ШИФР ВИЖЕНЕРА

ОСНОВНЫЕ ПОНЯТИЯ

Криптография представляет собой ***совокупность методов преобразования*** данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей.
Такие преобразования обеспечивают решение трех главных принципов защиты информации: обеспечение конфиденциальности, целостности и доступности передаваемых или сохраняемых данных.
Для реализации указанных принципов используются *криптографические технологии шифрования, цифровой подписи и аутентификации.*
Основой большинства криптографических средств защиты информации является *шифрование данных*.
Шифр - совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования.
Зашифровыванием *информации* понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст). *Процесс восстановления* исходного текста по криптограмме с использованием ключа шифрования называют расшифровыванием (дешифрованием).

КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

В ЗАВИСИМОСТИ ОТ ЧИСЛА КЛЮЧЕЙ, ПРИМЕНЯЕМЫХ В КОНКРЕТНОМ АЛГОРИТМЕ:

КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Все известные способы шифрования с симметричными ключами можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование (дешифрование).

1) Подстановочным шифром называется шифр, который каждый символ открытого текста в шифротексте заменяет другим символом, т.е. в рамках этого же сообщения. Например,

Шифр Цезаря: Y = (x + j) mod A

Y - получаемый символ

x – номер буквы

j – смещение буквы (вроде ключа)

A - алфавит, например, для зашифровки английского сообщения A=26, русского – 33.

Например, j = 3 ..

Другой разновидностью метода замены является *схема шифрования Вижинера (см.слайд 6)*

2) В перестановочном шифре меняется не открытый текст, а порядок символов.

Например, простой столбчатый перестановочный шифр: открытый текст пишется горизонтально на разграфлённой бумаге фиксированной ширины, а шифротекст считывается вертикально. Дешифрование представляет собой запись текста вертикально на разграфлённом листе фиксированной ширины, а затем считывание открытого текста горизонтально. Ключом здесь служит – фиксированная ширина строки.

КРИПТОГРАФИЯ И КРИПТОАНАЛИЗ

- **Криптография** занимается поиском и исследованием математических методов преобразования информации.
- Сфера интересов **криптоанализа** — исследование возможности расшифровывания информации без знания ключей

ШИФР ВИЖЕНЕРА

Шифр Виженера (фр. *Chiffre de Vigenère*) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (итал. *Giovan Battista Bellaso*) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году, однако в XIX веке получил имя Блеза Виженера, швейцарского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

ШИФР ВИЖЕНЕРА

Первое точное документированное описание многоалфавитного шифра было сформулированно **Леоном Баттиста Альберти** в 1467 году, для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, **Иоганн Трисемус** в своей работе «Полиграфия» изобрел tabula recta — центральный компонент шифра Виженера.

То, что сейчас известно под шифром Виженера, впервые описал Джованни Батиста Беллазо в своей книге La cifra del. Sig. Giovan Battista Bellaso. Он использовал идею tabula recta Трисемуса, но добавил ключ для переключения алфавитов шифра через каждую букву.

БЛЕЗ ВИЖЕНЕР

Блез Виженер представил своё описание простого, но стойкого шифра перед комиссией Генриха III во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему.

Давид Кан в своей книге «Взломщики кодов» отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания».

ШИФР ВИЖЕНЕРА

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр» англ. *The Alphabet Cipher*, опубликованной в детском журнале в 1868 году.

В 1917 году Scientific American также отозвался о шифре Виженера, как о неподдающемся взлому. Это представление было опровергнуто после того, как Казиски полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

ШИФР ВИЖЕНЕРА

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски.

