Лекция 1.

Введение в криптографию

1.1. Введение
1.2. История развития криптографии
1.3. Основные понятия и определения

Три возможности
передать нужную информацию нужному адресату в тайне от других:

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.
2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.
3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат.

Ситуация, в которой возникает задача скрытой передачи информации

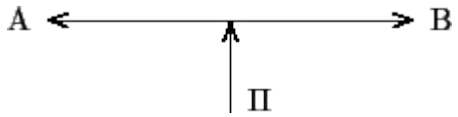

Рис. 1.1.

А и В - удаленные законные пользователи защищаемой информации;
П - незаконный пользователь (противник), который может перехватывать передаваемые по каналу связи сообщения и пытаться извлечь из них интересующую его информацию.

Решающие соображения
при выборе подходящих средств защиты информации:

1) является ли она для противника более ценной, чем стоимость атаки;
2) является ли она для вас более ценной, чем стоимость защиты.

История развития криптографии

Древний Египет.

Древнеегипетский криптоанализ был квазинаукой (т.н. «наивная» криптография). Но иероглифы Древнего Египта включали, хотя и в несовершенной форме, два важных элемента — секретность и преобразование письма, которые составляют основные атрибуты криптографии.

Древний Израиль.

В 600 - 500 годы до н. э. древние евреи создали упорядоченную систему криптографии "Атбаш" - в России известна под названием "тарабарская грамота". Суть метода проста: при письме одна буква алфавита заменяется другой, например, вместо буквы "а" всегда пишется буква "я".

Древняя Индия.

Классический древнеиндийский трактат об искусстве управлять государством, написанный между 321 и 300 годом до н. э., рекомендует, чтобы глава шпионской спецслужбы давал своим агентам задания с помощью тайнописи. Там же дипломатам дается совет прибегать к криптоанализу для получения разведывательных данных: «При невозможности беседовать с людьми пусть посол осведомится о происходящем у врага из речей нищих, пьяных, сумасшедших, спящих или из условных знаков, надписей, рисунков в храмах и местах паломничества».
Малоизвестно, что в известной древнеиндийской книге "Кама Сутра" криптография упоминается как одно из 64 искусств, обязательных к изучению.

Древний Китай.

Основные принципы разведки и контрразведки, включая и методы обработки информации, впервые сформулировал китайский ученый Сун Цзы в своей книге "Искусство войны" примерно в 500 году до н. э.

Древние Греция и Рим.

Шифр "Сцитала"

Известен со времен войны Спарты против Афин в **V веке до н.э.** Для его реализации использовалась **сцитала** - жезл, имеющий форму цилиндра. На сциталу виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль оси сциталы записывался открытый текст. Лента разматывалась и получалось (для непосвященных), что поперек ленты в беспорядке написаны какие-то буквы. Затем лента отправлялась адресату. Адресат брал такую же сциталу, таким же образом наматывал на нее полученную ленту и читал сообщение вдоль оси сциталы.
В этом шифре преобразование открытого текста в шифрованный заключается в определенной перестановке букв открытого текста. Поэтому класс шифров, к которым относится и шифр "Сцитала", называется **шифрами перестановки**.

Шифр Цезаря

Шифр реализует следующее преобразование открытого текста: каждая буква открытого текста заменяется **третьей** после нее буквой в алфавите, который считается написанным по кругу, т.е. после буквы "я" следует буква "а". Класс шифров, к которым относится и шифр Цезаря, называется **шифрами замены**.

Шифр "Полибианский квадрат“

Авторство приписывается греческому писателю **Полибию**. Является общей **моноалфавитной подстановкой**, которая проводится с помощью случайно заполненной алфавитом квадратной таблицы (для греческого алфавита размер составляет (5 × 5)). Каждая буква исходного текста заменяется на букву, стоящую в квадрате снизу от нее.

Научного криптоанализа не существовало ни в Египте, ни в Греции и Риме, ни в Индии, ни в Европе вплоть до 1400 года. Была только криптография.

Древний Восток.

Первыми открыли и описали методы **криптоанализа** арабы. В **855** году арабский ученый **Абу Бакр Ахмед бен-Али бен-Вахшия ан-Набати** включил несколько классических шифроалфавитов в свою «Книгу о большом стремлении человека разгадать загадки древней письменности».
Познания арабов в области криптологии были подробно изложены в произведении **Шехаба Калкашанди**, которое представляет собой громадную 14-томную энциклопедию, написанную в **1412** году для того, чтобы дать систематический обзор всех важных областей знания. Раздел под общим заголовком «Относительно сокрытия в буквах тайных сообщений» содержал две части: одна касалась символических действий и намеков, а другая была посвящена симпатическим чернилам и криптологии. Первый раз за всю историю шифров в энциклопедии приводился список как **систем перестановки**, так и **систем замены**.

