Unity. Precision. Perfection.

КОНСПЕКТ ЛЕКЦИЙ
по дисциплине «Криптография и защита информации»

Лектор: Племянников

Страниц: 13

Последнее обновление: 9 сентября 2019 г.

Автор: Корытов Павел, 6304

Санкт-Петербург

2019

Содержание

1. Введение

1.1. Криптография

Место криптографии среди других наук

- *Криптография* занимается разработкой методов (криптографических) преобразований информации с целью ее защиты от незаконных пользователей
- *Криптоанализ* — занимается оценкой сильных и слабых сторон криптографических методов, а также разработкой методов, позволяющих взламывать криптографические преобразования (шифры, например)
- *Криптология* — наука, занимающаяся исследованиями криптографических преобразований. Криптология состоит из двух частей — криптография и криптоанализ

Цели информационной безопасности

- Доступность (Availability)
- Целостность (Integrity)
- Конфиденциальность (Confidentiality)

S.c. AIC-триада

Угрозы в фокусе криптографии

- Раскрытие данных
- Модификация данных
- Имитация источника
- Отказ от авторства

Задачи криптографии

- Обеспечение конфиденциальности — защита содержимого информации от лиц, не имеющих к ней доступа.
- Обеспечение целостности — гарантирование невозможности несанкционированного изменения информации.
- Обеспечение аутентификации — разработка и внедрение методов подтверждения подлинности сторон и самой информации.
- Обеспечение невозможности отказа от авторства — предотвращение возможности отказа субъектов от некоторых совершенных ими действий.

Идентификация, аутентификация и авторизация

- Идентификация — Определение
- Аутентификация — Проверка
- Авторизация — Доступ

Стеганография — наука о скрытой передаче информации путём сохранения в тайне самого факта передачи

Базовая модель передачи данных

Рисунок 1. Базовая модель передачи данных

1.2. Определения

Определения из криптографии

- *Открытый текст (plaintext)* . Данные в читаемом формате, также называемые простым текстом (cleartext).
- *Зашифровка (encipher)* . Действие по преобразованию исходных данных внечитаемый формат.
- *Шифротекст (ciphertext)* — данные в форме, которая выглядит случайной и нечитаемой
- *Расшифровка (decipher)* . Действие по преобразованию шифротекста обратно в читаемую форму.
- *Шифр (cipher)* — набор математических правил (алгоритм), используемых для зашифрования и расшифрования.
- *Секретный ключ (secret key)* — секретная информация, используемая при зашифровании/расшифровании сообщений
- *Криптосистема (cryptosystem)* — набор криптографических преобразований или

алгоритмов, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информационного процесса

Определения из криптоанализа

- *Криптоаналитик* (нарушитель) — лицо (группа лиц), целью которых является прочтение или подделка защищённых криптографическими методами текстов
- *Атака* — Попытки получения какой-либо скрытой информации или скрытой подделкой истинной информации
- *Взлом* — Успешная проведённая атака

Виды атак

- На основе широтекста (Ciphertext Only)
- На основе невыбранного открытого текста (Known Plaintext)
- На основе выбранного открытого текста (Chosen Plaintext). Доступна аппаратура шифровальщика
- На основе выбранного шифротекста (Chosen Ciphertext). Доступна аппаратура принимающей стороны

1.3. История развития криптографии

Основные этапы развития криптографии

- Интуитивная (до начала XVI века)
- Формальная (XV — XX)
- Научная (30-е — 60-е годы XX века)
- Компьютерная (с 70-х годов XX века)

1.4. Интуитивная криптография

1.4.1. Шифр “Сцитала”

Открытый текст: ПРИМЕРШИФРАСЦИТАЛА

П	**Р**	**И**	**М**	**Е**	**Р**
Ш	**И**	**Ф**	**Р**	**А**	**С**
Ц	**И**	**Т**	**А**	**Л**	**А**

Текст наматывается на жезл.

Рисунок 2. Базовая модель классической криптосистемы

Зашифрованный текст: ПШЦРИИИФТМРАЕАЛРСА

Методика взлома (Аристотель): на длинный конус наматывалась лента, а затем эту ленту начинали сдвигать по конусу. Там, где буквы текста формировали слова или слоги, диаметр конуса совпадал с диаметром цилиндра.

