Курс: **эксплуатация подсистем безопасности АС**

Тема: **Криптографическое преобразование информации в АС**

Преподаватель: Пятков Антон Геннадьевич

Красноярск

Определения

Шифрование – преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре.

Дешифрование – преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Криптография (наука о шифровании) – раздел прикладной математики, в котором изучаются модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения, видоизменения или несанкционированного использования.

Криптосистема – система, реализованная программно, аппаратно или программно-аппаратно и осуществляющая криптографическое преобразование информации.

Криптоанализ (наука о дешифрации) – раздел прикладной математики, в котором изучаются модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или ее входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст.

Определения

Криптология – совокупность криптографии и криптоанализа.

Криптограмма – шифрованный текст (ШТ).

Текст – набор элементов алфавита имеющий определенный логический смысл.

Открытый текст (ОТ) – исходное, шифруемое сообщение.

Алфавит – конечное множество используемых для шифрования знаков.

Ключ – информация, необходимая для беспрепятственного шифрования или расшифрования текстов (обычно последовательность символов).

Криптостойкость – характеристика шифра, определяющая его стойкость к дешифрации. Часто измеряется количеством операций, необходимых для перебора всех возможных ключей, или интервалом времени, необходимого для дешифрования.

(получение ШТ) Шифрование ≠Кодирование (преобразование в другой код)

Основная идея шифрования – скрытие смысла передаваемого сообщения.

Выделяют два класса криптосистем:

- ✔ симметричные (одноключевые) криптосистемы;
- ✔ асимметричные (двухключевые) криптосистемы.

Виды шифров

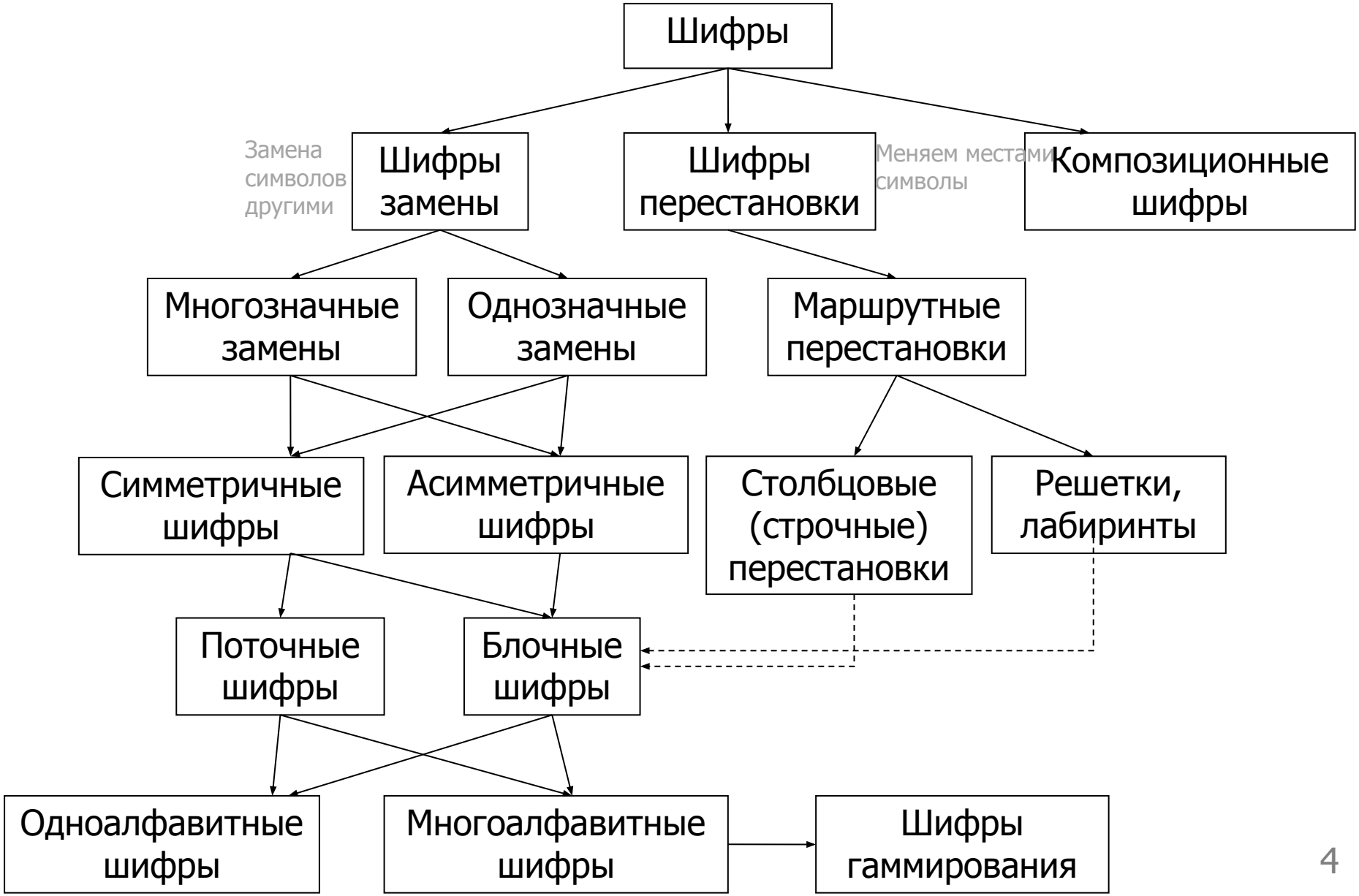

Шифры
Замена символов другими
Шифры замены
Шифры перестановки
Меняем местами символы
Композиционные шифры
Многозначные замены
Однозначные замены
Маршрутные перестановки
Симметричные шифры
Асимметричные шифры
Столбцовые (строчные) перестановки
Решетки, лабиринты
Поточные шифры
Блочные шифры
Одноалфавитные шифры
Многоалфавитные шифры
Шифры гаммирования

Схема передачи ШТ

Традиционная задача криптографии - проблема обеспечения конфиденциальности при передаче сообщений по контролируемому противником каналу связи.
В простейшем случае это взаимодействие 3 субъектов (сторон): отправитель, получатель и противник.

