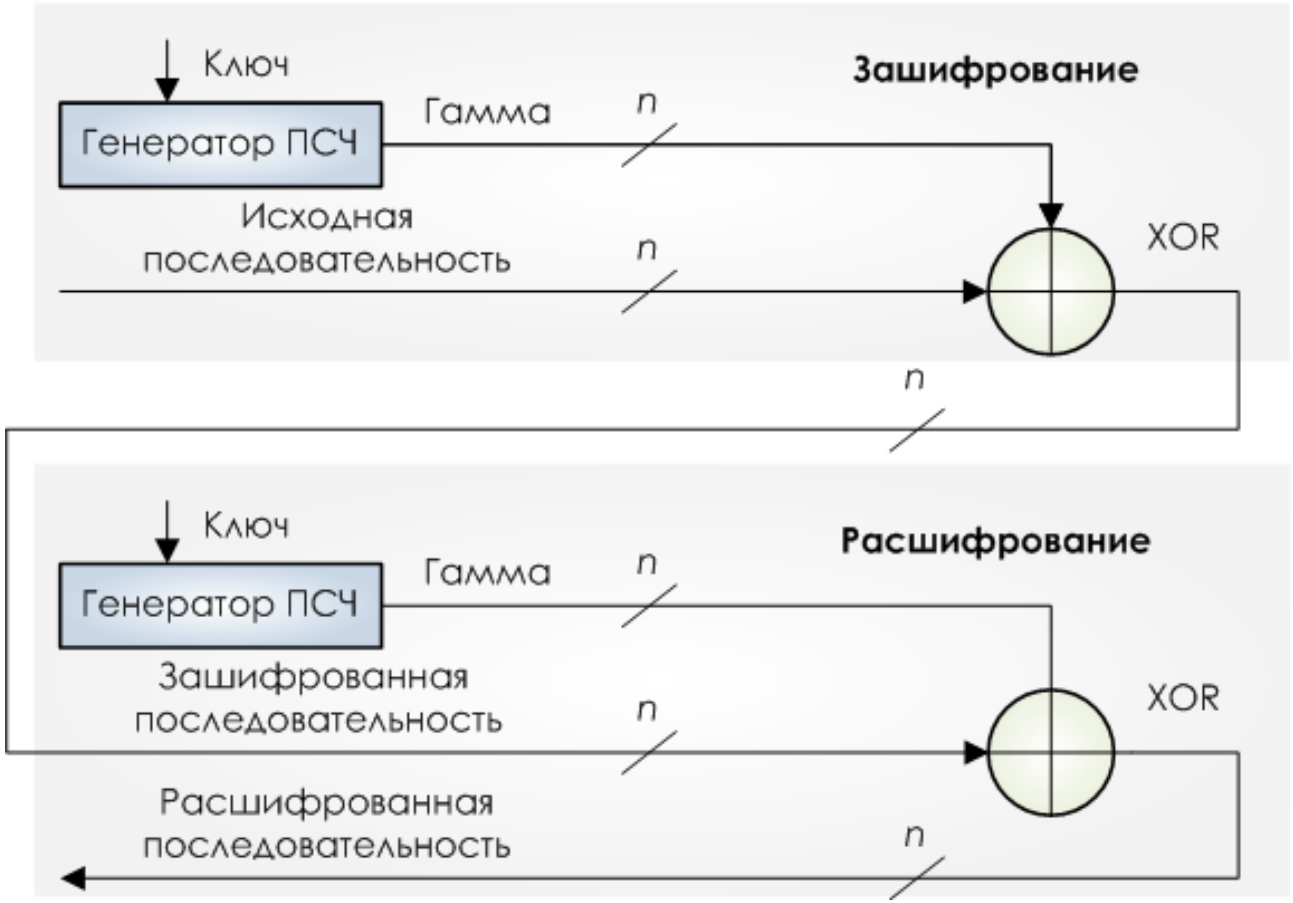
Гаммирование



Свойства

- Противник, не знающий ключа, всегда может вносить предсказуемые изменения в зашифрованный текст
- m = 0 → на выходе гамма