Это пример атаки методом “грубой силы” (brute force) — полный перебор ключей (секретов) шифра при известном алгоритме зашифровки. Чтобы предотвратить этот тип атаки, число возможных ключей должно быть очень большим

Шифр изгороди (rail fence)

.

Открытый текст: ПРИМЕРШИФРАИЗГОРОДИ

Рисунок 3. Зашифровка шифром изгороди

Шифротекст: ПИЕШФАЗООИРМРИРИГРД

В современном варианте уровней может быть произвольное количество с произвольным порядком.

В приведенном варианте шифр основан только на знании алгоритма; секрета нет.

1.4.2. Шифр Атбаш. Моноалфавитная замена

Основан на использовании таблиц вида:

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

1.4.3. Шифр Цезаря

Основан на сдвиге алфавита. У Цезаря алфавита сдвигался на 3 буквы

Еще совсем недавно (в 1980-х годах) применялся метод шифрования *ROT13* , в котором использовался сдвиг алфавита на 13 букв вместо трех. Этот шифр использовался в различных онлайновых форумах для публикации запрещенной информации.

Шифры “Изгородь”, “Атбаш”, “Цезаря” основаны на знании алгоритма. Это примеры безключевых шифров. Взлом подобных шифров не являются предметом криптоанализа

1.5. Формальная криптография

1.5.1. Аддитивный шифр

- Заменим буквы алфавита числами соответствующими их порядковым номерам в алфавите $0, 1, \ldots, n-1$.
- Представим символы открытого текста P_i и шифротекста C_i
- Выбираем в качестве ключа числа k
- Шифрование: $C_i = (P_i + k) \bmod n$
- Расшифровка: $P_i = (C_i - k) \bmod n$

Шифр уязвим к атакам методом “грубой силы”. Множество ключей аддитивного шифра равно числу букв алфавита. Нулевой ключ, является бесполезным (зашифрованный текст будет совпадать с исходным текстом). Требуется перебор $n-1$ возможных ключей

1.5.2. Мультипликативный шифр

- Заменим буквы алфавита числами соответствующими их порядковым номерам в алфавите $0, 1, \ldots, n-1$.
- Представим символы открытого текста P_i и шифротекста C_i

- Выбираем в качестве ключа число $k \in [1, n)$, $k \times k^{-}1 \equiv 1 \bmod n$ (существует мультипликативная версия)
- Шифрование символа: $C_i = (P_i \times k) \bmod n$
- Расшифровка символа: $P_i = (C_i \times k^{-}1) \bmod n$

Множество ключей мультипликативного шифра равно числу ключей аддитивного шифра, имеющих мультипликативную инверсию. Требуется перебор в худшем случае n-1 возможных ключей

1.5.3. Афинный шифр

- Комбинация аддитивного и мультипликативного шифров
- Ключ состоит из двух частей: k_1, k_2
- Шифрование: $C_i = (P_i \times k_1 + k_2) \bmod n$
- Расшифровка: $P_i = ((C_i - k_2) \times k_1^{-1}) \bmod n$
- При $k = 1$ — аддитивный шифр
- При $k = 1$ и $k_2 = 25$ — шифр Атбаш
- При $k_2 = 0$ — мультипликативный шифр

Сложность атаки грубой силой — $\varphi(n) \times n$, где $\varphi(n)$ — функция Эйлера.

Если известна биграмма P_iP_{i+1} и её шифр C_iC_{i+1}, можно решить систему уравнений:

$$\begin{cases} C_i = (P_i \times k_1 + k_2) \bmod n \\ C_{i+1} = (P_{i+1} \times k_1 + k_2) \bmod n \end{cases}$$

Т.е. определить $k_1 = ((C_{i+1} - C_i) \times k_1^{-1} + (P_{i+1} - P_i)) \bmod n$. В случае нескольких решений ориентироваться на связность расшифрованного текста

1.5.4. Шифр моноалфавитной подставновки

Символы алфафита однозначно заменяются на символы другого алфавита. Ключ — перестановка; количество перестановок — $n!$

