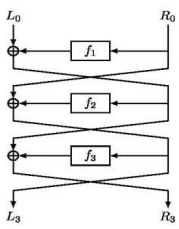
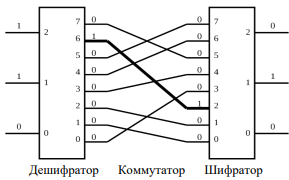
**1976** – утвержден стандарт DES (Data Encryption Standart). Сертифицируется каждые 5 лет.   
**1998** – принят станарт AES (Advanced…)стр 59

**Блочные шифры** – симметр комбинационные шифры, строятся на осн. подстан и перест шифров.  
Предполаг. разбиение откр. текста на равные блоки, к кот. примен однотипная процедура шифрования (раунды)

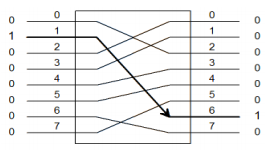
**Требования к шифрам:**  
\* чуть измен M == очень измен C  
\* устойч к атакам  
\* алг расш/заш реализ на разл. платформах  
\* алг базир на простых операциях  
\* алг прост для написания кода  
\* алг д. допуск модификацию

**Сеть Фейстеля:**

ячеистая топология, одна ячейка – один раунд  
\* М разбив на один. *входные* блоки (если длина меньше == удлин)  
\* к. блок дел на 2 один: левый (Lо) и правый (Ro)  
\* в каждом i-ом раунде преобразования:  
 Li = Ri-1  
 Ri = Li-1 + f (Ri-1, Ki)

по какому-то матем. пр-лу вычисл Ki (раундовый ключ)  
+ - поразрядное суммирование (XOR)

**Расшифр** также, но раундовые ключи в обратном порядке

**2 блока (ф-и) преобразований:**  
\* S-блок подстановок  
 - дешифратор (преобр n-разр. 2сс число в 1-разр сигнал по осн 2n)  
 - внутр. коммутатор  
 - шифратор (наоборот)  
\* P-блок перестановок  
 - линейное у-во, т.е. измен положение цифр

**Криптостойкость:**

шифр д. обладать св-вами:  
1) рассеивание – скрыв. отношения М и С  
 - если 1 символ в М измен, неск/все символы в С измен  
2) перемешивание – скрыв. отношения между С и ключом

**БАЗОВЫЕ ОПЕРАЦИИ СЛОЖЕНИЯ ЧИСЕЛ В БЛОЧНЫХ ШИФРАХ**

**A + B (mod 2n):**  
- самое большое слагаемое <2n  
- рез. слож – n-разр число  
- побит. сложение предусм. известную взаимосвязь м/сосед. символами  
- A + B (mod 2n) = остаток от деления (A + B)/2n

Пр: 6+10(mod 24) = 0; 0100+1010=1110 (итог число из 4 младших разрядов)

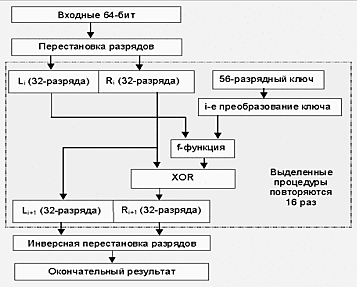
**АЛГОРИТМ DES:**

вх. блок [64] преобраз в вых. блок [64]  
исп *рассеивания* (подстановки) и *перестановки* битов  
=> образуется строит. блок DES – раунд (цикл)  
один блок шифруется 16 раундов

1) первонач. перестановка  
2) раздел блока на Ro[32] и Lo[32]  
3) 16 раундов один. д-й

**Начальная перестановка IP:**

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

  
1 бит на 40 позицию, 58 – на 1-ую и т.д. (рис.1 – общ. DES, рис.2 – ф.f())  
  
1) Ri [32->48] расшир + 16 битов   
лавинный эффект – возрастает завис. всех битов рез-та от исх. битов и ключа  
2) XOR c подключом Ki[48]   
3) рез.[48] на S-блок (подстановка) => [32]  
 S-блок: из 8 блоков [6] -> 8 блоков [4] по *таблице замен*  
4) рез. [32] на P-блок (перестан)  
5) рез. XOR с Lo[32]  
6) Lo и Ro мен. местами ==след.раунд==>

**Конечная перестановка IP-1: (обр. к IP)**

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

**КЛЮЧ:**ключ [64] – каждый 8й бит отбрас.  
изначально эти избыточные биты были доб в соотв. с кодом *прост. четности* для обнар ошибок

При *расшифр*. на вход алгоритма подается зашифр. текст  
**НО:** частичные ключи исп. в обр. порядке K16…K1

**Слабые и полуслабые ключи:**

1) Ключ измен при получении к. подключа => опред. первонач. ключи **слабые**  
Первонач. знач дел /2, к. половина сдвигается независимо

