Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Современные симметричные шифры. ГОСТ 28147-89

Современные симметричные шифры

Классификация современных симметричных шифров

- **Блочные** (**блоковые**) шифры:
  - текст обрабатывается блоками одинакового размера;
  - криптографическое преобразование является итерационным;
  - основные характеристики:
    - длина ключа;
    - длина блока данных;
    - число раундов основного преобразования;
  - предусмотрены специальные режимы для устранения межблочных зависимостей.
- **Поточные** (**потоковые**) шифры.
  - аналогичны шифрам гаммирования для двоичного алфавита;
  - могут строиться на основе блочных шифров с помощью специальных режимов работы.

Российские стандарты симметричного шифрования

- **ГОСТ 28147-89**. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования (**устаревший стандарт**).
  - шифр с длиной блока 64 бита и ключом 256 бит;
  - 4 режима работы шифра.
- **ГОСТ Р 34.12-2015**. Информационная технология. Криптографическая защита информации. Блочные шифры:
  - шифр «Магма» с длиной блока 64 бита и ключом 256 бит;
  - шифр «Кузнечик» с длиной блока 128 бит и ключом 256 бит.
- **ГОСТ Р 34.13-2015**. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров:
  - 6 режимов работы базовых блочных шифров.

Межгосударственные стандарты симметричного шифрования

- **ГОСТ 34.12-2018**. Информационная технология. Криптографическая защита информации. Блочные шифры.
- **ГОСТ 34.13-2018**. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.

Зарубежные стандарты симметричного шифрования

- Data Encryption Standard (DES), стандарт FIPS PUB 46 (**устаревший стандарт**):
  - шифр с длиной блока 64 бита и длиной ключа 64(56) бита.
- Advanced Encryption Standard (AES), стандарт FIPS PUB 197:
  - шифр с длиной блока 128 бит и варьируемой длиной ключа в 128, 192 или 256 бит.
- DES Modes of Operation, стандарт FIPS PUB 81 (с дополнениями):
  - 6 режимов работы базовых блочных шифров.

ГОСТ 28147-89

Общие сведения

- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования:
  - утратил силу 31 декабря 2015 г.;
  - включен в действующий ГОСТ Р 34.12-2015 под названием «Магма».
- Характеристики шифра:
  - длина блока: 64 бита;
  - длина ключа: 256 бит;
  - число раундов: 32;
  - основа: сеть Фейстеля.

Режимы работы

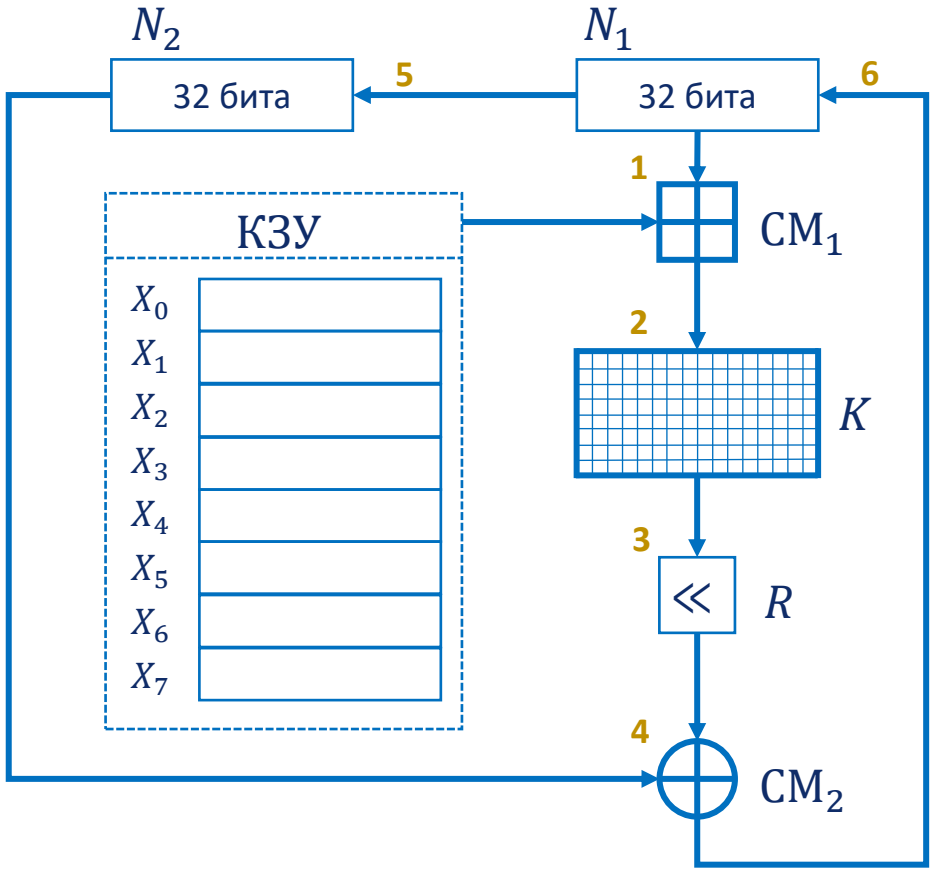
- режим простой замены;
- режим гаммирования;
- режим гаммирования с обратной связью;
- режим выработки имитовставки.

