

Лекция 8 (криптография)

1. Общие положения о безопасности ИС
2. Классификация сетевых атак
3. Криптографическая защита информации
4. Классификация алгоритмов шифрования
5. Структура системы засекреченной связи
6. Криптостойкость криптографического алгоритма
7. Типы алгоритмов шифрования
8. Примеры классических шифров
9. Самостоятельная работа



1. Общие положения о безопасности информационных систем (ИС)^D

- Термин "безопасность" шире «защиты», т.к. включает в себя не только понятие защиты, но также аутентификацию, аудит и обнаружение проникновения



Общие положения о безопасности информационных систем (ИС)

Основные понятия безопасности ИС

- **Уязвимость** - слабое место в системе.
- **Риск** - вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости.
- **Политика безопасности** - правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между информационными системами; набор критериев для предоставления сервисов безопасности.



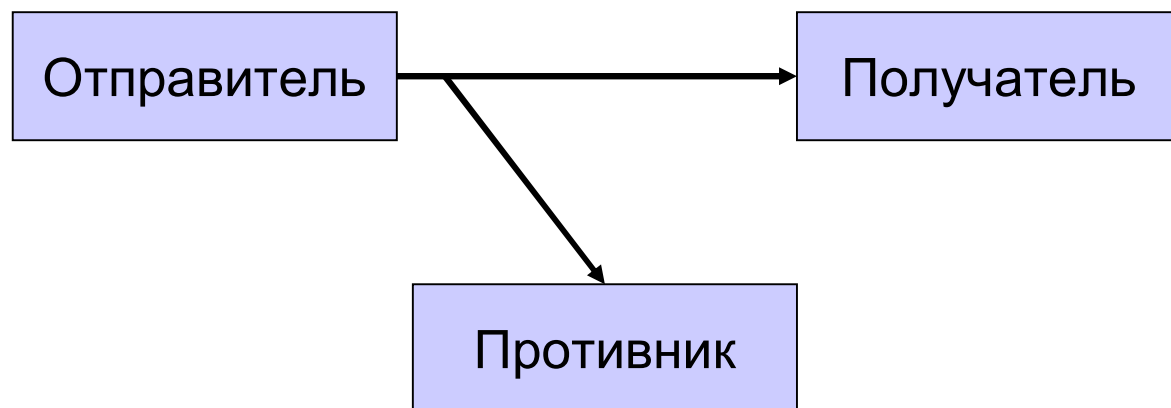
Общие положения о безопасности информационных систем (ИС)

- **Атака** - любое действие, нарушающее безопасность ИС.
- **Механизм безопасности*** - программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.
- **Сервис безопасности** - обеспечивает безопасность системы и/или передаваемых данных, либо определяет осуществление атаки. Сервис использует один или более механизмов безопасности.