Средневековая Европа.

Этап **формальной криптографии** (**конец XV – начало XX вв**.) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. **Леон Батист Альберти** предложил **многоалфавитную подстановку -** оригинальный шифр замены на основе двух концентрических кругов, по окружности которых записывались алфавиты открытого текста и шифротекста. При этом шифроалфавит был не последовательным *АБВГ… ЭЮЯ*, а произвольным *АЭВЮГ…,* и мог быть еще и смещен на любое число позиций.

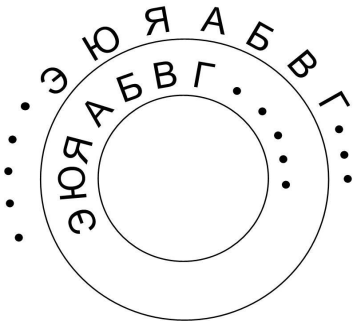

Рис.1.2.

Его работа **"Трактат о шифре"** (**1466 г.**) считается **первой** научной работой по криптологии.
Одна из первых печатных работ, в которой обобщены и сформулированы известные на тот момент алгоритмы шифрования, - **"Полиграфия"** (**1508** г.) немецкого аббата **Иоганна Трисемуса**. Ему принадлежат два небольших, но важных открытия: **способ заполнения полибианского квадрата** (первые позиции заполняются с помощью легко запоминаемого **ключевого** слова, остальные – оставшимися буквами алфавита) и **шифрование пар букв (биграмм)**.
В **1566** году известный математик **Джироламо Кардано** (отец теории вероятностей, матстатистики) опубликовал работу с описанием изобретенной им системы шифрования (**"решетка Кардано"**), положив, тем самым, начало **научной криптологии**.
В **1586** году дипломат **Блез Вижинер** предложил **полиалфавитный шифр**, который состоял в последовательном шифровании букв исходного текста по соответствующему алфавиту, выбираемому в соответствии с буквенным ключом (процедуру можно облегчить с помощью специальной таблицы).
Франция **XVI века** - шифры короля **Генриха IV** и **Ришелье**.
Англия **17 века** - ученый сэр **Фрэнсис Бэкон** создал устройство, где каждой букве алфавита могло соответствовать пять вариантов шифровки − т.е. использовалось представление букв алфавита **пятизначным двоичным кодом**: А - 00001, Б - 00010… .

Начало XIX в. - Чарльзом Уитстоном открыт способ многоалфавитной замены (подстановки биграмм) - шифр Плейфейера. Уитстону принадлежит и важное усовершенствование – шифрование "двойным квадратом".

В XIX в. голландец Керкхофф сформулировал главное требование к криптографическим системам, которое остается актуальным и поныне: секретность шифров должна быть основана на секретности ключа, но не алгоритма.

Последним словом в формальной криптографии, которое обеспечило еще более высокую криптостойкость, а также позволило автоматизировать (в смысле механизировать) процесс шифрования, стали роторные криптосистемы.

Одна из первых подобных систем (механическая машина) изобретена в 1790 г. Томасом Джефферсоном.

Одна из первых практически используемых машин - немецкая Enigma, разработанная в 1917 г. Эдвардом Хеберном и усовершенствованная Артуром Кирхом. Роторные системы – вершина формальной криптографии, так как относительно просто реализовывали очень стойкие шифры. Успешные криптоатаки на роторные системы стали возможны только с появлением ЭВМ в начале 40-х гг.