$E_{k1}(X)=Y$ – шифрование, X – сообщение, ОТ, k1 – ключ Ш.

$D_{k2}(Y)=X$ – дешифрование, Y – криптограмма, ШТ, k2 – ключ Расш.

Причём: $D_{k2}(E_{k1}(X))=X$ – принцип обратимости крипто-функции

Принцип симметричного шифрования

Принцип асимметричного шифрования

Гаммирование

Гаммирование – процесс наложения по определенному закону гаммы шифра на ОТ.

Гамма шифра – псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования ОТ и расшифрования ШТ.

Шифрование:

ОТ: 0 0 0 1 1 0 0 1 1 1

xor

Гамма: 0 1 0 1 0 1 0 1 0 1

ШТ: 0 1 0 0 1 1 0 0 1 0

Дешифрование

ШТ: 0 1 0 0 1 1 0 0 1 0

xor

Гамма: 0 1 0 1 0 1 0 1 0 1

ОТ: 0 0 0 1 1 0 0 1 1 1

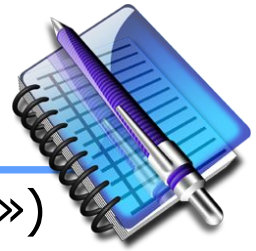
Гаммирование – блочный шифр

Основные типы атак на блочные шифры

- ✔ атака с использованием только ШТ;
- ✔ атака с известным парами ОТ и ШТ, цель атаки - найти ключ;
- ✔ атака с избранным ОТ – криптоаналитик самостоятельно подбирает ОТ;
- ✔ атака с избранным ШТ – криптоаналитик подбирает пары (ОТ, ШТ);
- ✔ атаки, в основе которых лежит парадокс задачи о днях рождения (birthday attack). Суть парадокса: если в комнате находятся 23 человека, то вероятность что 2 из них родились в 1 день, превышает 50%. Одинаковые значения появляются быстрее, чем можно было ожидать;
- ✔ двусторонняя атака (атака «встреча на середине», meet-in-the-middle attack) – криптоаналитик строит таблицу ключей, которые выбрал самостоятельно. При birthday attack криптоаналитик ждет, когда одно и то же значение появится дважды во множестве элементов, в двусторонней

два множества пересекутся.

Абсолютно стойкие шифры



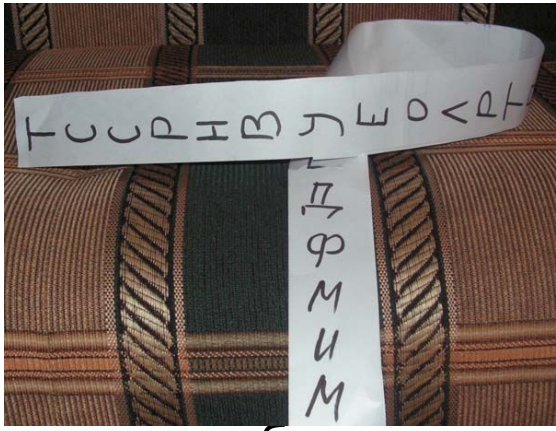
Пример (единственный) - «Одноразовый блокнот» («шифр Вернама»)

1) ОТ преобразуется в битовую последовательность;

2) Генерируется случайная битовая последовательность, длина которой равна длине сообщения (ключ).Передается всем участникам обмена.

3) Зашифрование происходит путем побитового сложения текста с ключом по модулю 2 (XOR). Расшифрование аналогично.

Для абсолютной стойкости обязательны требования к ленте однократного использования:



1) полная случайность (равновероятность) ключа;

2) равенство длины ключа и длины открытого текста;

3) однократность использования ключа.

Остальные шифры могут быть достаточно стойкими.

Отличие от гаммирования:

1. В гаммировании не используется никаких шифроблокнотов, требуется только знание параметров ГПСЧ (генератор псевдослучайных чисел).

2. Гаммирование является блочным шифром. Шифр Вернама блочным не является. Он относится к поточным шифрам.

Разрешено или запрещено?

В РФ коммерческая деятельность, связанная с использованием криптографических средств, подлежит обязательному (!) лицензированию.

Постановление Правительства РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании деятельности … шифровальных (криптографических) средств...»

Подлежит лицензированию деятельность по:

- разработке шифровальных (криптографических) средств (КСЗИ);
- производству, распространению КСЗИ;
- техническому обслуживанию, ремонту, установке КСЗИ;
- предоставлению услуг в области шифрования информации;
- передаче средств изготовления ключевых документов;
- изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов.

Для защиты ГТ и официальной защиты КТ разрешено использовать только отечественный стандарт шифрования ГОСТ 28147-89.

Для личных целей – свобода выбора алгоритмов шифрования.

Регулятор в области криптографии в РФ – ФСБ.