2. Основные виды сетевых атак^L

Пассивная атака

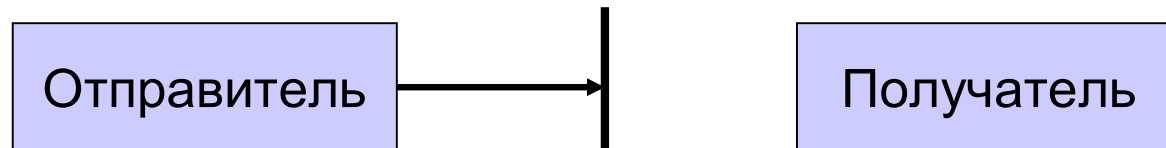




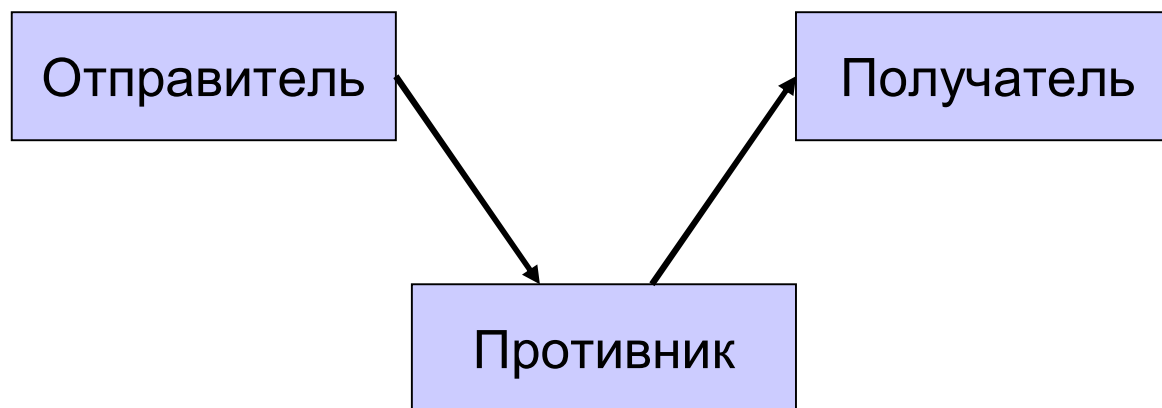
Активные атаки



1. Отказ в обслуживании - DoS-атака (Denial of Service*)