Для всех раундов исп. 1 ключ если:  
\* все биты к. половины равны 0 или 1  
\* одна половина сост. из 1, др – 0

2) нек. пары ключей переводят откр. текст в идентичный шифротекст  
т.е. ключ может расшифр сообщ, кот. было зашифровано другим ключом пары => **полуслабые**

**Криптоанализ DES:**

\* **Дифференциальный:** берет пару шифротекстом, анализирует эволюции разностей (XOR) при прохождении откр. текстом раундов DES при шифровании одним ключом  
Исп. эти разности, присваивает разл. вероятности разл. ключам  
наиб вероятный – верный ключ

\* **Линейный:** найдем «хорошие» однораундовые лин. приближения и объед. их

В целом у DES:  
- низкая криптостойкость (полу-слаб. ключи)  
+ выс. скорость (малая длина ключа)  
+ беспл. распростр. по миру  
+ общедоступность  
+ нет необх в лицензионных отчислениях

**3DES:** *форм. запись*: C i = f (Mj, (DES (K3, (DES KK2, (DES, K1))))))  
*реализации*:  
\* DES-EEE3: шифруется 3 раза с 3 разными ключами  
\* DES-EDE3: шифр – расш – шифр с 3 разными ключами  
\* DES-EEE2 и DES-EDE2: как пред, но на 1м и 3м шаге один. ключ   
Расшифр как в обыч. DES: в обра. порядке

**Стандарт AES (Advanced Encryption Standart)**

алг шифр – стандарт в США с 2001 – в основу шифр Rijndael (линейно-подстан. преобразования)

**Стандарт ГОСТ 28147-89: (СССР)**

\* предусм. 3 режима шифрования:  
 *- прост.замена* – для шифр. ключевой инфы *- гаммирование* – для шифр. других д-х *- гаммир. с обр. связью* –  
\* 1 режим выработки *имито-вставки* – для имитозащиты шифр. данных (для защиты от несанкц. изменений)  
\* здесь ключ 256 бит, 32 раунда шифрования, блок 64 бит

**Алгоритм ГОСТ: (это классическая сеть Фейстеля)**  
1) блок д-х разбив на Ri и Li  
2) Ro + подключ раунда (mod 232)  
 Lo шифруется по принятому алг.  
3) рез [32] делится на 8 чисел [4]  
4) к. число == S блок ==> другое [4]  
5) исх. ключ [256] дел на 8 подключей [32]  
 они исп. на к. раунде в порядке: 1-8, 1-8, 1-8, 8-1  
3) Lo шифруется  
4) Lo и Ro мен. местами

**Отличие DES и ГОСТ:**  
\* ключ [256] криптостойче [48]  
\* в осн раунде DES исп нерегулярные перестановки (лавин. эффект)  
 в ГОСТ – 11-битный цикл. сдвиг влево (лучше прогр. реализ)  
\* в ГОСТ надо 8 раундов прежде, чем измен 1 вх. бита повлияет на к. бит рез-та  
 в DES – 5 раундов

**Алгоритм Blowfish (с.73)**

в осн сеть Фейстеля с 16 раундами, длина блока – 64 бит, ключ – любая длина до 448 бит, быстрее чем DES. 2 части:  
\* расширение ключа – преобр ключ в неск массивов подключей общей длиной 4168 байт  
\* за(рас)-шифрование д-х  
к. раунд: перестановка (зав. от ключа) и подстановка (зав. от ключа и д-х)  
операции: XOR и слож по модулю 232успешные атаки не известны

**ЗАДАНИЕ:**

\* раздел вх. потока на блоки к-то длины с дополнением последнего блока  
\* вып. преобразования ключевой инфы  
\* вып. зашифр/расшифр  
\* оценка скорости  
\* пошаговый анализ лавин. эффекта с подсчетом кол-ва измен. символов по отн. к исх.слову  
алг – DES-EEE2 (шифр K1 – шифр K2 – шифр K1 ), ключ любой?

\* проанализ влияение (полу-)слабых ключей на конечный рез. зашифрования и лавинный эффект  
\* оценить степень сжатия М и С (с пом. архиватора)  
\* отчет

\* DES-EEE3: шифруется 3 раза с 3 разными ключами  
\* DES-EDE3: шифр – расш – шифр с 3 разными ключами  
\* DES-EEE2 и DES-EDE2: как пред, но на 1м и 3м шаге один. ключ  
Расшифр как в обыч. DES: в обра. порядке

**Вопросы для контроля и самоконтроля:**

1) Какие простейшие операции применяются в блочных алгоритмах шифрования?  
сложение чисел по модулю 2n, XOR