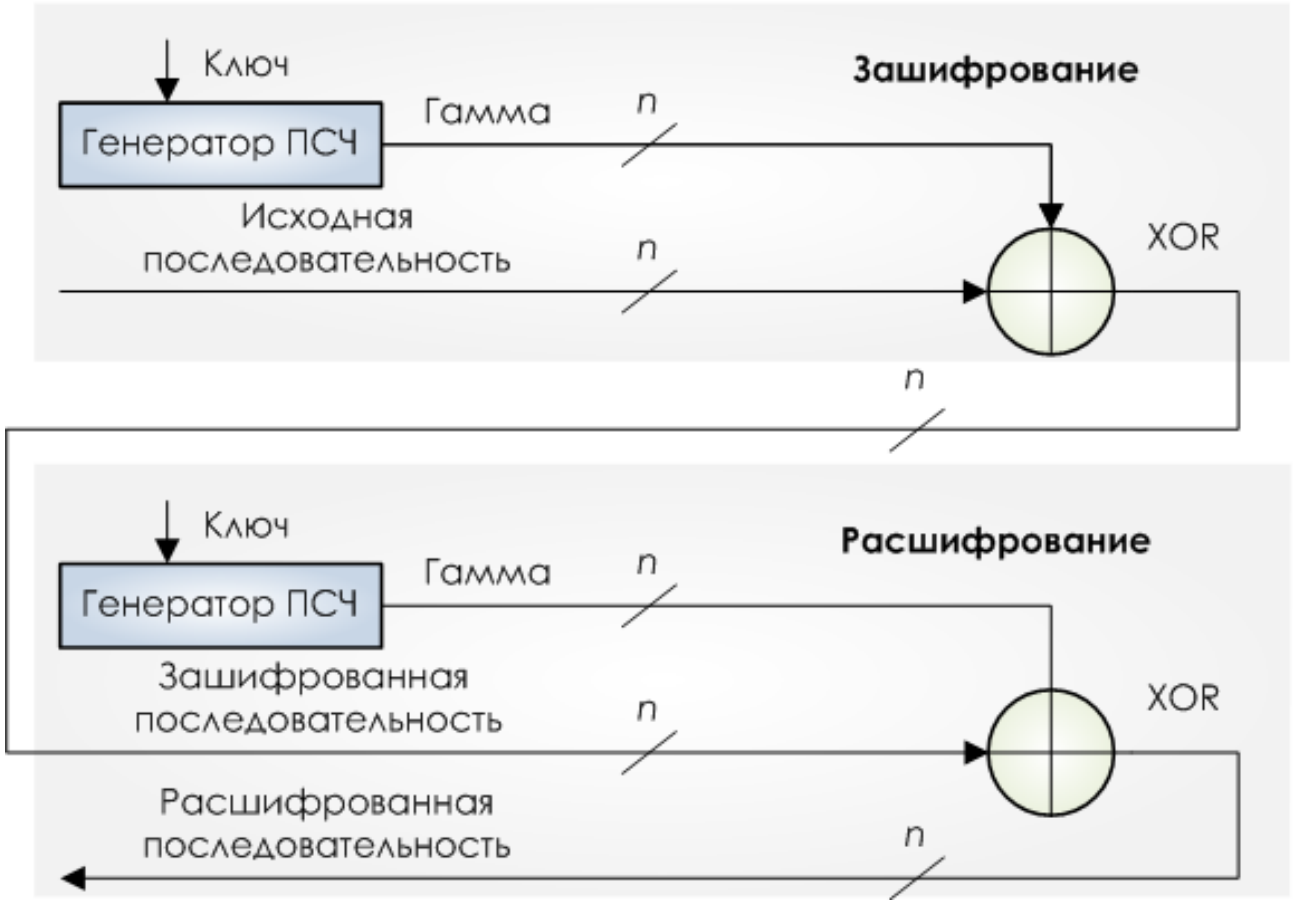
Гаммирование



Свойства

- Противник, не знающий ключа, всегда может вносить предсказуемые изменения в зашифрованный текст
- m = 0 → на выходе гамма
- m = 1 → на выходе инверсная гамма