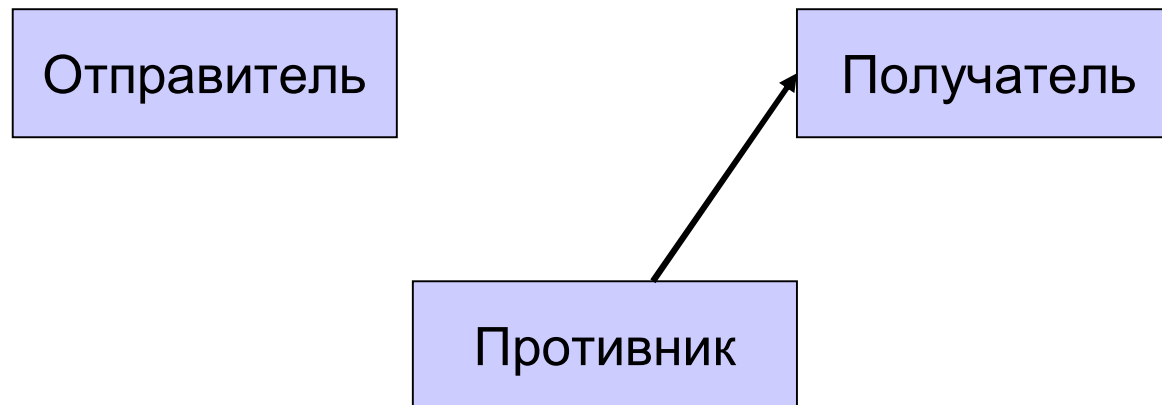


2. Модификация потока данных

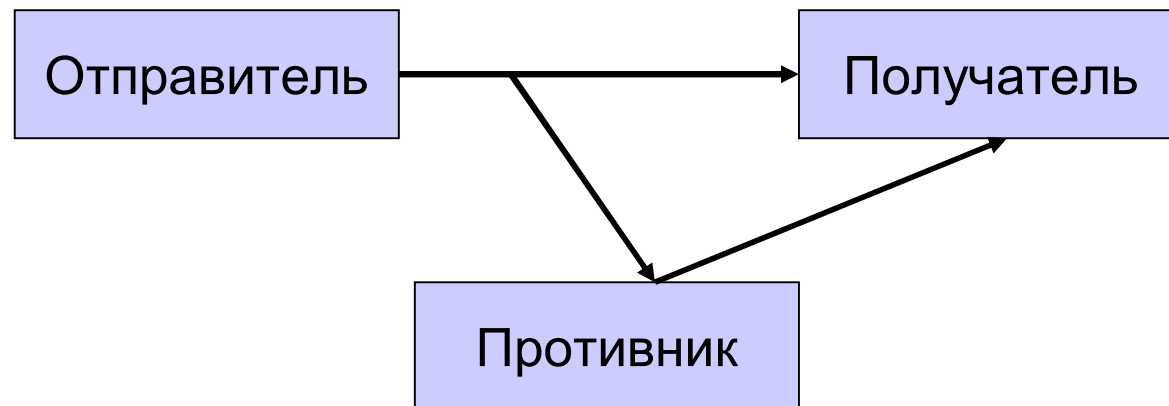




3. Создание ложного потока



4. Повторное использование^D





Механизмы безопасности

1. Алгоритмы **симметричного** шифрования
2. Алгоритмы **асимметричного** шифрования
3. **Хэш-функции**




Сервисы безопасности

- **Конфиденциальность** - предотвращение пассивных атак для передаваемых или хранимых данных.
- **Аутентификация** - подтверждение того, что информация получена из законного источника, и получатель действительно является тем, за кого себя выдает.
- **Целостность** - сервис, гарантирующий, что информация при хранении или передаче не изменилась.




Сервисы безопасности

- **Невозможность отказа** - невозможность, как для получателя, так и для отправителя, отказаться от факта передачи.
- **Контроль доступа** - возможность ограничить и контролировать доступ к системам и приложениям по коммуникационным линиям.
- **Доступность** - результатом атак может быть потеря или снижение доступности того или иного сервиса (минимизация возможности DoS-атак).



Задачи, решаемые при разработке сервиса безопасности

- Разработать **алгоритм** шифрования /дешифрования для выполнения безопасной передачи информации. Алгоритм д. б. таким, чтобы противник не мог расшифровать перехваченное сообщение, не зная **секретную** информацию.