Возможна атака методом *частотного анализа*:

- Подсчитывается частота появления каждой буквы шифротекста
- Полученное распределение частот сравнивается, например, со справочной таблицей частот для символов языка открытого текста
- Ввыдвигаются гипотезы о соответствии букв открытого текста и шифротекста

- Сделанные гипотезы проверяются с помощью справочных таблиц распределения биграмм и триграмм

1.5.5. Омофонический шифр

Идея — сделать частоту распределения символов максимально равномерной. Наиболее частым букв исходного алфавита ставится большее количество букв алфавита шифра

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
8.2	1.2	4.1	4.1	11.8	1.9	1.1	3.0	8.3	0.1	0.3	4.4	2.1	9.2	8.3	2.9	0.1	6.1	5.1	8.8	2.8	1.6	0.7	0.1	1.0	0.1
8	1	4	4	11	2	2	3	8	1	1	4	3	9	8	3	1	6	5	8	2	2	1	1	1	1
86, 3, 60, 14, 67, 42, 84, 41	36	95, 92, 38, 2	81, 48, 15, 80	98, 76, 40, 79, 75, 69, 62, 61, 82, 51,5	68, 29	96, 21	47, 74, 99	46, 52, 19, 33, 93, 94, 89, 9	63	83	45, 57, 16, 13	0, 65, 72	24, 7, 34, 12, 26, 1, 32, 30, 73	44, 87, 77, 97, 18, 90, 10, 23	20, 22, 37	35	17, 39, 91, 11, 50, 25	64, 85, 27, 55, 58	71, 70, 28, 53, 43, 31, 66, 54	6, 49	78, 8	56	59	88	4

Рисунок 4. Пример омофонического шифра для английского языка

1.5.6. Шифр Виженера

Шифр многоалфавитной замены.

Рисунок 5. Пример шифра Виженера

- Заменим буквы алфавита числами соответствующими их порядковым номерам в алфавите $0, 1, \ldots, n-1$.
- Представим символы открытого текста P_i, ключа K_i и шифротекста C_i
- Сформируем *гамму* повторением ключа: $G = (K_1, \ldots, K_M) \ldots (K_1, \ldots, K_m)$
- Шифрование символа: $C_i = (P_i + G_i) \bmod n$

- Расшифровка символа: $P_i = (C_i - G_i) \bmod n$

Сложность атаки грубой силы — $\frac{n!}{(n-m)!}$.

При атаке шифр рассматривается как комбинации аддитивных шифров.

1. Автокорреляционный метод. Определение длины ключевого слова.
   - Шифротекст (длиной L) выписывается в строку. Под ней выписываются строки, полученные сдвигом влево на $t = 1, 2, 3, \ldots$ позиций.
   - $\forall t$ подсчитывается n_t — число совпадений символов, находившихся на одинаковых позициях в шифротексте и его версии со сдвигом t
   - Вычисляеются автокорреляционные коэффициенты $K_t = \frac{n_t}{L-t}$
   - Для сдвигов, кратных периоду ключа, K_t будут заметно больше и будут иметь значение, близкое к индексу совпадений используемого языка (для русского языка ≈ 0.0533)
   - Соответствующие сдвиги t берутся в качестве оценки ключа
2. Статистический метод. Разделение шифротекста на части, зашифрованных одинаковым символом ключа и анализ полученных частей методами статистического анализа для поиска всех символов ключа
   - Анализируются фрагменты шифротекста, зашифрованные одной и той же буквой шифра
   - По возможности применяются методы частотного анализа

1.5.7. Свойства рассмотренных шифров

- Симметричность — отправитель и получатель обладают одинаковыми секретными ключами и одинаковыми алгоритмами для зашифрования и расшифрования
- Поточность — каждый символ открытого текста преобразуется в сисмвол зашифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста
- Основаны преимущественно на операциях перестановки и замены (подстановки)

1.5.8. Шифр двойной перестановки

Исходый текст записывается в матрицу. Ключ — перестановка столбцов и строк в матрице. Сложность атаки грубой силы — $n! \times m!$.

Общее название таких шифров — шифры маршрутных перестановок.