Гаммирование

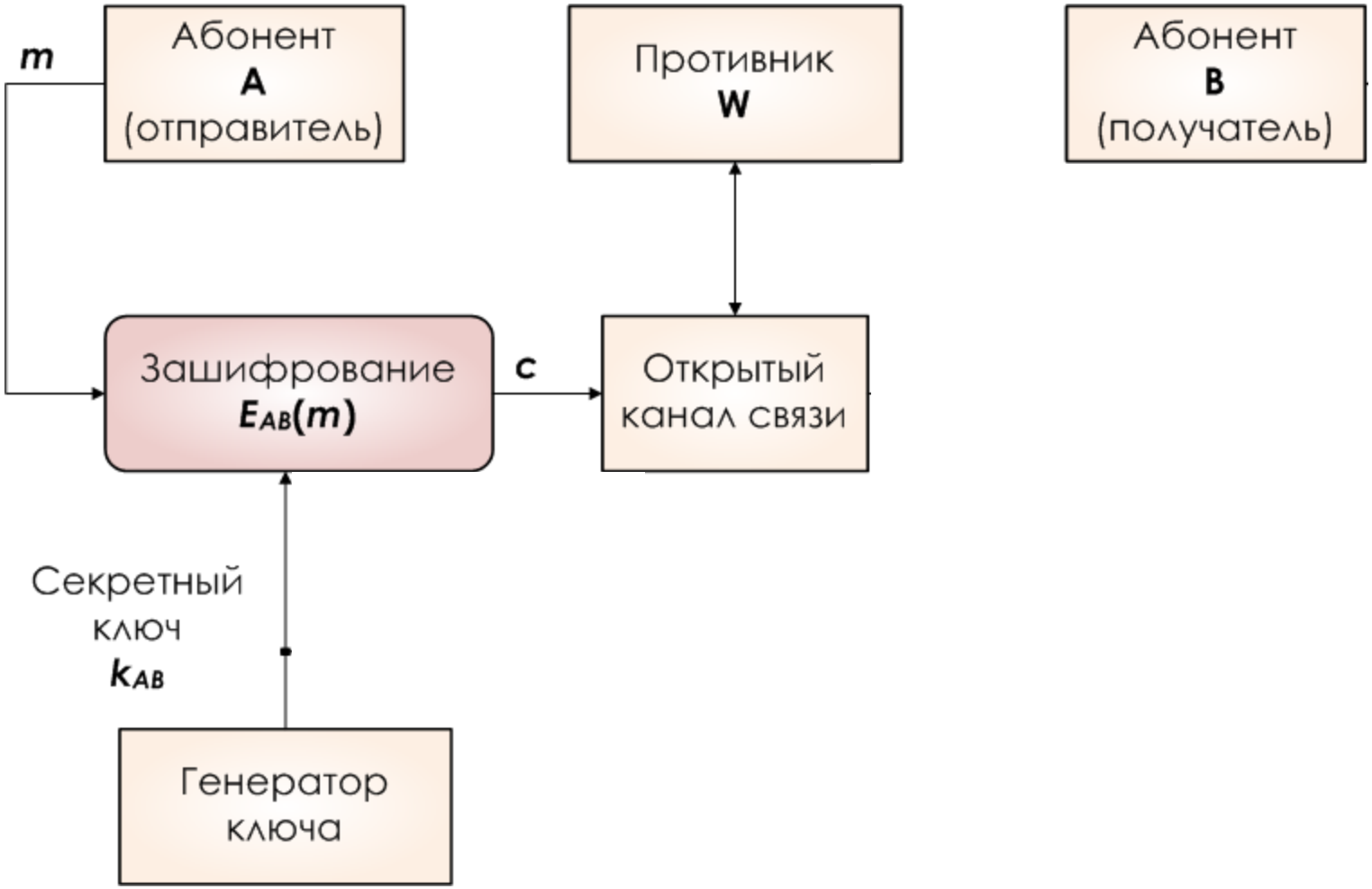


Свойства

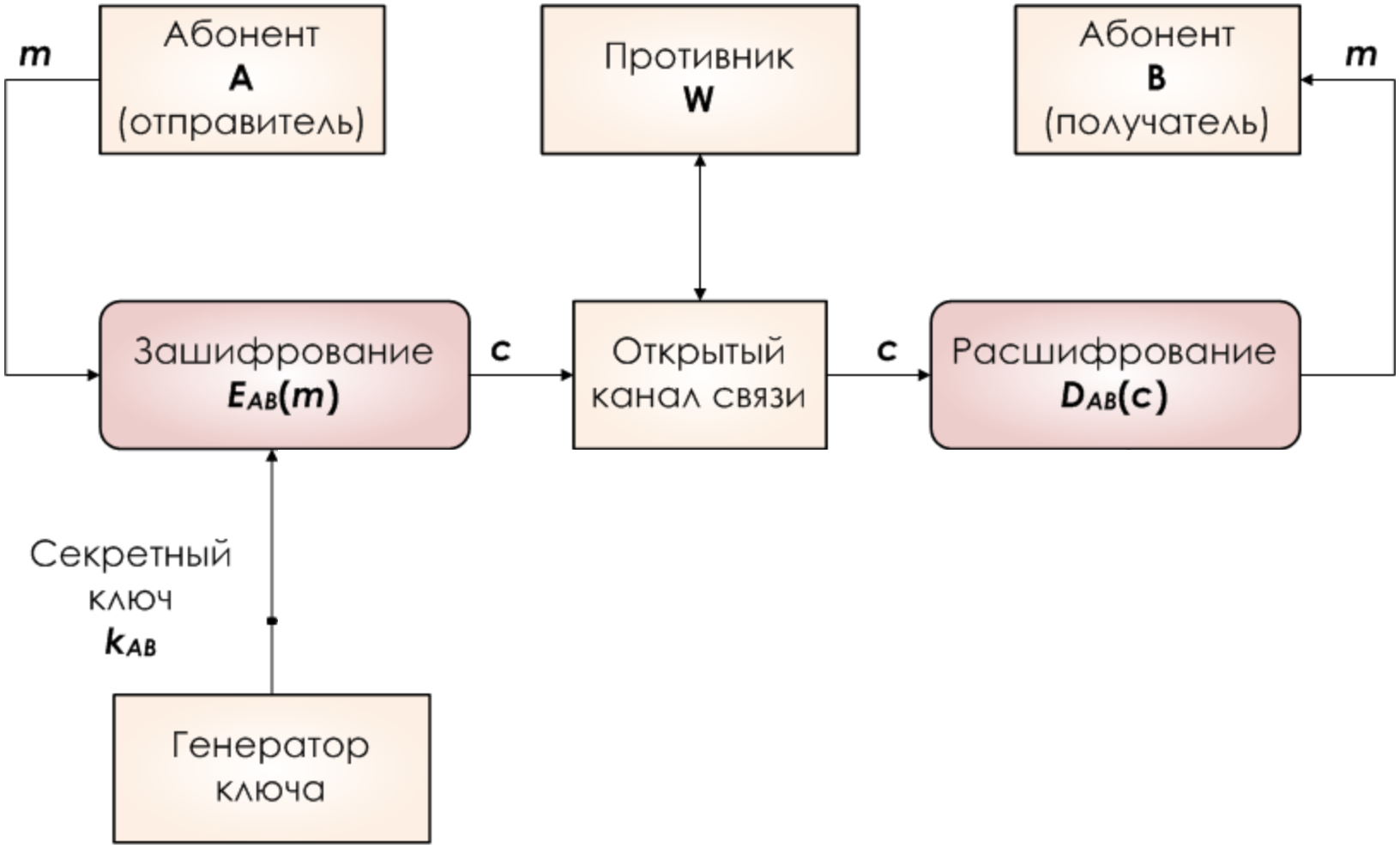
- Противник, не знающий ключа, всегда может вносить предсказуемые изменения в зашифрованный текст
- $m = 0 \rightarrow$ на выходе гамма
- $m = 1 \rightarrow$ на выходе инверсная гамма
- Повторное использование гаммы $\rightarrow c_1 \oplus c_2 = m_1 \oplus m_2$ с последующим применением частотного анализа