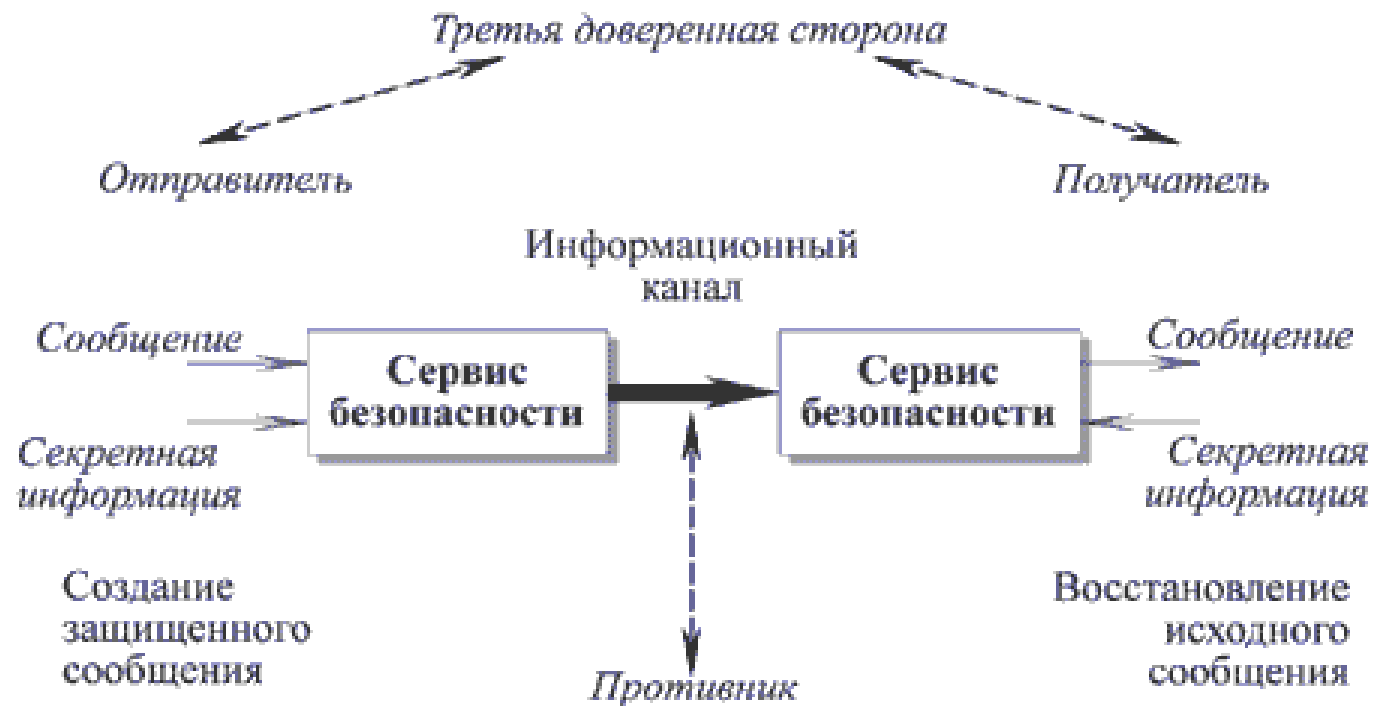


Задачи, решаемые при разработке сервиса безопасности

- Создать **секретную** **информацию**, используемую алгоритмом шифрования.
- Разработать **протокол** обмена сообщениями для распределения разделяемой секретной информации таким образом, чтобы она не стала известна противнику.

Модель сетевой безопасности

(асимметричный алгоритм шифрования)





3. Криптографическая защита информации



Определения

- **Криптология** (kryptos - тайный, logos - наука) - наука, изучающая проблемы защиты информации путем ее преобразования. Криптология состоит из *криптографии* и *криптоанализа*.
- **Криптография** занимается поиском и исследованием математических методов преобразования информации.
- **Криптоанализ** - исследование возможности расшифровывания информации без знания ключей.



Направления криптографии

1. Симметричные криптосистемы.
 2. Криптосистемы с открытым ключом.
 3. Системы электронной подписи.
 4. Управление ключами.
- Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.



L

-
- В качестве информации, подлежащей зашифрованию и расшифрованию, рассматриваются **тексты**, построенные на некотором **алфавите**.
 - **Алфавит** – конечное множество используемых для кодирования информации знаков.
 - **Текст** – упорядоченный набор из элементов алфавита.