Основные обозначения

- $КЗУ$ — ключевое запоминающее устройство;
- $X_0, \dots, X_7$ — 32-разрядные накопители в составе КЗУ;
- $СМ_1$ — сумматор, осуществляющий сложение по модулю 2^{32};
- $СМ_2$ — сумматор, осуществляющий поразрядное сложение по модулю 2;
- N_1, N_2 — 32-разрядные накопители;
- R — блок циклического сдвига на 11 позиций влево;
- K — блок замен 8×16, содержащий 4-разрядные значения.

Схема шифрования

- Порядок выбора ключей при зашифровании:
  - Раунды 1 – 8: $X_0 X_1 \dots X_7$
  - Раунды 9 – 16: $X_0 X_1 \dots X_7$
  - Раунды 17 – 24: $X_0 X_1 \dots X_7$
  - Раунды 25 – 32: $X_7 X_6 \dots X_0$
- Порядок выбора ключей при расшифровании:
  - Раунды 1 – 8: $X_0 X_1 \dots X_7$
  - Раунды 9 – 16: $X_7 X_6 \dots X_0$
  - Раунды 17 – 24: $X_7 X_6 \dots X_0$
  - Раунды 25 – 32: $X_7 X_6 \dots X_0$



Обратимость схемы шифрования

- Нелинейная функция:
  - $\Psi(T, X) = R\big(K(T \boxplus X)\big)$
- Зашифрование:

Блок открытого текста	A	B
Раунд 1	B	$\Psi(B, X_0) \oplus A$
Раунд 2	$\Psi(B, X_0) \oplus A$	$\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B$
Раунд 3	$\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B$	$\Psi(\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B, X_2) \oplus \Psi(B, X_0) \oplus A$
Блок шифртекста	$\Psi(\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B, X_2) \oplus \Psi(B, X_0) \oplus A$	$\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B$

Обратимость схемы шифрования

- Нелинейная функция:
  - $\Psi(T, X) = R\big(K(T \boxplus X)\big)$
- Расшифрование:

Блок шифртекста	$\Psi(\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B, X_2) \oplus \Psi(B, X_0) \oplus A$	$\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B$
Раунд 1	$\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B$	$\Psi(\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B, X_2) \oplus$ $\oplus \Psi(\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus B, X_2) \oplus$ $\oplus \boldsymbol{\Psi(B, X_0)} \oplus \boldsymbol{A}$
Раунд 2	$\Psi(B, X_0) \oplus A$	$\Psi(\Psi(B, X_0) \oplus A, X_1) \oplus \Psi(\Psi(B, X_0) \oplus A, X_1) \oplus \boldsymbol{B}$
Раунд 3	B	$\Psi(B, X_0) \oplus \Psi(B, X_0) \oplus \boldsymbol{A}$
Блок шифртекста	A	B

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru