СЕТИ. КРИПТОГРАФИЯ

Урок 5. Симметричное шифрование

Шифрование

Шифрова́ние — обратимое преобразование информации в целях сокрытия от неавторизованных лиц…

… с предоставлением, в это же время, **авторизованным** пользователям доступа к ней.

Авторизация

- **Авториза́ция** — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

- **Аутентифика́ция** — процедура проверки подлинности данных, например:
  - проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;
  - подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
  - проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Шифрование

С помощью шифрования обеспечиваются три состояния безопасности информации:

- Конфиденциальность.
  - Шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.
- Целостность.
  - Шифрование используется для предотвращения изменения информации при передаче или хранении.
- Идентифицируемость.
  - Шифрование используется для аутентификации источника информации и **предотвращения отказа отправителя** информации от того факта, что данные были отправлены именно им.

***шифрование

- Шифрование – закрытие информации
- Расшифрование – открытие информации авторизованным лицом
- Дешифрование – открытие информации **НЕ**авторизованным лицом

Разновидности

- Блочные шифры.
  - Обрабатывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами.

- Поточные шифры
  - В которых шифрование проводится над каждым битом либо байтом исходного текста с использованием гаммирования.

Разновидности

- Открытый/Закрытый ?

Принцип Шенонна: Враг знает систему

С.Ш. и А.Ш.

- Симметричное
  - Простое
  - Быстрое
  - Эффективное
- Ассиметричное
  - Архисложное
  - Долгое
  - Мистическое

С.Ш. = Кодирование+Ключ

- Место для рисунка:

Основные требования

- Функционал:
  - Однозначность результата шифрования
  - Ключ, как элемент алгоритма шифрования
- Качество
  - Сильная зависимость результата от входных данных
  - Непредсказуемость результата
  - Длина ключа равна длине сообщения
- Стойкость
  - Необратимость без ключа
  - Стойкость к коллизиям первого рода: невозможно подобрать сообщение или пароль под известный результат
  - Стойкость к коллизиям второго рода: невозможно подобрать пару сообщений или паролей с одинаковым результатом
  - Стойкость алгоритма тождественна секретности ключа

Полная схема симметричного шифрования

- Место для рисунка:

Мировые стандарты

Блочные шифрыAES (англ. Advanced Encryption Standard) - американский стандарт шифрования

- ГОСТ 28147-89 советский и российский стандарт шифрования, также является стандартом СНГ
- DES/AES (англ. Data Encryption Standard) - стандарт шифрования данных в США
- 3DES (Triple-DES, тройной DES)
- RC2 (Шифр Ривеста (Rivest Cipher или Ron's Cipher))
- RC5
- Blowfish
- Twofish
- NUSH
- IDEA (International Data Encryption Algorithm, международный алгоритм шифрования данных)
- CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares)
- CRAB
- 3-WAY
- Khufu и Khafre
- Kuznechik

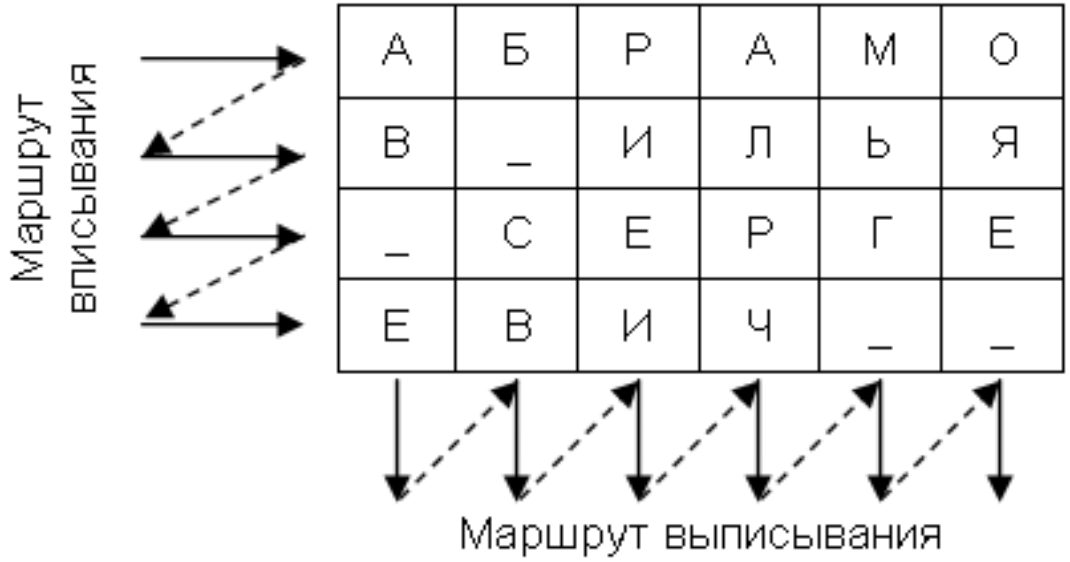
Потоковые шифры

- RC4 (алгоритм шифрования с ключом переменной длины)
- SEAL (Software Efficient Algorithm, программно-эффективный алгоритм)
- WAKE (World Auto Key Encryption algorithm, всемирный алгоритм шифрования на автоматическом ключе)

ПРАКТИЧЕСКИЙ БЛОК

Табличная перестановка.

Табличная перестановка



Табличная перестановка

Ключ →

П	Е	Л	И	К	А	Н
7	2	5	3	4	1	6
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

До перестановки

А	Е	И	К	Л	Н	П
1	2	3	4	5	6	7
Г	Н	В	Е	П	Л	Т
О	А	А	Д	Р	Н	Е
В	Т	Е	Ь	И	О	Р
П	О	Т	М	Б	Ч	М
О	Р	С	О	Ы	Ь	И

После перестановки

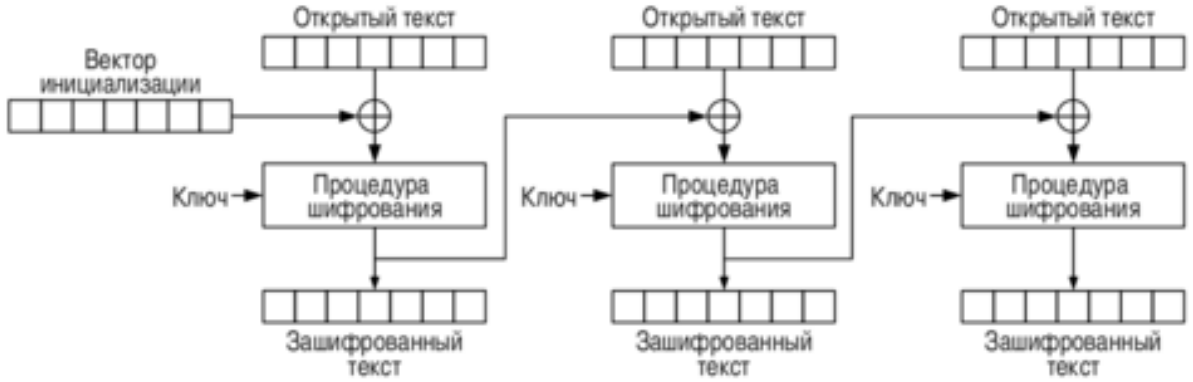
Задачи

- Задачи!! …. Вас ждут задачи!!!

Ключ **vs** Шифр-последовательность

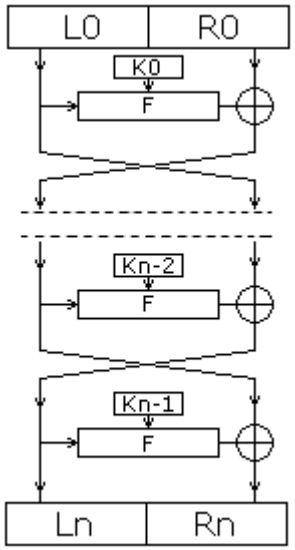
- **Хеш-сумма** – математическая функция от входной строки (пароля)
  - **CRC32**: F6DE2FEA
  - **MD5**: *026f8e459c8f89ef75fa7a78265a0025*
  - **SHA-1**: 7DD987F846400079F4B03C058365A4869047B4A0

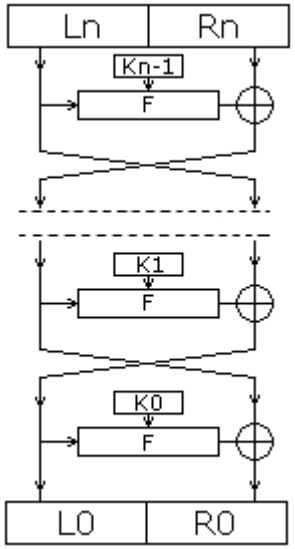
- Каскадное применение ключа в блочных алгоритмах:



Сеть Фейстеля

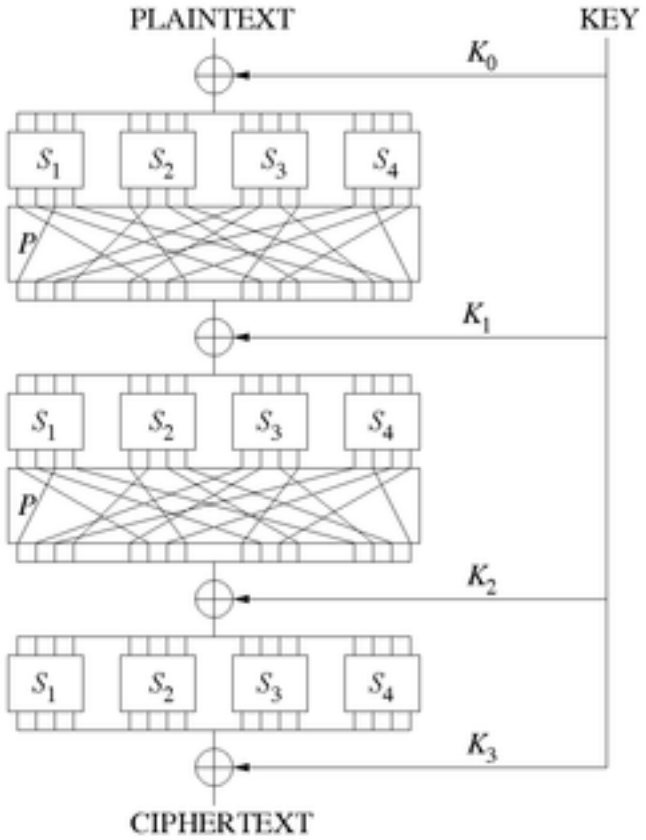
- Один из методов построения блочных шифров. Сеть состоит из ячеек, называемых ячейками Фейстеля.
- На вход каждой ячейки поступают данные и ключ.
- На выходе каждой ячейки получают изменённые данные и изменённый ключ.
- Все ячейки однотипны
- Ключ выбирается в зависимости от алгоритма шифрования/расшифрования и меняется при переходе от одной ячейки к другой.
- При шифровании и расшифровании выполняются одни и те же операции; отличается только порядок ключей.
- Ввиду простоты операций сеть Фейстеля легко реализовать как программно, так и аппаратно. Большинство современных блочных шифров (DES, RC2, RC5, RC6, Blowfish, FEAL, CAST-128, TEA, XTEA, XXTEA и др.) используют сеть Фейстеля в качестве основы.





Подстановочно-перестановочная сеть

- Шифр на основе SP-сети получает на вход блок и ключ и совершает несколько чередующихся раундов, состоящих из чередующихся стадий подстановки (англ. substitution stage) и стадий перестановки (англ. permutation stage).
  - Для достижения безопасности достаточно одного S-блока, но такой блок будет требовать большого объёма памяти. Поэтому используются маленькие S-блоки, смешанные с P-блоками.
  - Нелинейная стадия подстановки перемешивает биты ключа с битами открытого текста, создавая конфузию Шеннона.
  - Линейная стадия перестановки распределяет избыточность по всей структуре данных, порождая диффузию.
- S-блок (англ. substitution box or S-box) замещает маленький блок входных бит на другой блок выходных бит.
  - Эта замена должна быть взаимно однозначной, чтобы гарантировать обратимость.
  - Назначение S-блока заключается в нелинейном преобразовании, что препятствует проведению линейного криптоанализа.
  - Одним из свойств S-блока является лавинный эффект, т.е. изменение одного бита на входе приводит к изменению всех бит на выходе.
- P-блок (англ. permutation box or P-box) — перестановка всех бит: блок получает на вход вывод S-блока, меняет местами все биты и подает результат S-блоку следующего раунда.
  - Важным качеством P-блока является возможность распределить вывод одного S-блока между входами как можно больших S-блоков.
- Для каждого раунда используется свой, получаемый из первоначального, ключ. Подобный ключ называется раундовым. Он может быть получен как делением первоначально ключа на равные части, так и каким-либо преобразование всего ключа.



Демонстрация

- Демонстрация **AES**

- Демонстрация **ГОСТ 28147-89**

Использование физических принципов:

- Демонстрация клеточных автоматов **Фредкина**