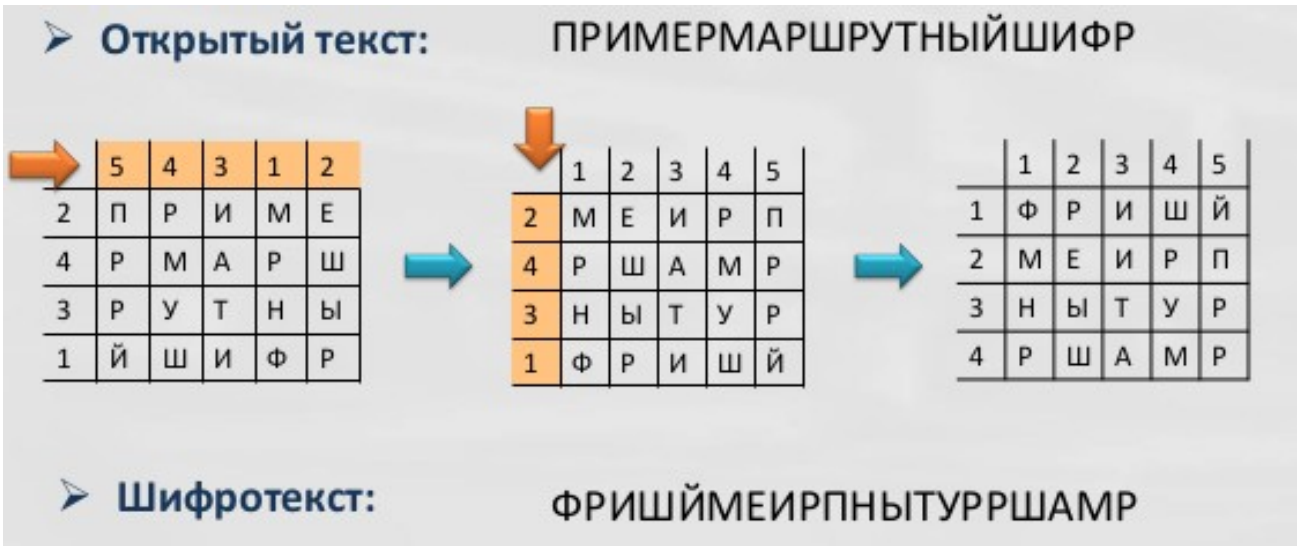

Рисунок 6. Пример шифра двойной перестановки

Для расшифровки применим частотный анализ биграмм. Предпринимаются попытки определить размер столбца; затем отсеиваются гипотезы перестановок с помощью обнаружения запретных биграмм.

Желательно знание фрагментов открытого текста.

1.5.9. Шифр Плейфера

Военный шифр 1854 года. Первый пример блочного шифра.

Исходный текст разбивается на блоки — биграммы по 2 символа. Ключом является матрица $5\times$.

- Если две буквы находятся в одной строке, то они заменяются на букву справа
- Если в одном столбце, то аналогично для столбца
- Если в разных, то составляется биграмма из букв, расположенных по противоположной диагонали

Сложность атаки грубой силой — $25!$.

Преимущество шифра в том, что он скрывает частоту отдельных букв, но возможна атака на основе анализа частоты биграмм. Для расшифровки полезно знание фрагментов исходного текста, например стандартной формы обращения.

Во время войны устраивались провокации, после чего на основе данных о провокации проводилась расшифровка.

