Тема: Основные понятия криптографии

Учебные вопросы:

1. Основные термины криптологии.

2. Требования к криптографическим системам

3. Составляющие криптостойкости (по Шеннону)

4.Общая структура криптосистемы

5. Классификация алгоритмов шифрования

6. Классы симметричных криптосистем

КРИПТОЛОГИЯ

наука о защите информации, путем ее преобразования.

Объединяет два направления – криптографию и криптоанализ.

Криптография занимается поиском и исследованием методов преобразования информации с целью скрытия ее содержания.

Криптоанализ - исследование возможности расшифровывания информации без знания ключей.

Основные направления использования криптографических методов

– передача конфиденциальной информации по каналам связи;

–установление подлинности передаваемых сообщений;

–хранение информации на носителях в зашифрованном виде.

Алфавит

конечное множество используемых для кодирования информации знаков.

В качестве алфавита могут выступать как множество символов национальных алфавитов, так и множество различных символов и цифр

Текст

упорядоченный набор из элементов алфавита

Шифрование - **процесс преобразования исходного текста в шифрованный текст.**

Расшифрование - **процесс, обратный шифрованию. На основе ключа шифрованный текст преобразуется в исходный**

Ключ

это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма. Обычно ключ представляет собой последовательный ряд символов алфавита.

Пространство ключей K

набор возможных значений ключа.

Требования к криптографическим системам:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

- число операции, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

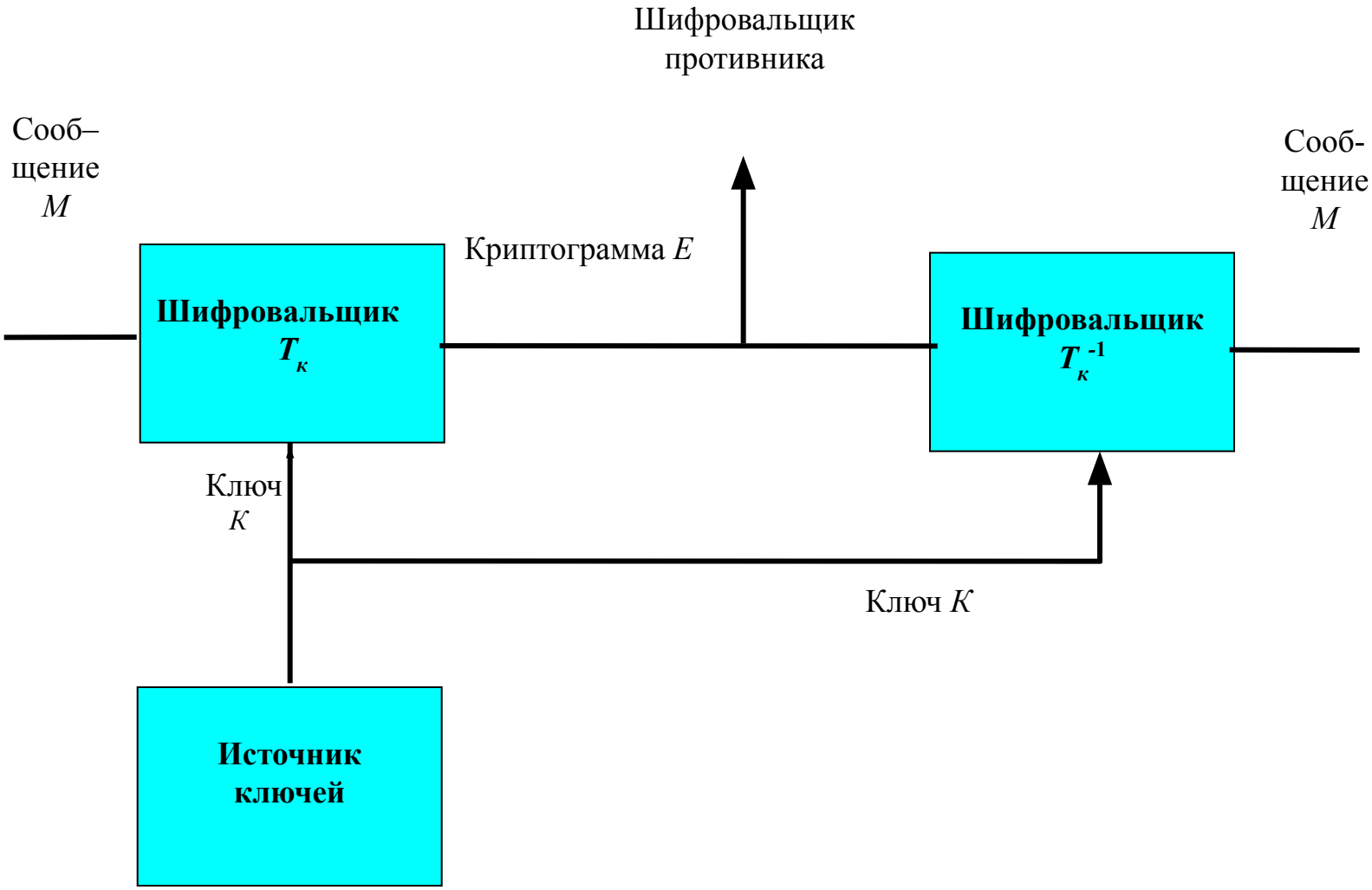
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений) или требовать неприемлемо высоких затрат на эти вычисления;

- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при шифровании одного и того же исходного текста;

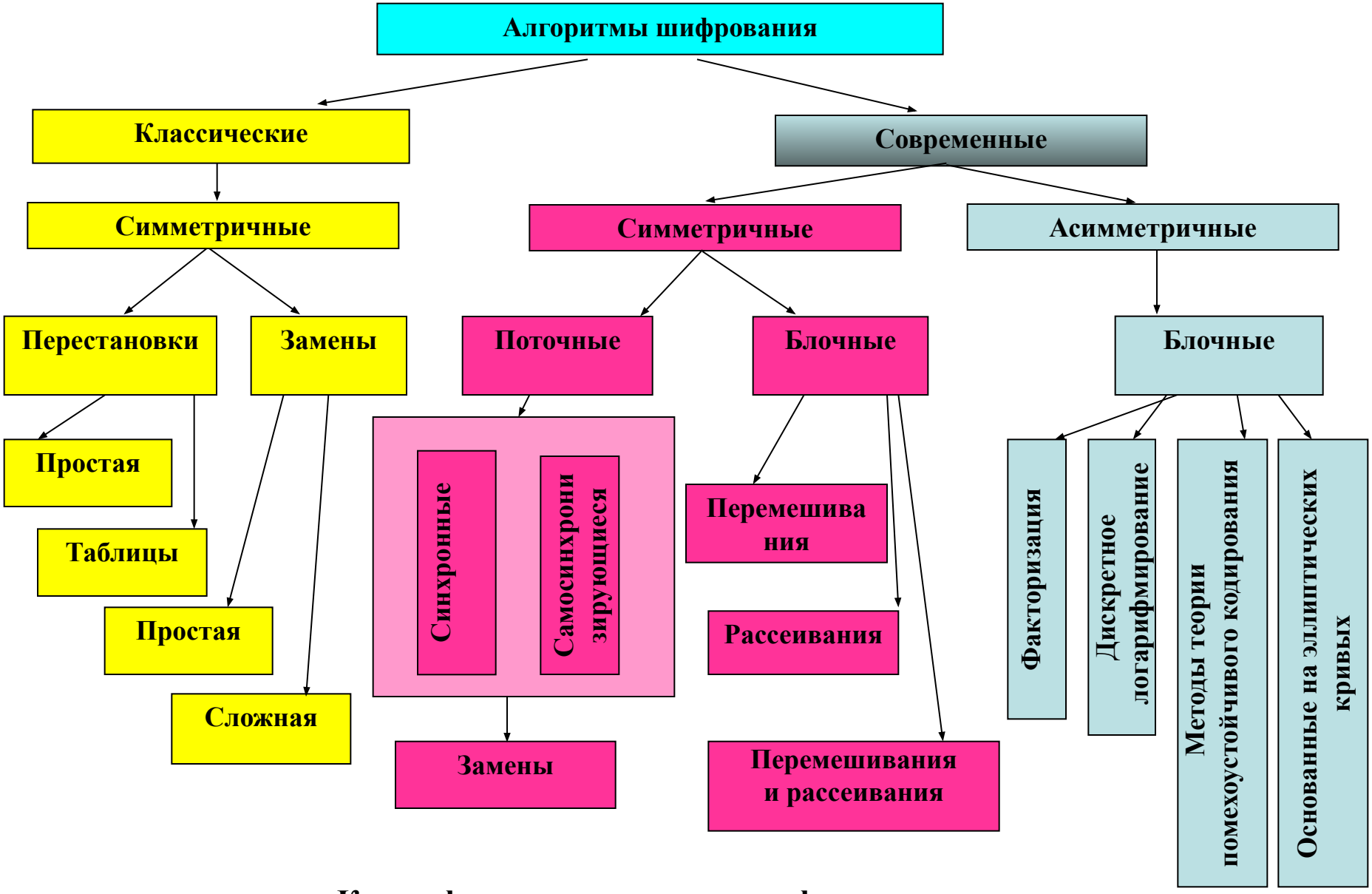
- незначительное изменение исходного текста должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- знание алгоритма шифрования не должно влиять на надежность защиты;
- структурные элементы алгоритма шифрования должны быть неизменными;
- длина шифрованного текста не должна превосходить длину исходного текста;

- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;

- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.



Общая структура криптосистемы



Классификация алгоритмов шифрования

К.ШЕННОН

- «проблема создания хорошего шифра является по существу проблемой нахождения наиболее сложных задач, удовлетворяющих определенным условиям... Можно составить шифр таким образом, чтобы его раскрытие было эквивалентно (или включало в себя) решению некоторой проблемы, про которую известно, что для ее решения требуется большой объем работ».

- В своей работе К.Шеннон выделил два наиболее общих принципа построения шифров. Это **рассеивание и перемешивание.**
- Рассеивание – распространение влияния одного знака открытого текста на много знаков шифртекста. Это позволяет скрыть статистические характеристики исходного текста.
- Перемешивание – использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов.

Составляющие криптостойкости (по Шеннону)

1. Количество секретности.
2. Объем ключа.
3. Сложность операции шифрования и дешифрирования.
4. Разрастание числа ошибок.
5. Увеличение объема сообщения.

Количество секретности.

Некоторые секретные системы являются совершенными в том смысле, что положение противника не облегчается в результате перехвата любого количества сообщений.

Другие системы, хотя и дают противнику некоторую информацию при перехвате очередной криптограммы, но не допускают единственного «решения».

Системы, допускающие единственное решение, очень разнообразны как по затрате времени и сил, необходимых для получения этого решения, так и по количеству материала, который необходимо перехватить для получения единственного решения.

Объем ключа.

Ключ должен быть передан из передающего пункта в приемный пункт таким способом, чтобы его нельзя было перехватить. Иногда его нужно запомнить.

Поэтому желательно иметь ключ настолько малый, насколько это возможно

Сложность операции шифрования и дешифрирования

Операции шифрования и дешифрирования должны быть простыми.

Если эти операции производятся вручную, то их сложность приводит к потере времени, появлению ошибок и т. д.

Если они производятся механически, то сложность приводит к использованию больших и дорогих устройств.

Разрастание числа ошибок

В некоторых типах шифров ошибка в одной букве, допущенная при шифровании или передаче, приводит к большому числу ошибок в расшифрованном тексте.

Такие ошибки разрастаются в результате операции дешифрирования, вызывая значительную потерю информации и часто требуя повторной передачи криптограммы.

Естественно, желательно минимизировать это возрастание числа ошибок.

Увеличение объема сообщения

В некоторых типах секретных систем объем сообщения увеличивается в результате операции шифрования.

Этот нежелательный эффект можно наблюдать в системах, в которых делается попытка потопить статистику сообщения в массе добавляемых нулевых символов, или где используются многократные замены.

Оценка эффективности

- **Время, необходимое для реализации успешной криптоатаки.**
- **Количество операций, необходимых для реализации успешной криптоатаки.**

(MIPS – количество операций, которое произведет ЭВМ за год с производительностью 1 млн. операций в секунду)

Классы симметричных криптосистем

- шифры перестановки;
- шифры простой замены;
- шифры сложной замены;
- шифры с использованием гаммирования;
- блочные шифры;
- поточные шифры.

Шифры перестановки

Шифры перестановки являются самыми простыми и, вероятно, самыми древними шифрами. В настоящее время подобными шифрами в чистом виде не пользуются, так как их криптостойкость мала.

С к и т а л а
6 1 3 5 7 2 4
к л и а т с а

- Количество вариантов написания слова, зашифрованного таким образом, можно оценить как

N*(N-1)

Шифрующие таблицы

В качестве ключа в шифрующих таблицах используются:

- размер таблицы;

- слово, фраза или числовая последовательность, определяющие перестановку;

- особенности структуры таблицы.

КРИПТОЛОГИЯ ЭТО КРИПТОГРАФИЯ И КРИПТОАНАЛИЗ

К	О	Я	Р	Г	Я	П	А
Р	Л	Э	И	Р	И	Т	Л
И	О	Т	П	А	К	О	И
П	Г	О	Т	Ф	Р	А	З
Т	И	К	О	И	И	Н	

КОЯРГ ЯПАРЛ ЭИРИТ ЛИОТП АКОИП ГОТФР АЗТИК ОИИН

Количество вариантов шифртекста при таком способе можно определить как

$$Q = (\mathrm{div}(N/P))!,$$

где N – количество символов в сообщении;

P – количество строк в таблице

	1	2	3	4	5	6	7	8								
3	Г	Я	А	К	Р	П	О	Я	Р	Э	Л	Р	И	Т	Л	И
1	Р	Э	Л	Р	И	Т	Л	И	Ф	О	З	П	Т	А	Г	Р
5	А	Т	И	И	П	О	О	К	Г	Я	А	К	Р	П	О	Я
2	Ф	О	З	П	Т	А	Г	Р	И	К		Т	О	Н	И	И
4	И	К		Т	О	Н	И	И	А	Т	И	И	П	О	О	К

РЭЛРИ ТЛИФО ЗПТАГ РГЯАК РПОЯИ К ТОН ИИАТИ ИПООК

- Количество вариантов шифртекста при таком способе можно определить как

$$Q = K! * P!\ ,$$

где K – количество столбцов в таблице,

P – количество строк в таблице.

ЛИТЕРАТУРА

1. Шеннон К.Э. Теория связи в секретных системах. В кн. Шеннона К.Э. “Работы по теории информации и кибернетике”.-М.: ИЛ,1963.- С. 243-332.
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии.-М.: Горячая Линия-Телеком, 2001.-120 с.
3. Романец Ю.И., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетах.-М.: Радио и связь, 1999.-328 с.
4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - Г.: ДМК, 2000.-448 с.
5. Жельников В.А. Криптография от папируса к компьютеру.-М.: ABF,1997.-336с.