

ЛЕКЦИЯ 2.

Понятие о традиционных методах шифрования

2.1. МОДЕЛЬ ТРАДИЦИОННОГО ШИФРОВАНИЯ

2.2. ТРЕБОВАНИЯ К КРИПТОГРАФИЧЕСКИМ СИСТЕМАМ

2.3. КРАТКИЕ СВЕДЕНИЯ О КРИПТОАНАЛИЗЕ

2.4. КЛАССИФИКАЦИЯ МЕТОДОВ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ ИНФОРМАЦИИ

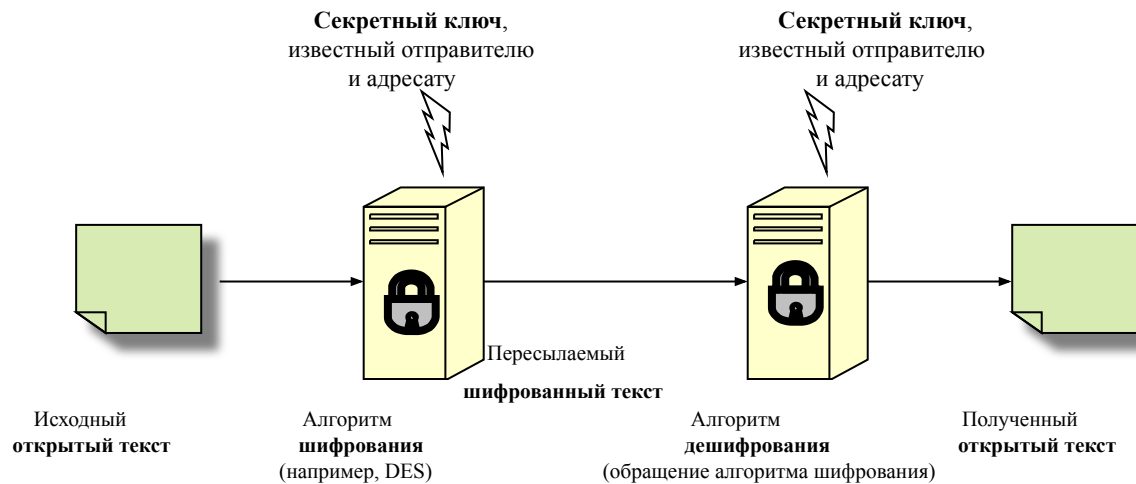


Рис.2.1. Модель традиционного шифрования

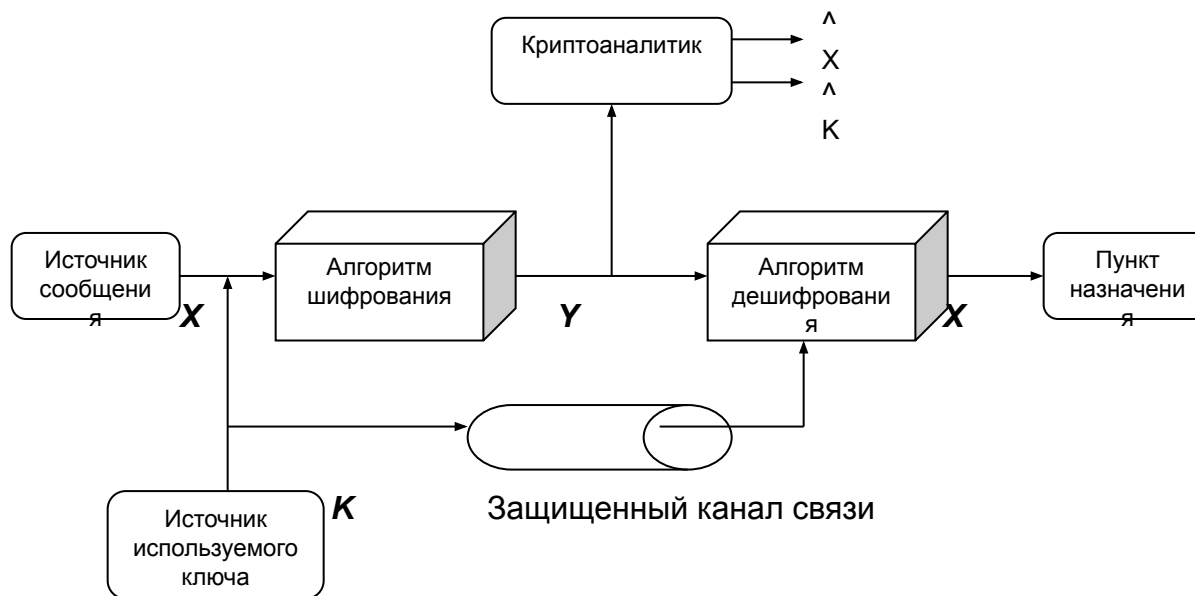


Рис.2.2. Функциональная схема традиционного шифрования

Элементы схемы традиционного шифрования

1. Сообщение в виде открытого текста $X = [X_1, X_2, \dots, X_M]$ Элементами X_i открытого текста X являются символы некоторого **конечного алфавита**.