Криптосистема с секретным ключом

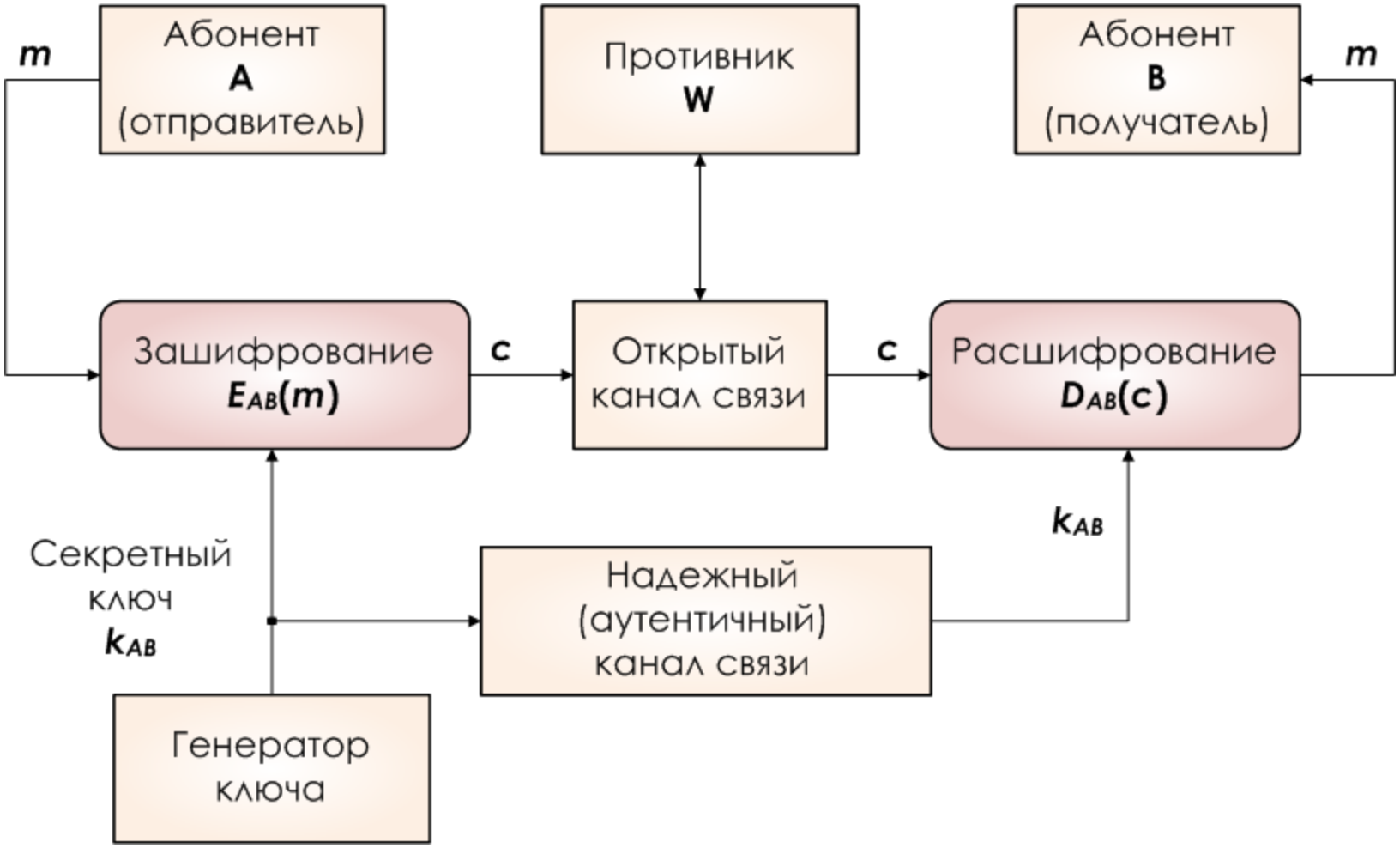
Криптосистема с секретным ключом



Криптосистема с секретным ключом



Криптосистема с секретным ключом



Блочные итерационные шифры

$G = (M, C, K, F)$ – детерминированный шифр

M – множество входных значений

C – множество выходных значений

K – пространство ключей

F – функция зашифрования, $F: M \times K \rightarrow C$

G_i – семейство преобразований

$M_i = C_i = M$, $F_i: M_i \times K_i \rightarrow C_i$, $k_i \in K_i$

Композиционный шифр

