Оглавление

[Введение 2](#_Toc208426444)

[Компьютерная Криптография 3](#_Toc208426445)

[Многоалфавитная замена 4](#_Toc208426446)

[Научная криптография 5](#_Toc208426447)

[Data Encryption Standard (DES) 6](#_Toc208426448)

Введение

64 часов лекций и практик

Оценивание:

* 30(Кт1) + 30(Кт2) + 40(ДЗ + посещаемость)

Контрольные точки — это проектно-аналитические работы.

Компьютерная Криптография

Криптография - наука о методах преобразования информации с целью ее защиты от несанкционированного доступа

* ﻿﻿Открытый текст (**plaintext** или **cleartext**)
* ﻿﻿Шифрование (**encryption**) - изменение исходного текста для того, чтобы скрыть его содержание
* ﻿﻿Шифротекст (**ciphertext**) - зашифрованное сообщение
* ﻿﻿Дешифрование (**decryption**)
* Ключ (**кеу**) шифрования

Этапы развития:

* ﻿Наивная (до начала XVI в.)
* ﻿﻿Формальная (XVI в. - начало ХХ в.)
* ﻿﻿Научная (30-60 годы XX в.)
* ﻿﻿Компьютерная (с 60 г. ХХ в.)

Шифр цезаря (отставание на 3):

