Многофункциональный синтез систем передачи данных

Лекция 6
Методы шифрования

каф. СС и ПД,

2016 г.

Основные понятия

Шифрование

Обратимое преобразование информации в целях сокрытия от сторонних (неавторизованных) лиц, с предоставлением, в это же время, авторизованным легитимным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

Криптография

Наука о методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.
Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). *Традиционная криптография* образует раздел *симметричных криптосистем*, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает:

- асимметричные криптосистемы,
- системы электронной цифровой подписи (ЭЦП),
- хеш-функции, управление ключами,
- квантовую криптографию.

Криптографическая система (шифр)

Семейство обратимых преобразований открытого текста в шифрованный. Совокупность (обычно пара) алгоритмов шифрования и дешифрования.

Основные понятия

Открытый (исходный) текст

Данные (не обязательно текстовые), передаваемые без использования криптографии.

Шифротекст

Данные, полученные после применения криптосистемы.

Ключ

Параметр шифра, определяющий выбор конкретного преобразования данного текста. *В современных криптографических стойких шифрах используется открытый ключ* (принцип Керкгоффса).

Шифрование (как процедура)

Процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Асимметричный шифр

Шифр, в котором используются два ключа, шифрующий и дешифрующий.

Основные понятия

Расшифровывание

Процесс нормального применения криптографического преобразования шифрованного текста в открытый.

Дешифрование

Процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин дешифрование обычно применяют по отношению к процессу *криптоанализа* шифротекста.

Криптоанализ

Наука, изучающая математические методы нарушения конфиденциальности и целостности информации. Криптография и криптоанализ составляют *криптологию*, как единую науку о создании и взломе шифров.

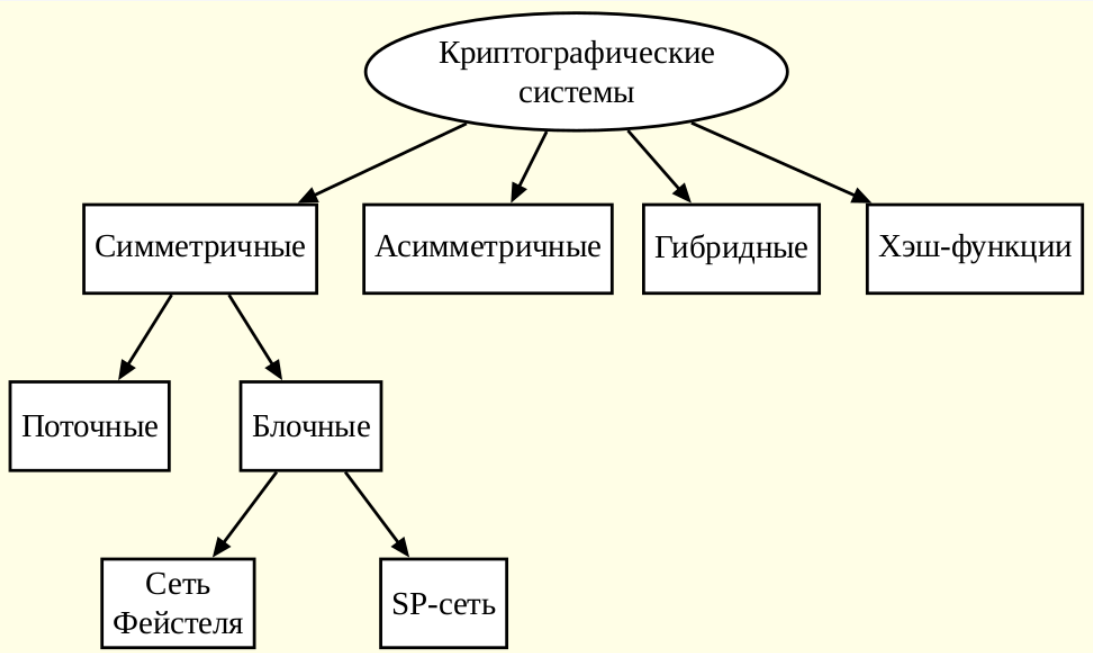
Криптоаналитик

Человек, создающий и применяющий методы криптоанализа.

Криптографическая стойкость

Способность криптографического алгоритма противостоять криптоанализу.

Классификация



Квантовая криптография

Метод защиты коммуникаций, основанный на принципах квантовой физики. Сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма информации всегда выполняется физическими средствами, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. А подслушивание может рассматриваться, как измерение определённых параметров физических объектов–переносчиков информации. А попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика.