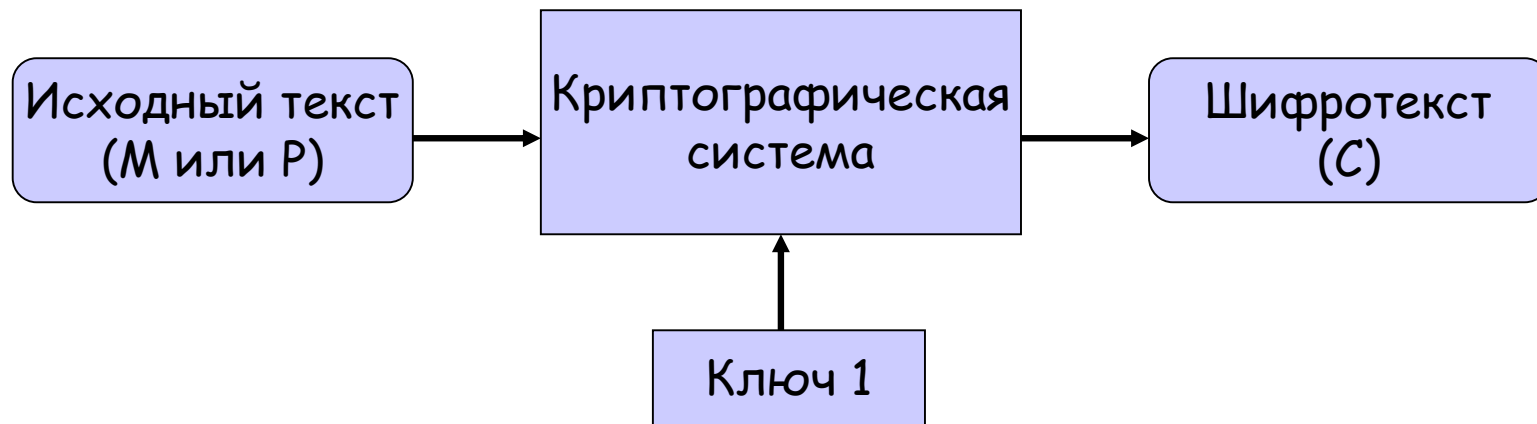


Примеры алфавитов

1. Z33 - 32 буквы русского алфавита и пробел;
2. Z44 - 32 буквы русского алфавита, знаки препинания и пробел;
3. Z256 - символы, входящие в стандартные коды ASCII и КОИ-8;
4. бинарный - $Z2 = \{0,1\}$;
5. восьмеричный - $Z8 = \{0,1,2,3,4,5,6,7\}$;
6. шестнадцатеричный - $Z16 = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$

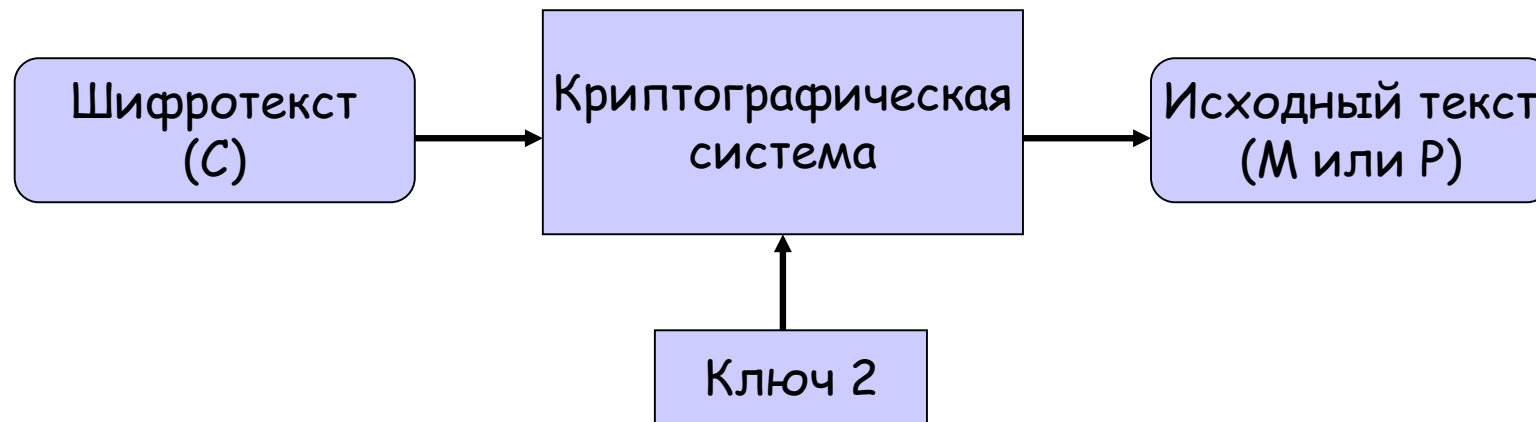
Зашифрование

- Процесс преобразования открытого текста (M) в криптограмму (C).




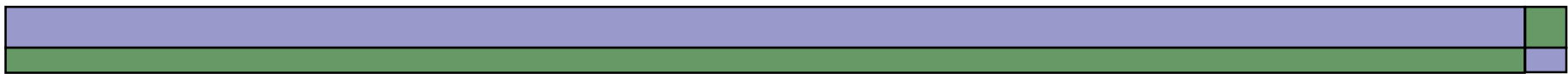
Расшифрование

- Процесс обратный зашифрованию. На основе ключа (К) C преобразуется в открытый текст.