ABCDEFGHIJKI.MNOPORSTUVWXYZ

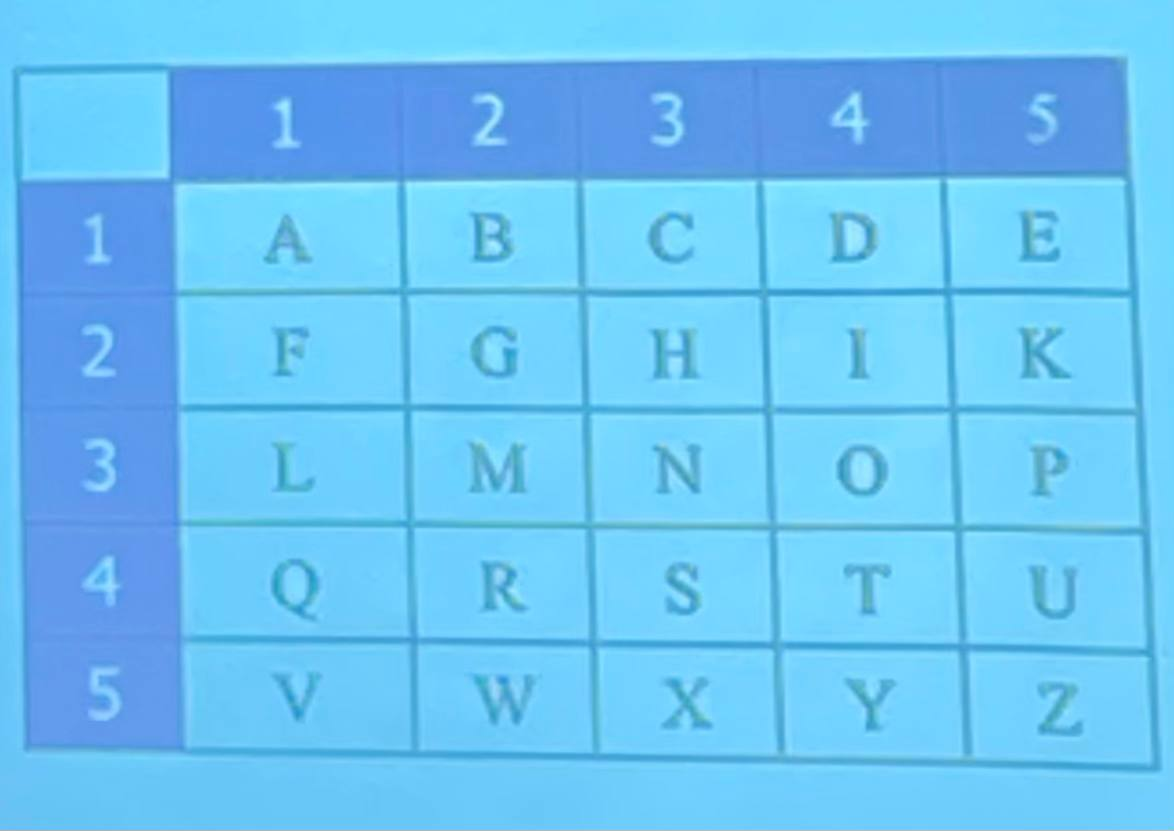
DEFGHIJKLMNOPORSTUVWXYZABC

VENI VIDI VICI

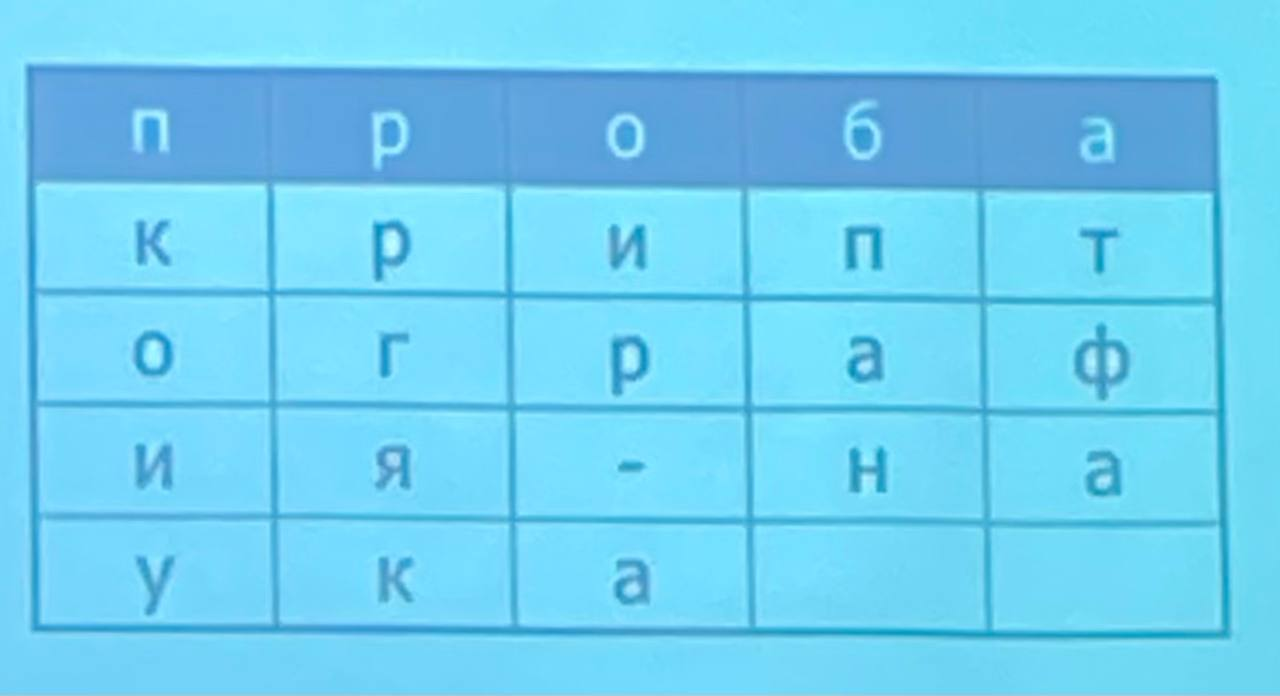
YHQL Y….

ДЗ реализовать

Шифр Полибия:



Шифр перестановки (табличная самая простая):



ДЗ – шифр цезаря и табличная перестановка.

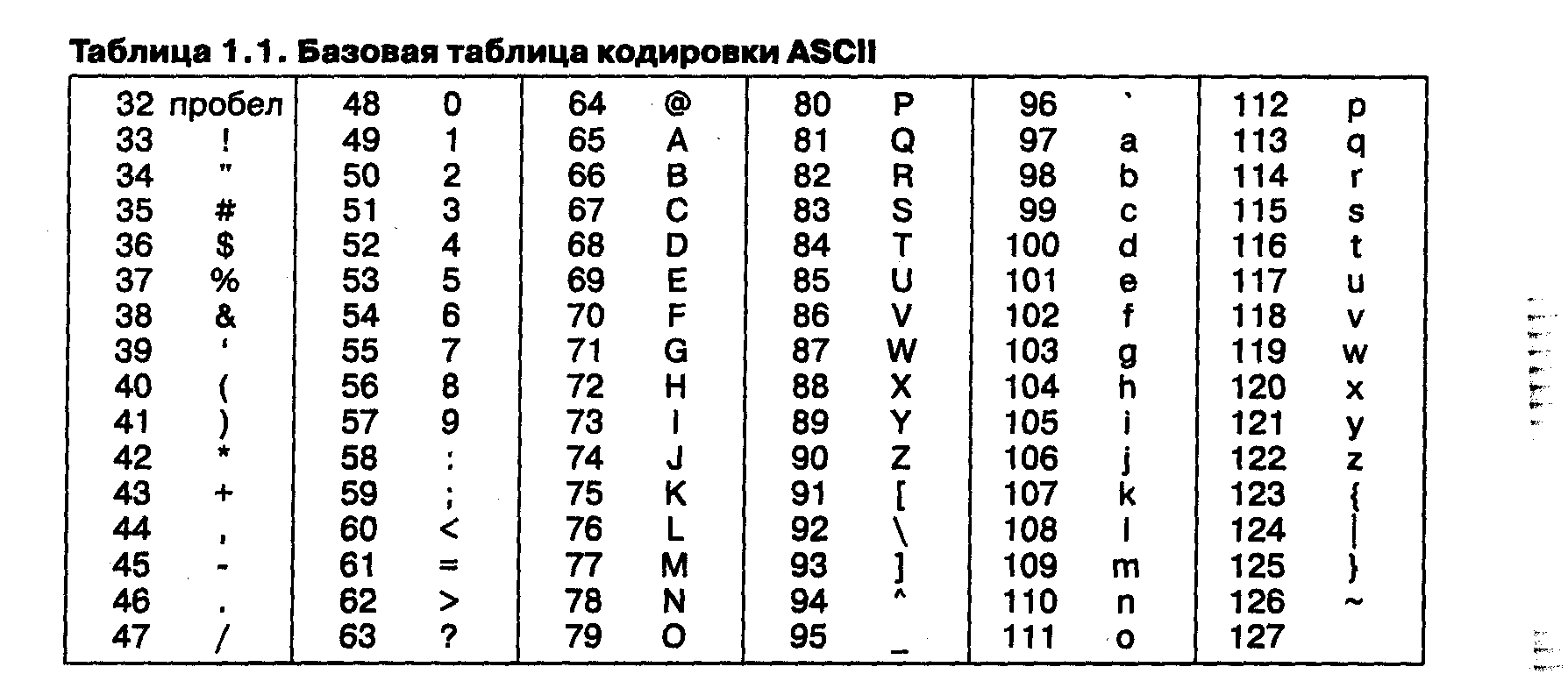
Многоалфавитная замена

Шифр Виженера

– шифр\_буква; – исходное; – номер символа ключа.

Шифр Вернама (одноразовый шифр блокнота)

XOR используется для шифровки.



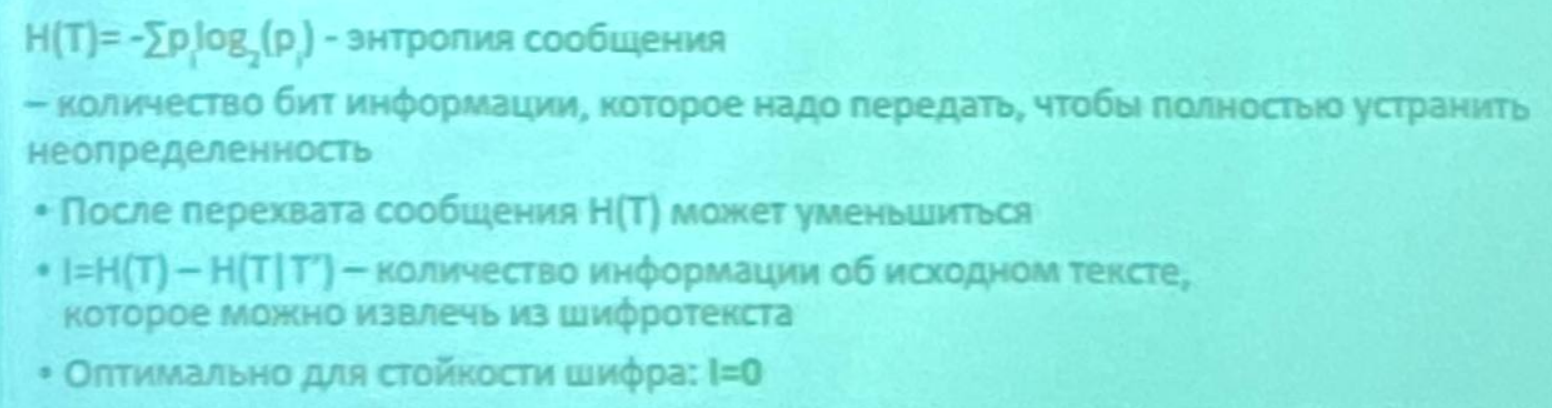
B и D

1000010 – 66  
1000100 – 68 |  
0000110 – 6

Научная криптография

Стойкость шифра – способность шифра противостоять атакам на него.

Мера неопределенности сообщения:



Абсолютная стойкость — это свойство, при котором зашифрованное сообщение не поддается криптоанализу, так как не дает злоумышленнику никакой информации.

**Принципы разработки вычислительно стойких шифров:**

* ﻿Зашифрованное сообщение невозможно расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.
* ﻿﻿Безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма.
* ﻿﻿Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями.
* ﻿﻿Алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение) полученных при шифровании с использованием данного ключа.

Свойства:

* Рассеивание (Диффузия) - распространение влияния одного знака открытого текста на многие символы шифротекста.
* Перемешивание (Конфузия) преобразование, нарушающее взаимосвязи статистических характеристик входного и выходного текста, уничтожение статистической взаимосвязи между зашифрованным текстом и ключом.

Схемы, решающие такие задачи, называют SP-сетями.

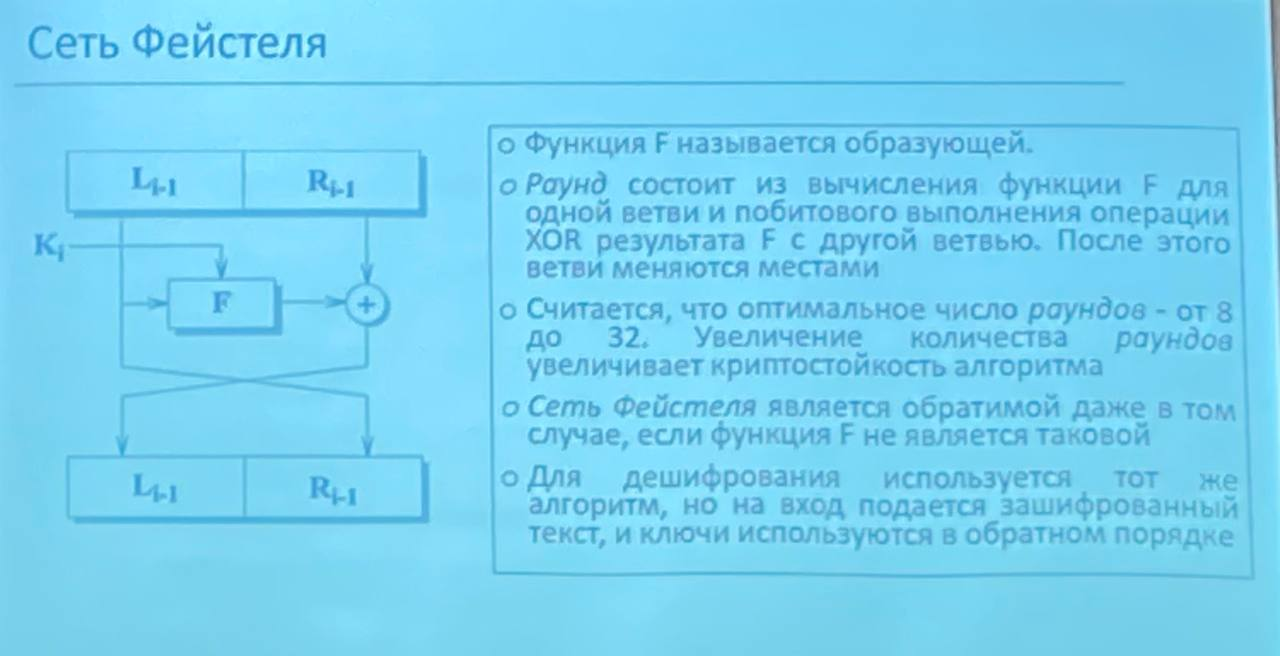
Основные операторы блочных шифров:

* Операторы перестановки, называемые P-боксами
* Операторы подстановки, которые называются S-боксами
* Операция исключающего ИЛИ
* Циклический сдвиг
* Замена
* Разбиение и объединение блоков

Симметричные шифры (блоками/потомками)

* ﻿В процессе шифрования используется определенный алгоритм шифрования, на вход которому подаются исходное незашифрованное сообщение (plaintext), и ключ.
* ﻿﻿Выход алгоритм зашифрованное сообщение, называемое также ciphertext
* ﻿﻿Ключ является значением, не зависящим от шифруемого сообщения.
* ﻿﻿Изменение ключа должно приводить к изменению зашифрованного сообщения

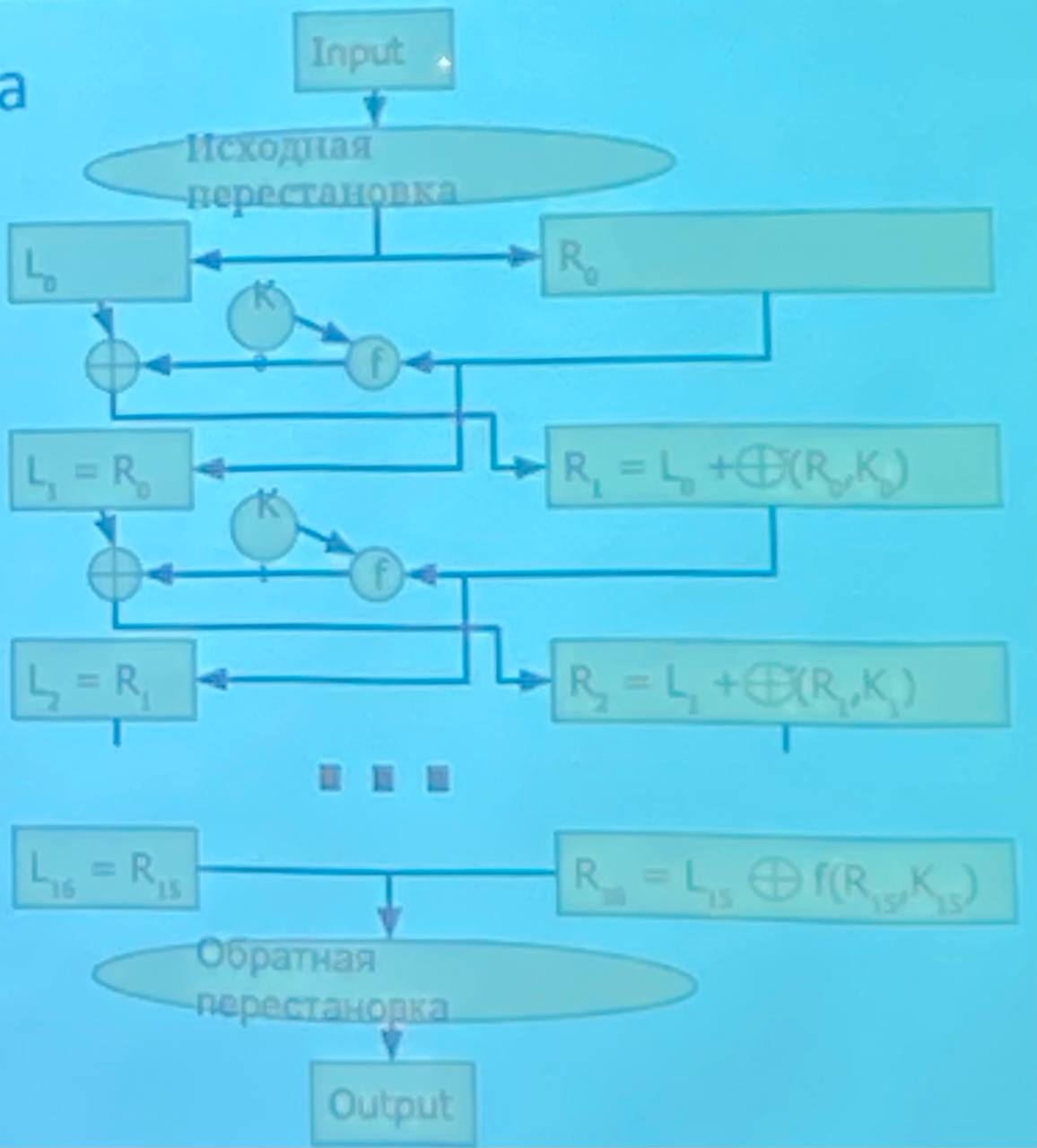
Сеть Фейстеля

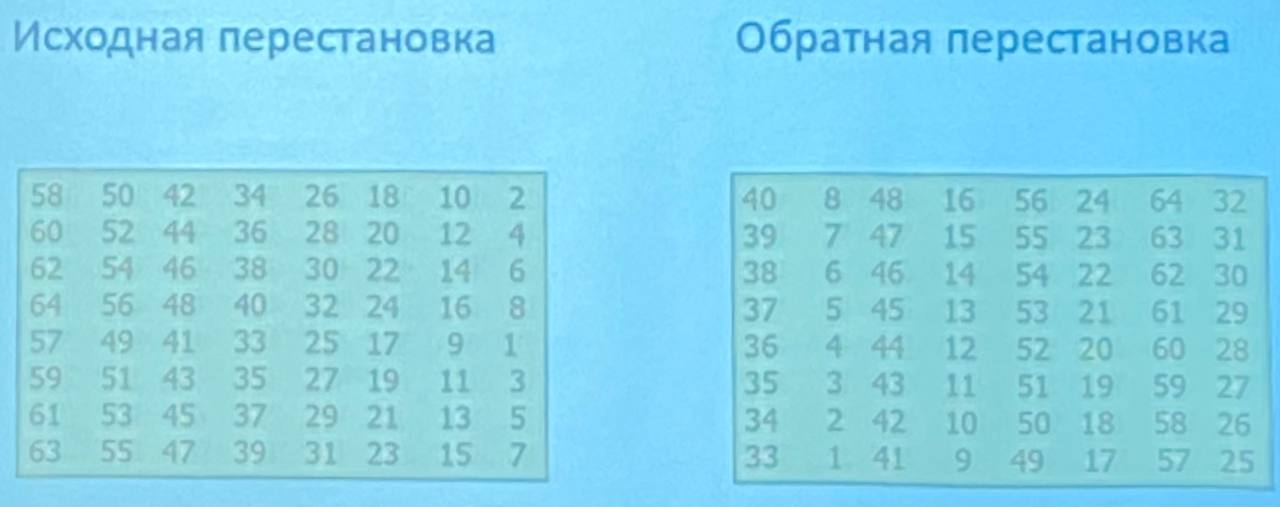


Data Encryption Standard (DES)

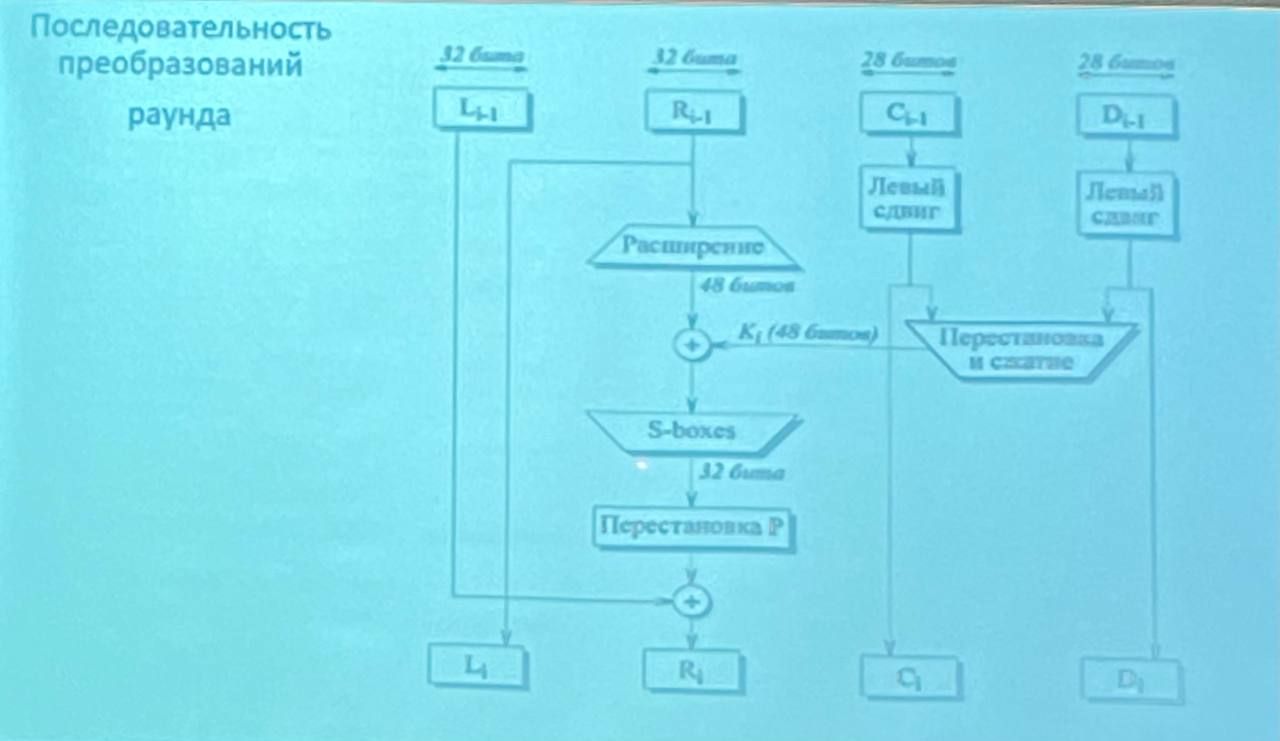
Алгебра, поле, кольцо – сообщение

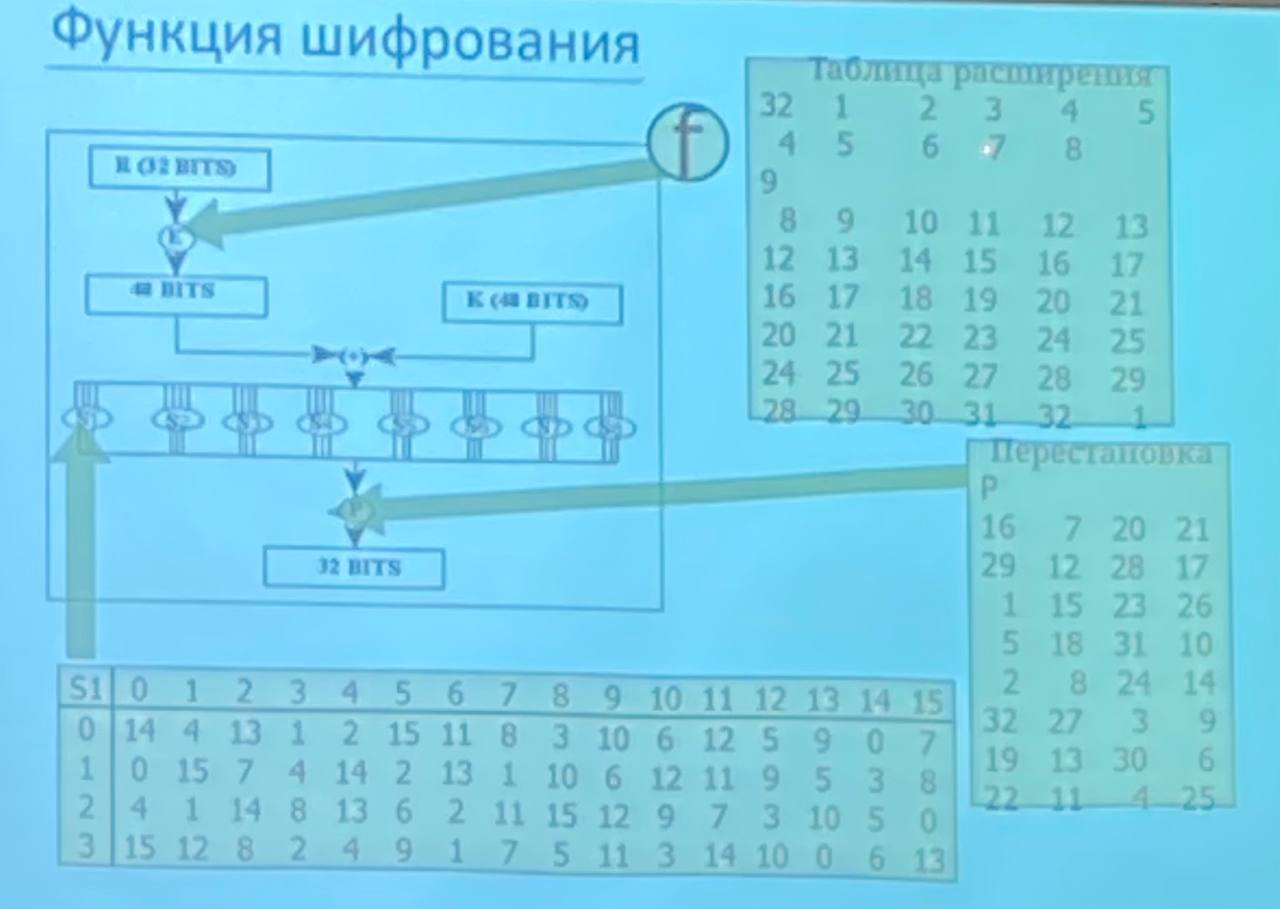
Схема





Сначала все четные, потом нечетные (они перемешаны). Обратная используется в самом конце (столбцы).





Номер строки в S1 = 10(2) = 2(10). Номер столбца S1 = 01110(2) = 6(10) и в табличку 32-х битную смотрим.

Режимы шифрования:

* ECB (Electronic Code Book) - электронная кодовая книга
* ﻿CBC (Cipher Block Chaining) - сцепление блоков по шифротексту
* ﻿CFB (Cipher Feed Back) - обратная загрузка шифротекста
* ﻿OFB (Output Feed Back) - обратная загрузка выходных данных
* ﻿CTR (Counter) - шифрование со счётчиком

Фейстель

* ﻿Входной блок делится на несколько равной длины подблоков, называемых ветвями.
* ﻿﻿Каждая ветвь обрабатывается независимо от другой, после чего осуществляется циклический сдвиг всех ветвей влево.
* ﻿﻿Такое преобразование выполняется несколько циклов или раундов.
* ﻿Функция F называется образующей.
* ﻿﻿Каждый раунд состоит из вычисления функции F для одной ветви и побитового выполнения операции XOR результата F с другой ветвью.
* После этого ветви меняются местами.
* ﻿﻿Считается, что оптимальное число раундов - от 8 до 32. Увеличение количества раундов увеличивает криптостойкость алгоритма.

Алгоритм шифрования ГОСТ 28147-89

\*Куча фото в телефоне\*

﻿Имитовставка - контрольная комбинация, зависящая от открытых данных и секретной ключевой информации.

﻿﻿Цель использования имитовставки - обнаружение всех случайных или преднамеренных изменений в массиве информации.

DZ – реализовать шифр Виженера

Advanced Encryption Standard (AES)

А

Дискретный логарифм:

Количество простых чисел меньших

Простые близнецы – пары простых чисел, отличающихся на 2 (6n +-1, кроме (3,5))

КТ – поле, рса

Эллиптические кривые