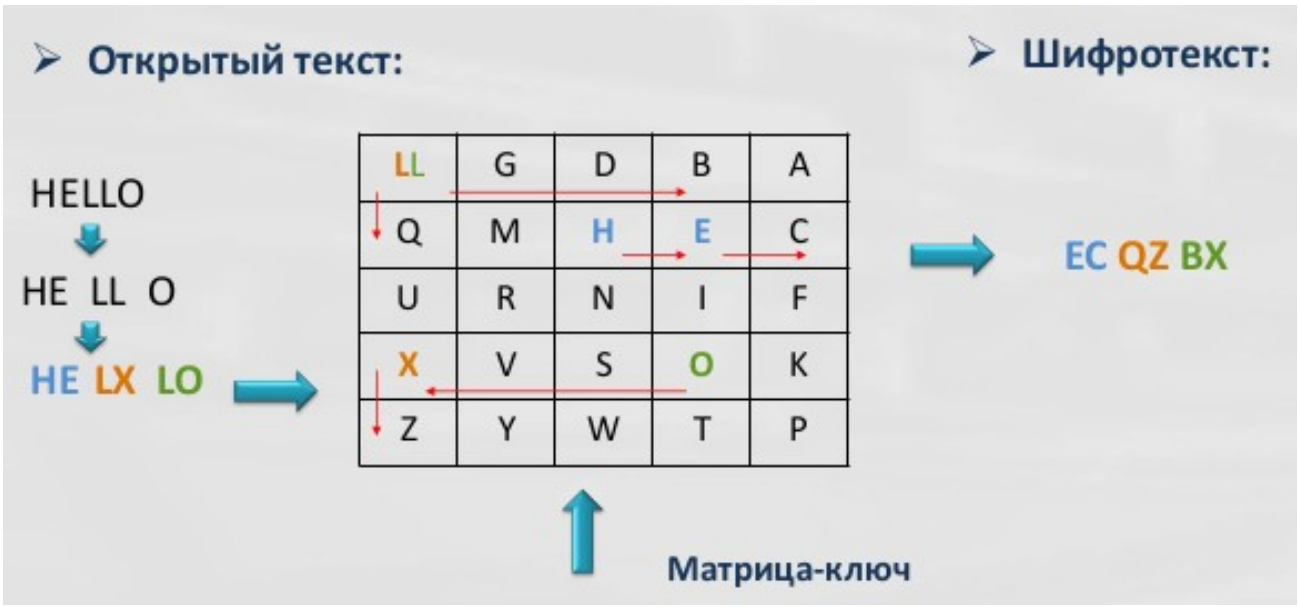

Рисунок 7. Пример шифра Плейфера

1.5.10. Шифр Хилла

Изобретён в 1929 году.

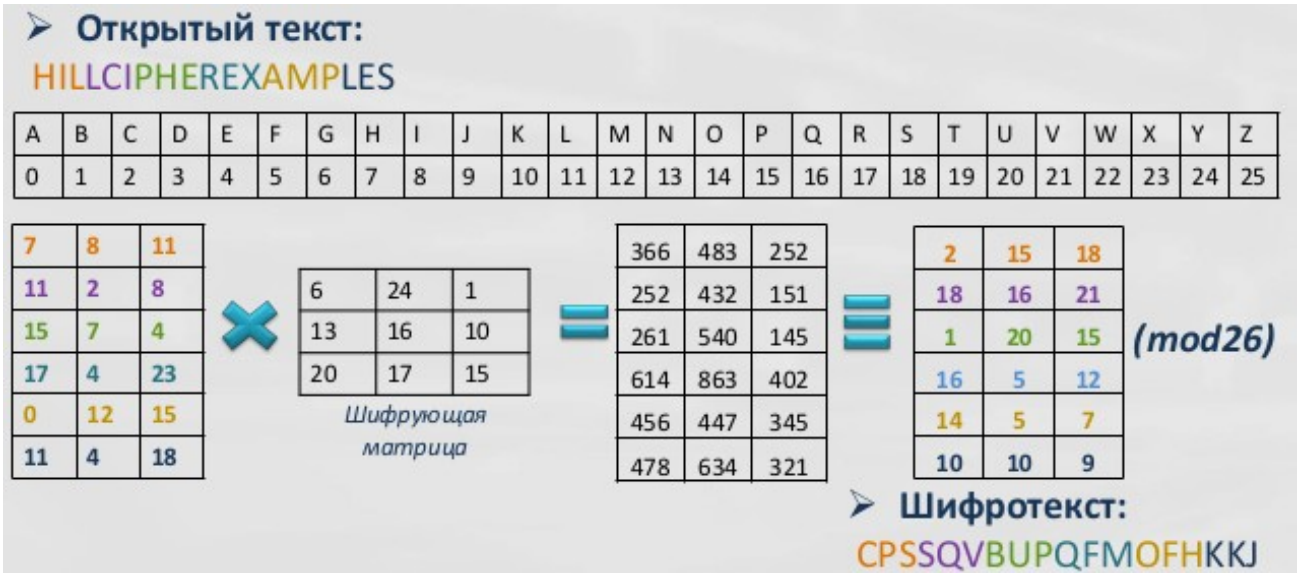

Рисунок 8. Зашифровка шифром Хилла

Требования к матрице — она должна быть обратима, т.е. $|M| \neq 0$. В таком случае M^{-1} — мультипликативная инверсия в $\mathbb{Z}_{26}$: $M \times M^{-1} \equiv I \bmod 26$