2. Генерируется ключ в форме $K = [K_1, K_2, \dots, K_j]$.

3. С помощью алгоритма шифрования формируется шифрованный текст $Y = [Y_1, Y_2, \dots, Y_N]$:

$$Y = E_K(X)$$

4. Предполагаемый получатель сообщения, располагая ключом K , должен иметь возможность выполнить обратное преобразование:

$$X = D_K(Y)$$

5. Подразумевается, что противник знает и алгоритм шифрования (**E**), и алгоритм дешифрования (**D**).

Типы криптоанализа шифрованного сообщения.

Тип криптоанализа	Данные, известные криптоаналитику
Анализ только шифрованного текста	•Алгоритм шифрования •Подлежащий расшифровке шифрованный текст
Анализ с известным открытым текстом	•Алгоритм шифрования •Подлежащий расшифровке шифрованный текст •Один или несколько соответствующих фрагментов открытого и шифрованного текста, созданных с одним и тем же секретным ключом
Анализ с избранным открытым текстом	•Алгоритм шифрования •Подлежащий расшифровке шифрованный текст •Выбранный криптоаналитиком открытый текст и соответствующий шифрованный текст, созданный с помощью секретного ключа
Анализ с избранным шифрованным текстом	•Алгоритм шифрования •Подлежащий расшифровке шифрованный текст •Выбранный криптоаналитиком шифрованный текст и соответствующий открытый текст, расшифрованный с помощью секретного ключа
Анализ с избранным текстом	•Алгоритм шифрования •Подлежащий расшифровке шифрованный текст •Выбранный криптоаналитиком открытый текст и соответствующий шифрованный текст, созданный с помощью секретного ключа •Выбранный криптоаналитиком шифрованный текст и соответствующий открытый текст, расшифрованный с помощью

Схема шифрования называется **безусловно защищенной (абсолютно стойкой)**, если порожденный по этой схеме шифрованный текст не содержит информации, достаточной для **однозначного** восстановления соответствующего открытого текста, **какой бы большой по объему** шифрованный текст не имелся у противника.

Пользователь может получить лишь **относительно надежный** алгоритм, удовлетворяющий следующим **требованиям**:

- **Стоимость** взлома шифра **превышает** стоимость расшифрованной информации.
- **Время**, которое требуется для того, чтобы взломать шифр, **превышает** время, в течение которого информация актуальна.

Схема шифрования называется **защищенной по вычислениям**, если она соответствует обоим указанным критериям.

Среднее время анализа при простом переборе ключей

Длина ключа, бит	Число различных ключей	Необходимое время при скорости 1 шифрование/мс	Необходимое время при скорости 10^6 шифрований/мс
32	$2^{32} = 4,3 \cdot 10^9$	2^{31} мс = 35,8 мин	2,15 мс
56	$2^{56} = 7,2 \cdot 10^{16}$	2^{55} мс = 1142 года	10,01 часа
128	$2^{128} = 3,4 \cdot 10^{38}$	2^{127} мс = $5,4 \cdot 10^{24}$ лет	$5,4 \cdot 10^{18}$ лет
26 символов (перестановка)	$26! = 4 \cdot 10^{26}$	$2 \cdot 10^{26}$ мс = $6,4 \cdot 10^{12}$ лет	$6,4 \cdot 10^6$ лет

Все формы традиционного криптоанализа для схем традиционного шифрования разрабатываются на основе того факта, что некоторые **характерные особенности структуры открытого текста могут сохраняться при шифровании, проявляясь в соответствующих особенностях структуры шифрованного текста.**

- **ТРЕБОВАНИЯ К КРИПТОГРАФИЧЕСКИМ СИСТЕМАМ:**

- – **стойкость** шифра *противостоять криптоанализу* должна быть такой, чтобы вскрытие его могло быть осуществлено только решением задачи **полного перебора ключей** и должно либо выходить за пределы возможностей современных компьютеров, либо требовать создания использования *дорогих* вычислительных систем;
- – **крипτοстойкость** обеспечивается **не** секретностью алгоритма, а **секретностью ключа** (разделяет криптосистемы *общего* использования (алгоритм **доступен** потенциальному нарушителю) и *ограниченного* использования (алгоритм держится в **секрете**));
- – зашифрованное сообщение должно поддаваться чтению **только при наличии** ключа;
- – шифр должен быть стойким даже в случае, если нарушителю **известно** достаточно большое количество исходных данных и соответствующих им зашифрованных данных;