- Ключи зашифрования и расшифрования в общем случае могут быть различными.

- 
-
- Незашифрованное сообщение обозначают **P** или **M** (англ. **P**laintext и **M**essage).
 - Зашифрованное сообщение обозначают **C** (англ. **C**iphertext).
 - **Ключ** — информация, необходимая для шифрования и расшифрования текстов.



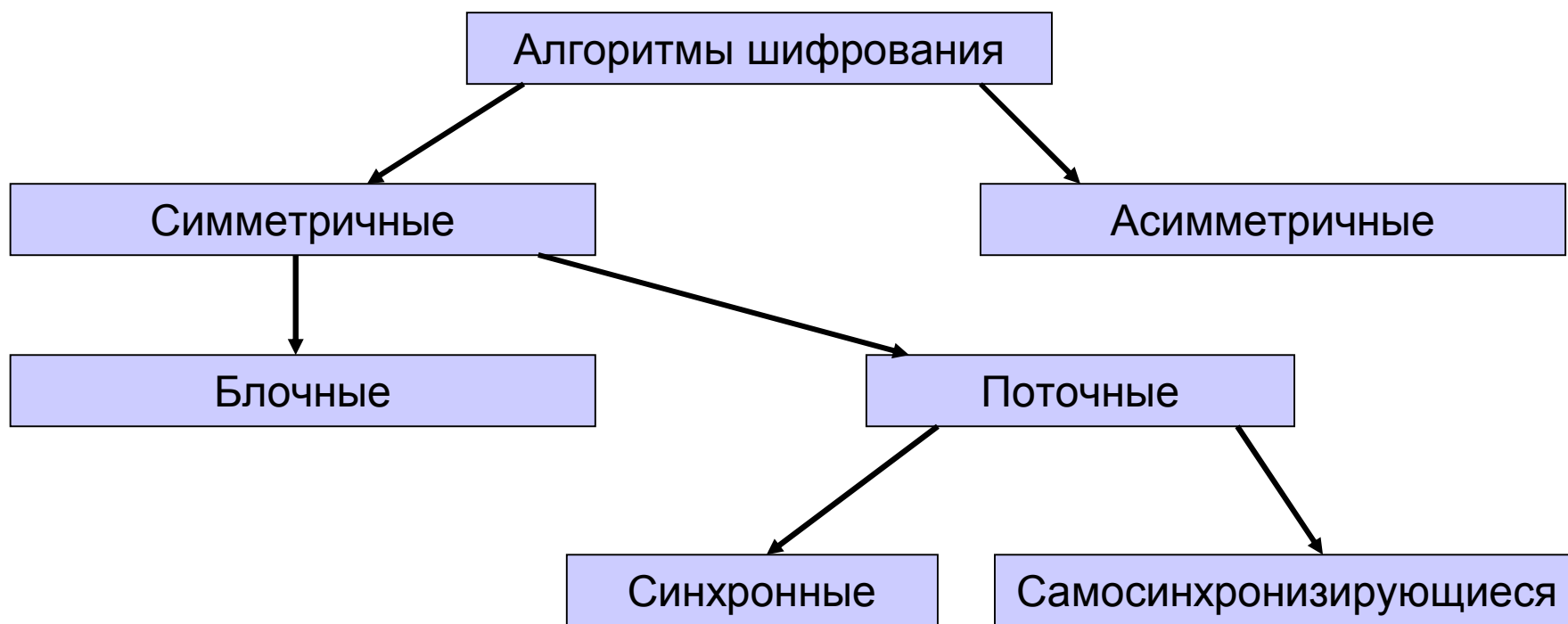
-
- **Ключевое пространство** — множество, из которого выбираются ключи.
 - **Алгоритмом зашифрования/расшифрования** называется совокупность процессов зашифрования/расшифрования, множества открытых сообщений, множества возможных закрытых сообщений и ключевого пространства.


- 
-
- Термины **распределение ключей** и **управление ключами** относятся к процессам системы обработки информации, содержанием которых является генерация и распределение ключей между пользователями.


- 
-
- **Электронной подписью** называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.



4. Классификация алгоритмов шифрования



- 
-
- Криптосистемы подразделяются на симметричные и асимметричные (с открытым ключом)
 - В симметричных криптосистемах для зашифрования и расшифрования используется один и тот же ключ.

- 
-
- В асимметричных системах используют два ключа: **открытый** и **закрытый**, которые математически связаны друг с другом. Информация зашифровывается на открытом ключе, который является общедоступным. Расшифрование осуществляется на закрытом ключе, который известен только получателю сообщения.



Симметричные КА

- разделены на два больших класса — **блочные** и **поточные**.
- 1. В блочных КА **M** разбивается на блоки определенной длины и каждый блок шифруется отдельно.
- 2. В поточных алгоритмах каждый символ **M** зашифровывается независимо от других.

5. Структура системы засекреченной связи






Работа системы засекреченной связи

- Из ключевого пространства выбирается ключ зашифрования K и отправляется по надежному каналу передачи.
- Формируют зашифрованное сообщение
$$C = E_k(M)$$
- Пересылают C по каналу передачи данных.
- На принимающей стороне преобразуют полученное сообщение C в M
$$M = D_k(C)$$



6. Криптостойкость КА

- 
-
- **Криптостойкость** – характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (стойкость к криптоанализу).
 - При **оценке криптостойкости** учитывают многие факторы:
 1. мощность ключевого пространства;
 2. количество операций, необходимое для вскрытия шифра;
 3. объем выборки **M** и **C**, необходимый для определения ключа;
 4. сложность решения математической задачи, лежащей в основе системы шифрования*.



Условия абсолютной стойкости КА

К. Шенноном были сформулированы следующие условия абсолютной стойкости алгоритмов шифрования

- длина ключа и длина открытого сообщения должны быть одинаковы;
- ключ должен использоваться только один раз;
- выбор ключа из ключевого пространства должен осуществляться равновероятно.




-
- **Стойкость системы** секретной связи не может быть выше стойкости алгоритмов шифрования, однако может быть и гораздо ниже.



Принцип Керкгоффса

- ПК — правило разработки системы секретной связи, согласно которому секретом является только ключ, а сам алгоритм может быть открыт без снижения его стойкости ниже допустимых значений.
- Т.е. при оценке стойкости системы считают, что противник знает о ней всё, кроме ключей.
- Впервые данный принцип сформулировал в XIX веке голландский криптограф Огюст Керкгоффс.



Причины осуществления **успешных атак** на алгоритмы шифрования

- статистическая структура естественных языков;
- наличие вероятных слов.



ОСНОВНЫЕ ТИПЫ АТАК

1. с известным C (ciphertext-only attack)
2. с известным M (known plaintext attack)
3. простая атака с выбором M (chosen-plaintext attack).
4. адаптивная атака с выбором M (adaptive-chosen-plaintext attack).
5. с выбором C (chosen-ciphertext attack).
6. адаптивная атака с выбором C (adaptive-chosen-ciphertext attack).
7. с выбором текста (chosen-text attack).
8. с выбором ключа (chosen-key attack).




Методы противодействия криптоанализу*

- **рассеивание** или **диффузия** (влияние одного символа **M** распространяется на множество символов **C**);
- **запутывание** или **конфузия** (влияние одного символа **K** распространяется на множество символов **C**);
- **перемешивание** (вероятные последовательности рассеиваются по всему пространству возможных открытых сообщений). Развитием метода явилось применение составных алгоритмов, состоящих из последовательности операций **перестановки** и **подстановки (замены)**.



7. Типы алгоритмов шифрования

- 
-
- В криптографии существуют два основных типа преобразований — **замены** и **перестановки**, все остальные преобразования являются их комбинацией.