Сложность атаки грубой силов — $n^{m \times m}$.

Этот шифр совсем не сохраняет статистику исходного текста. Атака возможна на основе знания исходного текста:

- Делается предположение о размере блока (например, m)

Рисунок 9. Расшифровка шифра Хилла

- Добываются не менее m пар блоков открытого текста и шифротекста и строится уравнение $C = P \times K$
- Выполняется попытка восстановить матрицу-ключ $K = C \times P^{-1}$
- В случае неудачи выбирается другой размер блока m

1.5.11. Комбинированный шифр ADFGVX

Ещё один военный шифр; изобретен в 1918 году.

Рисунок 10. Шаг 1 шифра ADFGVX — замена

Атаки основаны на знании фрагментов открытого текста:

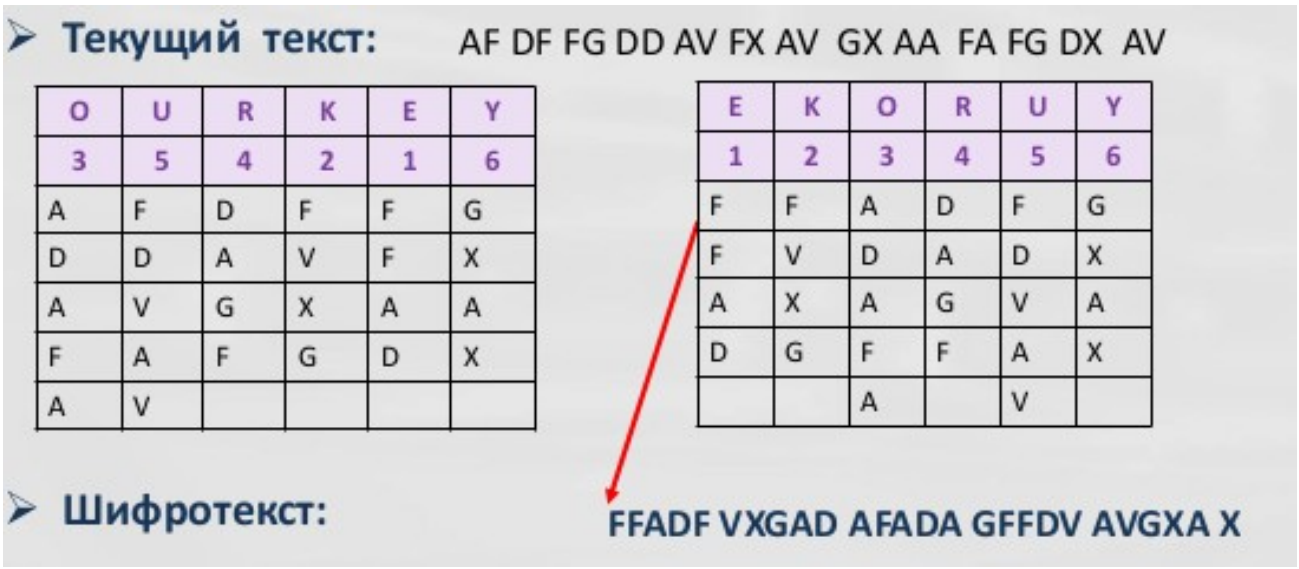

Рисунок 11. Шаг 2 — перестановка

- На основе анализа 2-х или более сообщений с одинаковым начальным текстом
- На основе анализа 2-х или более сообщений с одинаковым окончанием
- На основе сообщений одинакового размера

Определяется перестановка, а затем — частотным анализом — шифрующая матрица