2) В чем отличие блочных алгоритмов шифрования от потоковых?  
разбиение М на равные блоки, к кот. примен однотипная процедура шифрования (раунды)  
поток – шифруемые символы – одна буква, бит или байт

3) Что понимается под «раундом» алгоритма шифрования?  
Раунд – сов. повторяющихся наборов преобразований, при за(рас)шифровании

4) Охаректиризовать и привести формальное описание сети Фейстеля  
ячеистая топология, одна ячейка – один раунд  
\* М разбив на один. *входные* блоки (если длина меньше == удлин)  
\* к. блок дел на 2 один: левый (Lо) и правый (Ro)  
\* в каждом i-ом раунде преобразования:  
 Li = Ri-1  
 Ri = Li-1 + f (Ri-1, Ki)

по какому-то матем. пр-лу вычисл Ki (раундовый ключ)  
+ - поразрядное суммирование (XOR)

5) Какие стандартные операции исп в блочных алгоритмах шифрования?  
**2 блока (ф-и) преобразований:**  
\* S-блок подстановок  
 - дешифратор (преобр n-разр. 2сс число в 1-разр сигнал по осн 2n)  
 - внутр. коммутатор  
 - шифратор (наоборот)  
\* P-блок перестановок  
 - линейное у-во, т.е. измен положение цифр

6) В чем состоит особенность сложения чисел по модулю 2N?  
- самое большое слагаемое <2n  
- рез. слож – n-разр число  
- побит. сложение предусм. известную взаимосвязь м/сосед. символами  
- A + B (mod 2n) = остаток от деления (A + B)/2n

7) Сложить по модулю 102 пары чисел:  
8) Сложить по модулю 28 двоич. и 16сс:

9) Дать пояснение принципам реализации «лавинного эффекта»  
лавинный эффект – возрастает завис. всех битов рез-та от исх. битов и ключа  
1) Ri [32->48] расшир + 16 битов

10) Выбрать два произвольных блочных алгоритма. В чем стостоят отличия между ними?  
**Отличие DES и ГОСТ:**  
\* ключ [256] криптостойче [48]  
\* в осн раунде DES исп нерегулярные перестановки (лавин. эффект)  
 в ГОСТ – 11-битный цикл. сдвиг влево (лучше прогр. реализ)  
\* в ГОСТ надо 8 раундов прежде, чем измен 1 вх. бита повлияет на к. бит рез-та  
 в DES – 5 раундов

11) Представить графически и пояснить функционал одного раунда блочного алгоритма DES (AES, ГОСТ 28147-89, Blowfish)  
**DES:**  
1) Ri [32->48] расшир + 16 битов  
2) XOR c подключом Ki[48]   
3) рез.[48] на S-блок (подстановка) => [32]  
 S-блок: из 8 блоков [6] -> 8 блоков [4] по *таблице замен*  
4) рез. [32] на P-блок (перестан)  
5) рез. XOR с Lo[32]  
6) Lo и Ro мен. местами ==след.раунд==>

12) Сколько можно реализовать (теоритически) разновидностей алгоритма 3DES?  
*реализации*:  
\* DES-EEE3: шифруется 3 раза с 3 разными ключами  
\* DES-EDE3: шифр – расш – шифр с 3 разными ключами  
\* DES-EEE2 и DES-EDE2: как пред, но на 1м и 3м шаге один. ключ

13) Какие факторы влияют на стойкость блочного алгоритма шифрования?  
\* рассеивание – скрыв. отношения М и С  
 - если 1 символ в М измен, неск/все символы в С измен  
\* перемешивание – скрыв. отношения между С и ключом

14) В чем состоит сущность дифференциального криптоаанлиза?  
**Дифференциальный:** берет пару шифротекстов, анализирует эволюции разностей (XOR) при прохождении откр. текстом раундов DES при шифровании одним ключом  
Исп. эти разности, присваивает разл. вероятности разл. ключам  
наиб вероятный – верный ключ

15) В чем состоит сущность линейного криптоанализа?  
**Линейный:** найдем «хорошие» однораундовые лин. приближения и объед. их

16) Какие ключевые комбинации относятся к слабым (полуслабым) и почему?  
1) Т.к. ключ измен при получении к. подключа => опред. первонач. ключи **слабые**  
Первонач. знач дел на 2 половины, к. половина сдвигается независимо

Для всех раундов исп. 1 ключ если:  
\* все биты к. половины равны 0 или 1  
\* одна половина сост. из 1, др – 0

2) нек. пары ключей переводят откр. текст в идентичный шифротекст  
т.е. ключ может расшифр сообщ, кот. было зашифровано другим ключом пары => **полуслабые**

17) Где применяются блочные криптоалгоритмы?  
\* алг базир на простых операциях  
\* алг прост для написания кода  
\* устойч к атакам