- – **незначительное** изменение ключа или исходного текста должно приводить к **существенному** изменению вида зашифрованного текста;
- – структурные элементы алгоритма шифрования должны быть **неизменными**;
- – шифртекст не должен существенно превосходить **по объему** исходную информацию;
- – **ошибки**, возникающие при шифровании, не должны приводить к **искажениям** и **потерям** информации;
- – не должно быть простых и легко устанавливаемых **зависимостей между ключами**, последовательно используемыми в процессе шифрования;
- – любой ключ из множества возможных должен обеспечивать **равную криптостойкость** (обеспечение линейного (**однородного**) пространства ключей);
- – **время** шифрования не должно быть **большим**;
- – **стоимость** шифрования должна быть согласована со **стоимостью закрываемой информации**.

Нарушитель (или **криптоаналитик**) - лицо (группа лиц), целью которых является прочтение или подделка защищенных криптографическими методами сообщений.

Допущения в отношении **криптоаналитика** (нарушителя) :

1. Нарушитель знает **алгоритм шифрования (или выработки ЭЦП)** и особенности его реализации в конкретном случае, но не знает секретного ключа.
2. Нарушителю доступны **все зашифрованные тексты**.
Нарушитель может иметь доступ к **некоторым исходным** текстам, для которых известны соответствующие им зашифрованные тексты.
3. Нарушитель имеет в своем распоряжении вычислительные, людские, временные и иные ресурсы, объем которых оправдан потенциальной ценностью информации, которая будет добыта в результате криптоанализа.

Попытку прочтения или подделки зашифрованного сообщения, вычисления ключа методами криптоанализа называют **криптоатакой** или **атакой на шифр**.

Удачную криптоатаку называют **взломом**.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа (т.е. *криптоатаке*).

Показатель криптостойкости – главный параметр любой криптосистемы. В качестве **показателя криптостойкости** можно выбрать:

- количество **всех возможных ключей** или вероятность подбора ключа за заданное время с заданными ресурсами;
- количество **операций** или **время** (с заданными ресурсами), необходимое для взлома шифра с заданной вероятностью;
- **стоимость** вычисления ключевой информации или исходного текста.

Основные направления методов криптоанализа.

1. **Статистический криптоанализ** — исследует возможности взлома криптосистем на основе изучения *статистических закономерностей* исходных и зашифрованных сообщений.

2. **Алгебраический криптоанализ** — занимается поиском *математически слабых* звеньев криптоалгоритмов.

Например, в 1997 г. в эллиптических системах был выявлен класс ключей, существенно упрощавший криптоанализ.

3. **Дифференциальный (или разностный) криптоанализ** — основан на анализе *зависимости изменения* зашифрованного текста от изменения исходного текста.

4. **Линейный криптоанализ** — метод, основанный на поиске *линейной аппроксимации* между исходным и зашифрованным текстом. Как и дифференциальный анализ в реальных криптосистемах, может быть применен только для анализа *отдельных* блоков криптопреобразований.

Уровни криптоатаки по нарастанию сложности.

1. **Атака по шифрованному тексту (Уровень КА1)** – нарушителю доступны все или **некоторые зашифрованные** сообщения.
2. **Атака по паре "исходный текст – шифрованный текст" (Уровень КА2)** – нарушителю доступны **все** или **некоторые зашифрованные** сообщения и соответствующие им **исходные** сообщения.
3. **Атака по выбранной паре "исходный текст – шифрованный текст" (Уровень КА3)** – нарушитель имеет возможность **выбирать исходный** текст, **получать** для него **шифрованный** текст и на основе анализа зависимостей между ними **вычислять ключ**.

Классификация методов шифрования (криптоалгоритмов)

по типу ключей:

- симметричные криптоалгоритмы;
- асимметричные криптоалгоритмы;

по размеру блока информации:

- потоковые шифры;
- блочные шифры;

по характеру воздействий, производимых над данными:

- метод замены (перестановки),
- метод подстановки,
- аналитические методы,
- аддитивные методы (гаммирование),
- комбинированные методы;

по используемым лингвистическим методикам:

- смысловое шифрование,
- символьное шифрование,
- комбинированное шифрование.