Научно-техническая революция и ее влияние на криптографию

Телеграф

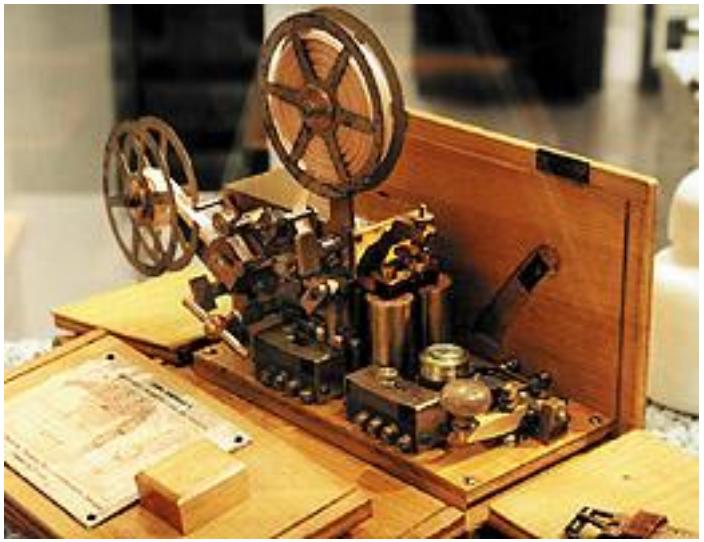

Рис. 1.3. Пишущий телеграфный аппарат Морзе, выпущенный заводами "Сименс и Гальске" в России

В 1844 году С. Морзе использовал специальную азбуку для кодирования букв, получившую название “азбуки Морзе”. В 1845 году Ф. Смит − юрист С. Морзе, опубликовал коммерческий код под названием “Словарь для тайной корреспонденции; приспособлен для применения на электромагнитном телеграфе Морзе”. В 1904 году в Англии появился словарь Уайтло для кодобозначений, содержавший, по утверждению автора, 400 млн. произносимых слов. В 1905 году Э. Бентли создал универсальный 5-буквенный код для телеграфных сообщений. Разбиение шифртекстов на пятибуквенные сочетания дошло до наших дней.
Д. Кан: “свой современный вид шифровальное дело получило, благодаря телеграфу”.

Радио.

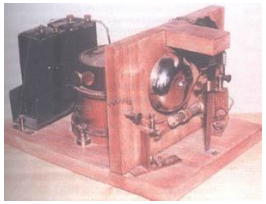

Рис. 1.4. Радиоаппарат Попова

Радиосвязь дала импульс к развитию стеганографических методов защиты информации. Широкое развитие радиосвязи привело к так называемой “радиоэлектронной войне”.

Рис. 1.5. Комната, оборудованная радио Маркони

Массовый характер приняли разработка и внедрение различных механических (позднее и электромеханических) приборов для шифрования и дешифрования сообщений - шифраторов.

Д. Кан: “телеграф создал современное шифровальное дело, радио - современный криптоанализ”.

Телефон.

Рис. 1.6. Настенный телефонный аппарат производства L. M. Ericsson & Co, Стокгольм

XX век

- СИЧ-передачи, в которых несущая частота быстро меняется в широком диапазоне по некоторому сложному закону СИЧ (скачкообразное изменение частоты);
- предварительное шифрование текста с последующей передачей шифрованного текста по телефону.

Рис. 1.7. Береговой центр морской радиосвязи

В 1900 году **Паульсеном** была предложена разбивка речевого сигнала на сегменты и передача их в обратном направлении (**временная инверсия**). В 1918 году **Тигерстедт** предложил разбивать речь на временные сегменты и переставлять их во времени (**временные перестановки**). В 1920 году **М. А. Бонч-Бруевич** усовершенствовал временную перестановку, введя **кадровую структуру преобразований** (каждые N сегментов переставлялись по-своему). В 1922 году **Хоу-Гольд** предложил применять **синхронное изменение несущей частоты** передатчика и настройки приемника (для засекречивания радиотелефонной связи).

Современная криптография.

Главная отличительная черта научной криптографии (1930 – 60-е гг.) – появление криптосистем со строгим математическим обоснованием криптостойкости. Работа Клода Шеннона "Теория связи в секретных системах" (1949) подвела научную базу под криптографию и криптоанализ.

В 1960-х гг. ведущие криптографические школы подошли к созданию блочных шифров, еще более стойких по сравнению с роторными криптосистемами, однако допускающих практическую реализацию только в виде цифровых электронных устройств.

Компьютерная криптография (с 1970-х гг.) обязана своим появлением вычислительным средствам с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры.

В 70-е гг. был разработан американский стандарт шифрования DES (принят в 1978 г.).

Хорст Фейстель (сотрудник IBM), описал модель блочных шифров, на основе которой были построены другие, более стойкие симметричные криптосистемы, в том числе, отечественный стандарт шифрования ГОСТ 28147–89.