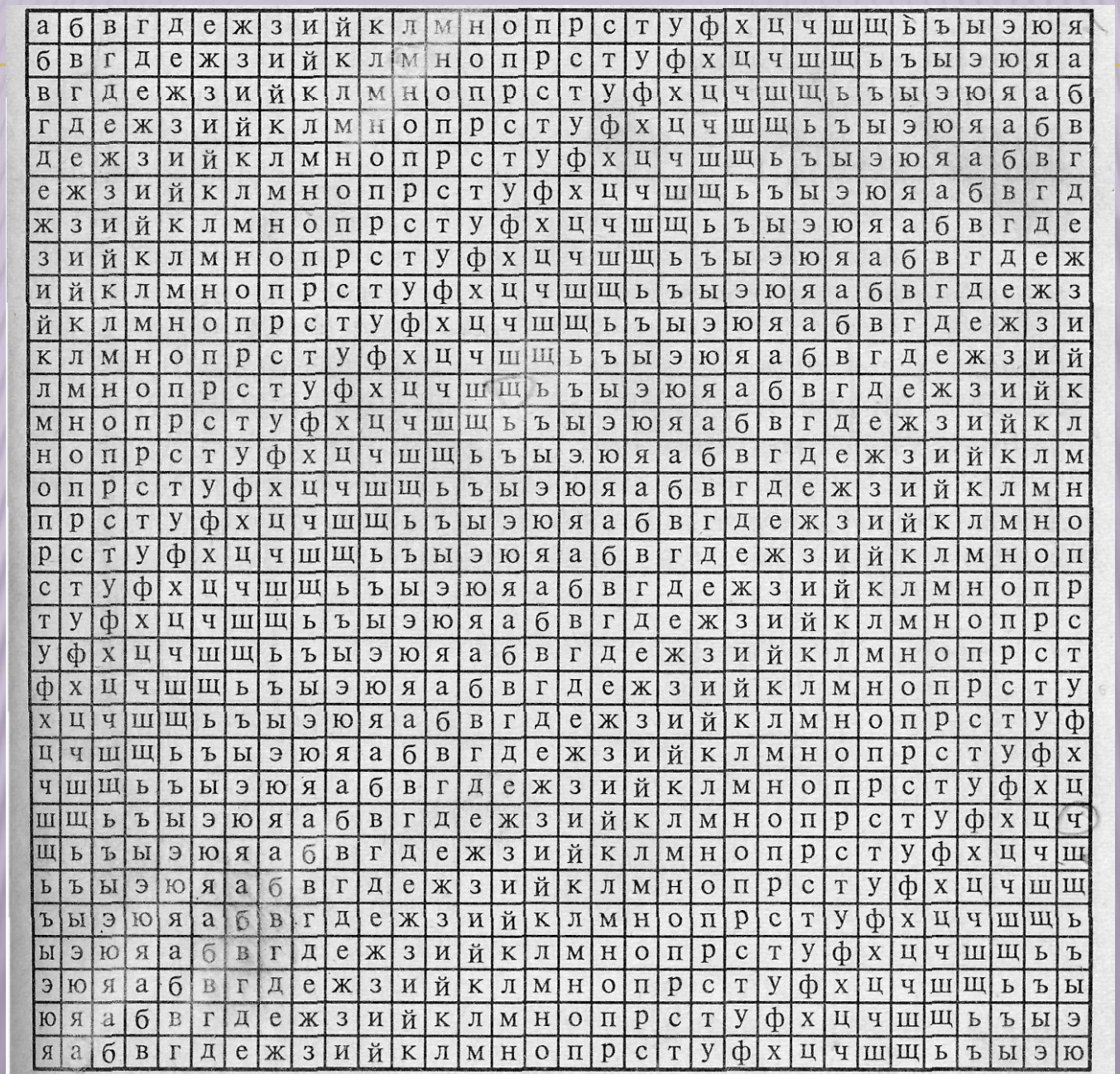
Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе Гражданской войны. Послания Конфедерации были далеки от секретных, и их противники регулярно взламывали сообщения. Во время войны командование Конфедерации полагалось на три ключевых словосочетания: «Manchester Bluff», «Complete Victory» и — так как война подходила к концу — «Come Retribution».