$F: M \times (K_1 \times K_2 \times \ldots \times K_r) \rightarrow C$

$F = F_r \bullet \ldots \bullet F_2 \bullet F_1$

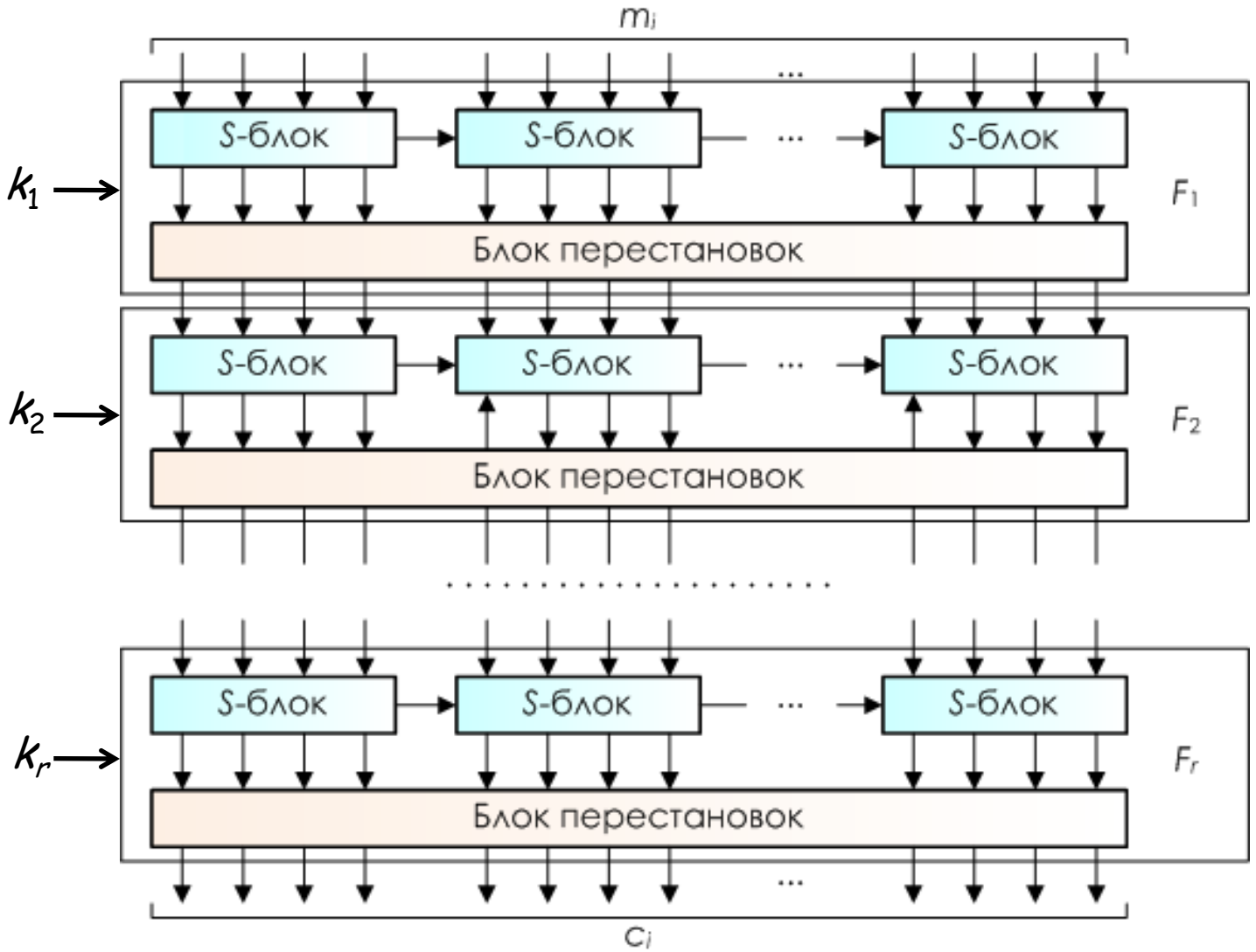
F_i – раунд шифрования

k_i – раундовый ключ

Итеративный шифр суть композиция одной и той же криптографической функции, используемой с разными ключами

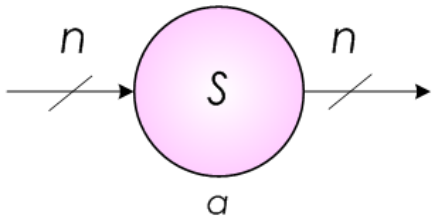
$K_1 = K_2 = \ldots = K_r$, $F_1 = F_2 = \ldots = F_r$

Принцип построения блочных симметричных шифров. SP-сеть

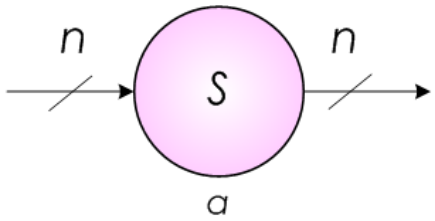


SP-сеть
обеспечивает интенсивное рассеивание и перемешивание информации !!!