Стеганография

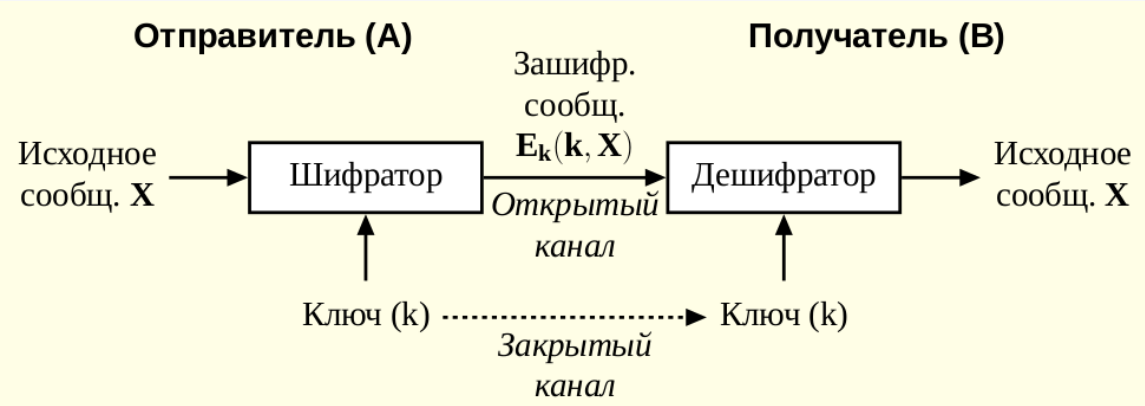
Наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Симметричное шифрование

Симметричное шифрование

Способ шифрования, в котором для шифрования и дешифрования применяется один и тот же криптографический ключ.

Схема



Блочное шифрование

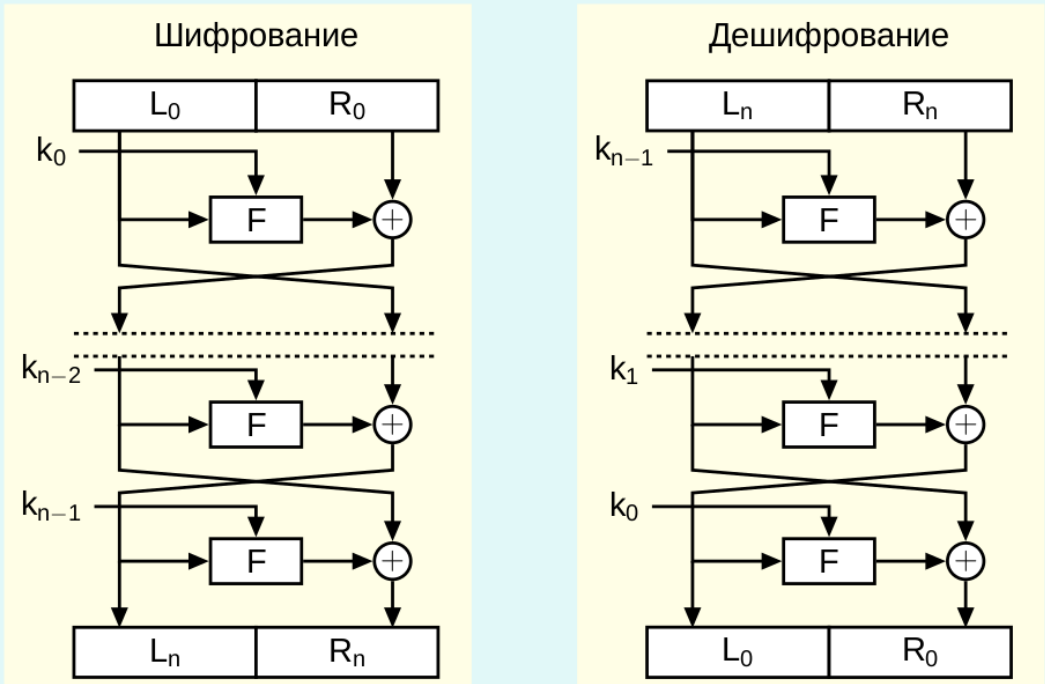
Информация обрабатывается блоками определённой длины. К каждому блоку в установленном порядке в установленном порядке применяется ключ, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является *лавинный эффект* — нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

Блочное шифрование. Сеть Фейстеля

Сеть Фейстеля

Один из методов построения блочных шифров. Сеть представляет собой определённую многократно повторяющуюся (итерированную) структуру, называющуюся ячейкой Фейстеля. При переходе от одной ячейки к другой меняется ключ, причём выбор ключа зависит от конкретного алгоритма. Операции шифрования и расшифрования на каждом этапе очень просты, и при определённой доработке совпадают, требуя только обратного порядка используемых ключей.

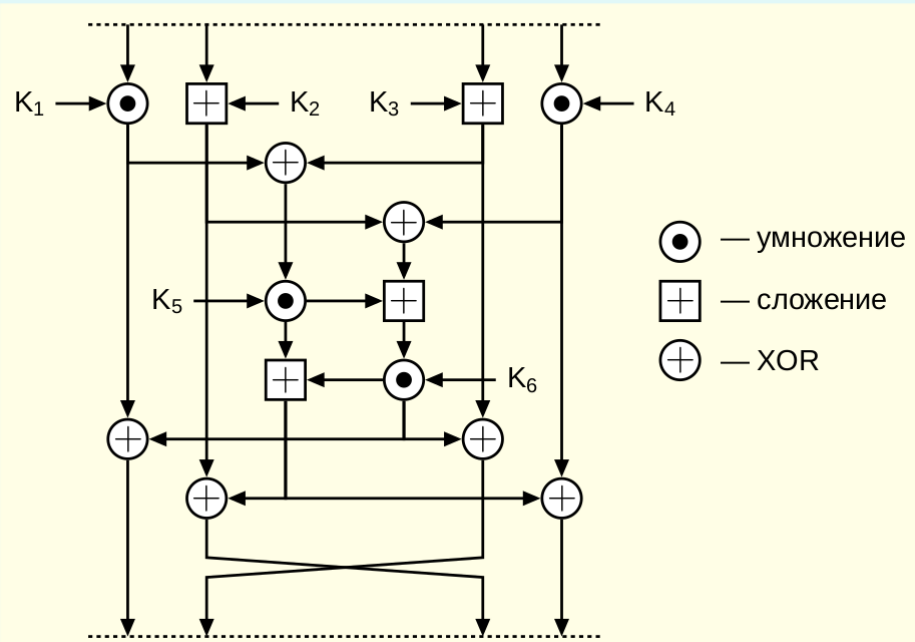
Схема шифрования/дешифрования блочного кода на основе сети Фейстеля



Блочное шифрование. Сеть Фейстеля

При большом размере блоков шифрования (128 бит и более) обычно применяются модифицированные варианты этой конструкции. Обычно используются сети с 4 ветвями. Также существуют схемы, в которых длины половинок L_0 и R_0 не совпадают. Они называются *несбалансированными*.
Примером алгоритма, использующим глубоко модифицированную сеть Фейстеля, является алгоритм IDEA. В нём 64-х битные входные блоки данных делятся на 4 подблока длиной 16 бит. На каждом этапе используется 6 16-ти битных ключей. Всего используется 8 основных этапов и 1 укороченный.

Схема одной итерации полного раунда алгоритма IDEA



Примеры алгоритмов

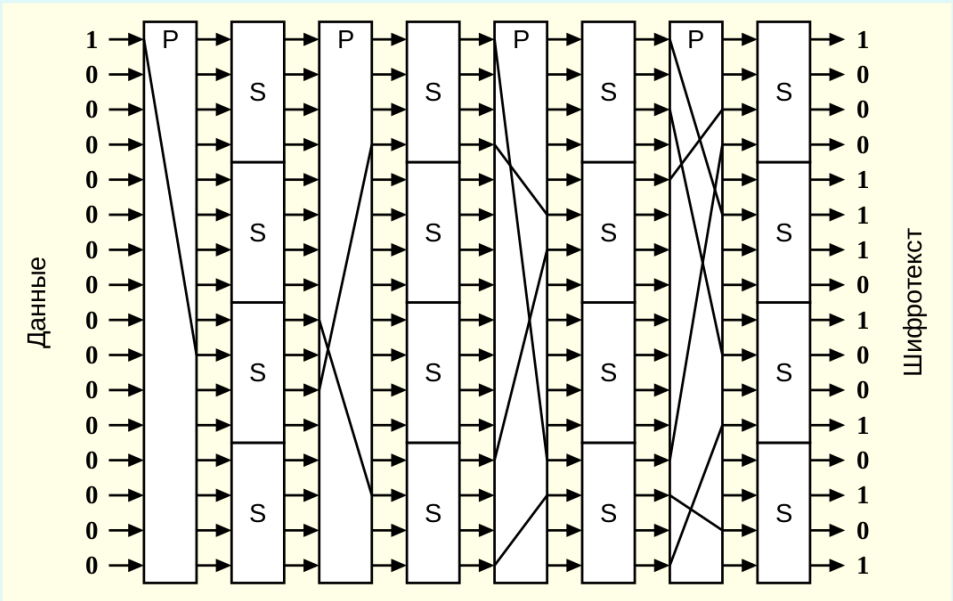
- DES
- Triple DES
- ГОСТ 28147-89
- Blowfish
- Camellia
- SEED
- CAST-128
- KASUMI
- IDEA

Блочное шифрование. SP-сеть

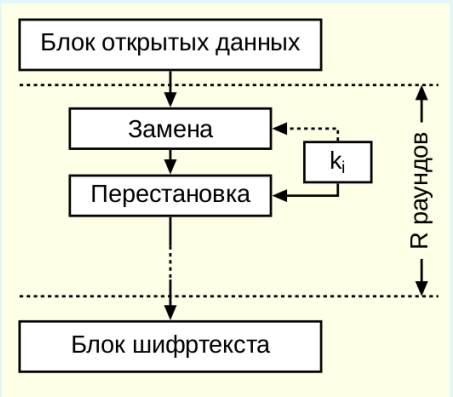
SP-сеть (Substitution-Permutation network, подстановочно-перестановочная сеть)

Разновидность блочного шифра, предложенная в 1971 году Хорстом Фейстелем. В простейшем варианте представляет собой «сэндвич» из слоёв двух типов, используемых многократно по очереди. Первый тип слоя — P-слой, состоящий из P-блока большой разрядности, за ним идёт второй тип слоя — S-слой, представляющий собой большое количество S-блоков малой разрядности, потом опять P-слой и т. д. В современных алгоритмах вместо S- и P-блоков используются различные математические или логические функции.
При этом за один раунд обрабатывается целиком шифруемый блок. Обработка данных сводится, в основном, к заменам (когда, например, фрагмент входного значения заменяется другим фрагментом в соответствии с таблицей замен, которая может зависеть от значения ключа K_i) и перестановкам, зависящим от ключа K_i.

Упрощённая схема работы S- и P-слоёв в ранней версии алгоритма Lucifer



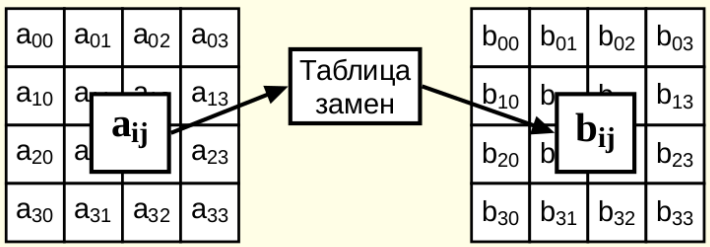
Упрощённая схема работы SP-сети в современных алгоритмах



Блочное шифрование. SP-сеть

Иногда из семейства алгоритмов на основе SP-сети выделяют алгоритмы со структурой «квадрат» (Square). Для структуры «квадрат» характерно представление шифруемого блока данных в виде двумерного байтового массива. Криптографические преобразования могут выполняться над отдельными байтами массива, а также над его строками или столбцами.
В качестве примера такого алгоритма шифрования можно привести алгоритм AES (Rijndael)

Пример операции над блоком данных в алгоритме AES.
a_{00} *— 1-й байт входящих данных,* a_{01} *— 2-й байт* и т. д.



Примеры алгоритмов

- 3-Way
- ABC
- AES (Rijndael)
- Anubis
- ARIA
- Diamond2
- KHAZAD
- Lucifer (1971 год)
- Rainbow
- SAFER
- SHARK
- Serpent

Поточное шифрование

Поточный шифр

Симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста.

Синхронные поточные шифры

Шифры, в которых поток ключей генерируется независимо от открытого текста и шифротекста.
Плюсы СПШ:

- отсутствие эффекта распространения ошибок (только искажённый бит будет расшифрован неверно);
- предохраняют от любых вставок и удалений шифротекста, так как они приведут к потере синхронизации и будут обнаружены.

Минусы СПШ:

- уязвимы к изменению отдельных бит шифрованного текста. Если злоумышленнику известен открытый текст, он может изменить эти биты
- так, чтобы они расшифровывались, как ему надо.

Асинхронные (самосинхронизирующиеся) поточные шифры

Шифры, в которых поток ключей создаётся функцией ключа и фиксированного числа знаков шифротекста.
Плюсы АПШ:
Размешивание статистики открытого текста. Так как каждый знак открытого текста влияет на следующий шифротекст, статистические свойства открытого текста распространяются на весь шифротекст. Следовательно, АПШ может быть более устойчивым к атакам на основе избыточности открытого текста, чем СПШ.
Минусы АПШ:

- распространение ошибки (каждому неправильному биту шифротекста соответствуют N ошибок в открытом тексте);
- чувствительны к вскрытию повторной передачей.