Появление DES обогатило криптоанализ − для атак на американский алгоритм было создано несколько новых видов криптоанализа (линейный, дифференциальный и т.д.). В середине 70-х гг. XX столетия произошел прорыв в современной криптографии – появление асимметричных криптосистем, которые не требовали передачи секретного ключа между сторонами. Здесь отправной точкой принято считать работу, опубликованную Уитфилдом Диффи и Мартином Хеллманом в 1976 г. под названием "Новые направления в современной криптографии".

Несколькими годами позже Рон Ривест, Ади Шамир и Леонард Адлеман открыли систему RSA, первую практическую асимметричную криптосистему, стойкость которой была основана на проблеме факторизации больших простых чисел. Асимметричная криптография открыла сразу несколько новых прикладных направлений, в частности, системы электронной цифровой подписи (ЭЦП) и электронных денег.

В 1980–90-е гг. появились совершенно новые направления криптографии: вероятностное шифрование, квантовая криптография и другие. В этот же период были разработаны нефейстелевские шифры (SAFER, RC6 и др.). В 2000 г. после открытого международного конкурса был принят новый национальный стандарт шифрования США – AES.

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Наукой, изучающей математические методы защиты информации путем ее преобразования, является криптология (от греческого kryptos – тайный и logos – сообщение).

Криптология разделяется на два направления – криптографию и криптоанализ.

Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность. Под конфиденциальностью понимают невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа). Аутентичность информации состоит в подлинности авторства и целостности.

Криптоанализ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

- **симметричные криптосистемы,**
- **криптосистемы с открытым ключом,**
- **системы электронной подписи,**
- **управление ключами.**

Основные направления использования криптографических методов:

- **передача конфиденциальной информации по каналам связи (например, электронная почта),**
- **установление подлинности передаваемых сообщений,**
- **хранение информации (документов, баз данных) на носителях в зашифрованном виде.**

В качестве информации, подлежащей шифрованию и расшифрованию, а также электронной подписи рассматриваются тексты (сообщения), построенные на некотором алфавите.
Алфавит – конечное множество используемых для кодирования информации знаков.
Текст (сообщение) – упорядоченный набор из элементов алфавита.

В шифре всегда различают два элемента: алгоритм и ключ.
Шифр - совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования. (Более строго, шифр – это совокупность инъективных отображений множества открытых текстов во множество шифрованных текстов, проиндексированная элементами из множества ключей). Криптографическая система, или шифр, представляет собой семейство T_k – обратимых преобразований открытого текста в шифрованный.
Членам этого семейства можно взаимно однозначно сопоставить число k, называемое ключом. Преобразование T_k определяется соответствующим алгоритмом и значением ключа k.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всех возможных для данного алгоритма.

Пространство ключей K – это набор возможных значений ключа. Следует отличать понятия "ключ" и "пароль". Пароль также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

Криптосистемы подразделяются на симметричные и асимметричные [или с открытым (публичным) ключом]. В симметричных криптосистемах для шифрования и для расшифрования используется один и тот же ключ. В асимметричных системах (системах с открытым ключом) используются два ключа: открытый (публичный) и закрытый (секретный), которые математически связаны друг с другом. Информация зашифровывается с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины «распределение ключей» и «управление ключами» относятся к процессам обработки информации, содержанием которых является выработка и распределение ключей между пользователями.

Электронной (цифровой) подписью (ЭЦП) называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Зашифровыванием данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а расшифровыванием данных – процесс преобразования закрытых данных в открытые с помощью шифра.

Дешифрованием называется процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме, т.е. методами криптоанализа.

Шифрованием называется процесс зашифровывания или расшифровывания данных.

Неверно в качестве синонима шифрования использовать термин "кодирование" (а вместо "шифра" – "код"), так как под кодированием обычно понимают представление информации в виде знаков (букв алфавита).

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

Гамма шифра – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифровывания открытых данных и расшифровывания зашифрованных данных.

Гаммирование – процесс наложения по определенному закону **гаммы шифра** на открытые данные.

Имитозащита – защита от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется **имитовставка**, представляющая собой последовательность данных фиксированной длины, полученную по определенному правилу из открытых данных и ключа.

Криптографическая защита – это защита данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием и (или) выработкой имитовставки.

Синхропосылка – исходные открытые параметры алгоритма криптографического преобразования.

Уравнение зашифровывания (расшифровывания) – соотношение, описывающее процесс образования зашифрованных (открытых) данных из открытых (зашифрованных) данных в результате преобразований, заданных алгоритмом криптографического преобразования.