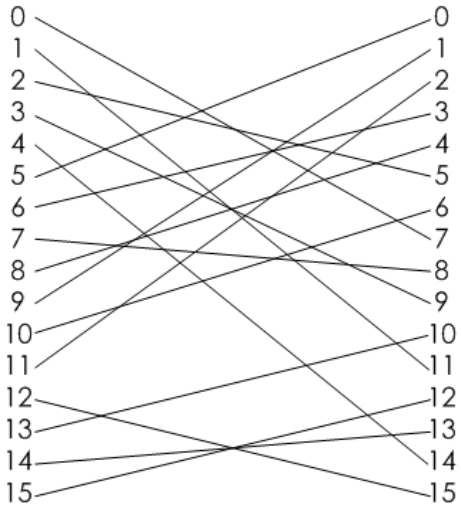
Блок замены (S-блок):
а – УГО



Блок замены (S-блок): а – УГО, б – два способа задания

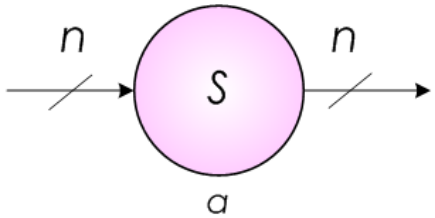


а

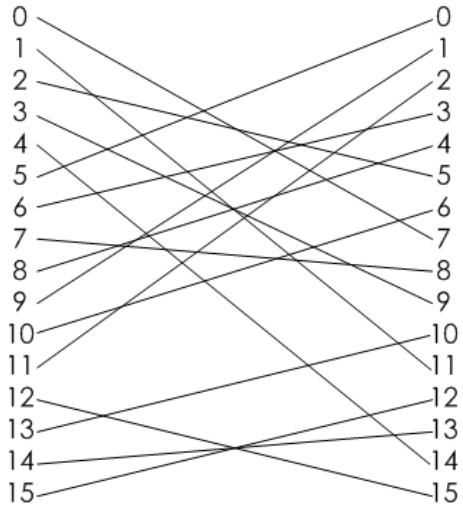


б

Блок замены (S-блок): а – УГО, б – два способа задания



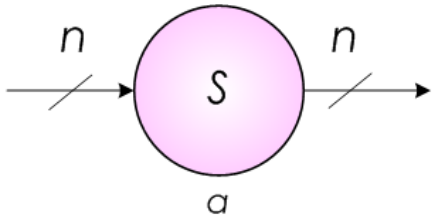
а



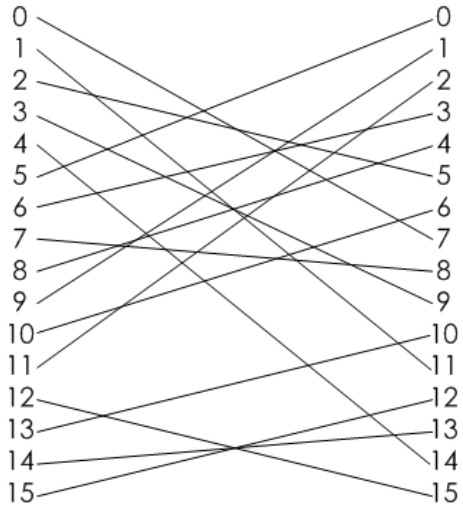
Вход	Выход
0000	0111
0001	1011
0010	0101
0011	1001
0100	1110
0101	0000
0110	0011
0111	1000
1000	0100
1001	0001
1010	0110
1011	0010
1100	1111
1101	1010
1110	1101
1111	1100

б

Блок замены (S-блок): а – УГО, б – два способа задания



а

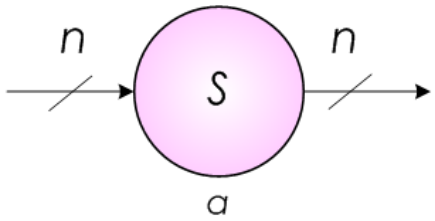


б

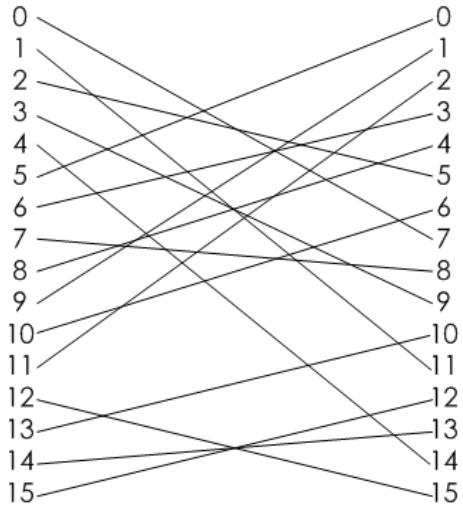
Вход	Выход
0000	0111
0001	1011
0010	0101
0011	1001
0100	1110
0101	0000
0110	0011
0111	1000
1000	0100
1001	0001
1010	0110
1011	0010
1100	1111
1101	1010
1110	1101
1111	1100

Объем таблицы замен $4 \times 2^4 = 64$ бита

Блок замены (S-блок): а – УГО, б – два способа задания



а



Вход	Выход
0000	0111
0001	1011
0010	0101
0011	1001
0100	1110
0101	0000
0110	0011
0111	1000
1000	0100
1001	0001
1010	0110
1011	0010
1100	1111
1101	1010
1110	1101
1111	1100

Объем таблицы замен $4 \times 2^4 = 64$ бита

б

В общем случае объем ***n***-разрядной таблицы замен равен $n \times 2^n$ бит

Чаще всего в окружающем мире используются
4- и 8-разрядные S-блоки

Ключевой вопрос:
Как получать блоки замен гарантированного качества?

Интересные (но не простые) темы для самостоятельной работы

Reverse-Engineering the S-Box

Algorithm Substitution Attacks (ASA) - a new type of attack against symmetric encryption methods

The questions are welcome !