-
- В шифрах **замены** один символ открытого текста замещается символом зашифрованного текста.
 - В **перестановочных** шифрах символы **М** изменяют свое местоположение.

Пример

(колонная
замена)

Задавая в качестве
перестановки
последовательность
2314675, получим
следующий
зашифрованный
текст

1	2	3	4	5	6	7
В		П	Е	Р	Е	С
Т	А	Н	О	В	О	Ч
Н	Ы	Х		Ш	И	Ф
Р	А	Х		С	И	М
В	О	Л	Ы		М	
И	З	М	Е	Н	Я	Ю
Т		С	В	О	Е	
М	Е	С	Т	О	П	О
Л	О	Ж	Е	Н	И	Е

2	3	1	4	6	7	5
	П	В	Е	Е	С	Р
А	Н	Т	О	О	Ч	В
Ы	Х	Н		И	Ф	Ш
А	Х	Р		И	М	С
О	Л	В	Ы	М		
З	М	И	Е	Я	Ю	Н
	С	Т	В	Е		О
Е	С	М	Т	П	О	О
О	Ж	Л	Е	И	Е	Н



Шифры замены

Различают четыре типа шифров замены

- **простой замены.** Один символ **М** заменяется одним символом зашифрованного текста;
- **сложной замены.** Один символ **М** заменяется одним или несколькими символами зашифрованного текста, например: «А» может быть заменен «С» или «SO5I»;
- **блочной замены.** Один блок символов **М** заменяется блоком закрытого текста, например: «ABC» может быть заменен «KDU» или «RIG»;
- **полиалфавитные шифры замены.** К **М** применяются несколько шифров простой замены.

8. Примеры классических шифров

1. Шифр Вернама
2. Квадрат Полибия
3. Шифр Виженера



Шифр Вернама

- Для получения **С** открытый текст объединяется с **К** операцией «исключающее ИЛИ» (**К** называется одноразовым блокнотом или шифроблокнотом).

Свойства К

- д.б. быть истинно случайным;
- совпадать по размеру с заданным открытым текстом;
- применяться только один раз.



Квадрат Полибия

- Применялся в Древней Греции (со II в. до н. э.).
- Это устройство представляло собой квадрат 5 x 5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку этого квадрата записывалась одна буква. (В греческом варианте одна клетка оставалась пустой, в латинском – в одну клетку помещали две буквы *i* и *j*.) В результате каждой букве отвечала пара чисел и шифрованное сообщение превращалось в последовательность пар чисел.

Квадрат Полибия

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z



Пример

13 34 22 24 44 34 15 42 22 34 43 45 32

- Это сообщение записано при использовании латинского варианта квадрата Полибия, в котором буквы расположены в алфавитном порядке. ("Cogito, ergo sum", "Я мыслю, следовательно существую").



Пример

- COMPUTER SCIENCE с помощью квадрата Полибия кодируется как
- 13 34 32 35 45 44 15 42 43 13 24 15
33 13 15



Шифр Виженера

- **Метод** полиалфавитного шифрования буквенного текста с использованием ключевого слова.
- Шифр изобретался многократно. Впервые его описал Джованни-Баттиста Беллазо в 1553 году. В XIX веке был назван по имени Блеза Виженера - швейцарского дипломата.
- Метод является недоступным для простых методов криптоанализа.

Шифр Виженера

[illegible]



Шифр Виженера

- Пример зашифрования фразы
«криптографиясерьезнаянаука»
с помощью пароля «математика»

м а т е м а т и к а м а т е м а т и к а м а т е м а
к р и п т о г р а ф и я с е р ь е з н а я н а у к а
ц р ь ф я о х ш к ф ф я д к э ь ч п ч а л н т ш ц а



9. Самостоятельная работа

Задание

Составить примеры зашифрования
текстового сообщения с помощью
классических шифров:

- ☐ Виженера;
- ☐ Квадрат Полибия;
- ☐ Цезаря;
- ☐ Колонной (строчной) замены;
- ☐ Вернама