ГИЛБЕРТ ВЕРНАМ

Гилберт Вернам попытался улучшить взломанный шифр (он получил название шифр Вернама-Виженера в 1918 году), но, несмотря на его усовершенствования, шифр так и остался уязвимым к криптоанализу.

Однако работа Вернама в конечном итоге всё же привела к получению шифра, который по-настоящему трудно взломать.

ТАБЛИЦА ВИНЕЖЕРА



ПРОЦЕСС ШИФРОВАНИЯ

Таблица Виженера состоит из алфавита, циклически сдвинутого на один символ влево, однако, возможны и другие перестановки. Кроме того, первая строка может представлять собой алфавит, случайным образом перемешанный.

Процесс шифрования выглядит следующим образом:

- открытый текст (который надо зашифровать) записывается в строчку без пробелов,
- далее необходимо определить ключ. Виженер предлагал в качестве ключа использовать сам открытый текст, с добавлением к началу ключа символ, выбранный случайным образом.

Не обязательно следовать установленному правилу создателя шифра. В качестве ключа вполне возможно использовать и любую другую последовательность символов длиною **равной** длине открытого текста.

ПРОЦЕСС ШИФРОВАНИЯ

Для получения шифр-текста (криптограмма) берем первый символ открытого текста в качестве указателя строки в **Таблице Виженера**, а стоящую под ним букву – в качестве столбца. На пересечении этой пары из таблицы выписываем символ шифр-текста.

Далее повторяем эти действия для всех оставшихся символов.

Пример: рассмотрим шифрование открытого текста – «яблочный джем». В качестве ключа будем использовать сам открытый текст с добавлением в начала случайного символа – **«щ»**.

Повторюсь, что ключ может быть образован иным способом, к примеру просто перемешанный случайным образом открытый текст – «ляйычнбо жемд». Но ключ должен быть известен получателю шифра, то есть известна схема перемешивания открытого текста для того, чтобы он мог расшифровать криптограмму.

ПРОЦЕСС ШИФРОВАНИЯ

Так, теперь записываем открытый текст в строку без пробелов, а под ней также записываем ключ. Получаем:

открытый текст: ***я б л о ч н ы й д ж е м***
ключ: ***щ я б л о ч н ы й д ж е***

шифр-текст: ***ш а м щ е д й д н к л с***

Далее берем первую букву ключа определяем соответствующий ей столбец в **Таблице Виженера** и пробегаемся по нему сверху вниз пока не встретим первый символ шифр-текста. Как только встретили нужный символ, выписываем букву указывающую на эту строку – таким образом мы получаем первый символ открытого текста.

Проделываем те же действия для оставшихся символов ключа и шифр-текста

ПРОЦЕСС РАСШИФРОВАНИЯ

Для того, чтобы восстановить (расшифровать) открытый текст, необходимо знать шифр-текст и ключ.

Дешифрование производится следующим образом:

- находим в таблице Виженера строку, соответствующую первому символу ключевого слова (**щ**);
- в данной строке находим первый символ зашифрованного текста **(ш)**;
- столбец, в котором находится данный символ, соответствует первому символу исходного текста **(я);**
- следующие символы зашифрованного текста расшифровываются подобным образом.

Поближе к математике

Если буквы A-Z соответствуют числам 0-25, то шифрование/дешифрование можно записать в виде формул:

C-символ зашифрованного текста

P- символ исходного текста

K - ключ

Шифрование:

$C = (P + K) \bmod 26$

Дешифрование:

$P = (C - K) \bmod 26$

Шифр Виженера был незаслуженно забыт на долгое время. И многие по сей день под этим шифром понимают самый простой вариант с коротким ключевым словом и с таблицей, состоящей из обычных алфавитов.

ЗАДАНИЕ

1 Зашифруйте произвольное сообщение (не менее 40 знаков) с помощью шифра Вижинера.

Ключевым словом является ваша фамилия в именительном падеже.

2 Расшифруйте сообщение соседа!!