Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Криптографическая защита информации**

Студент: Николаева Е.В.

ФИТ 2 курс 5 группа

Преподаватель: Берников В.О.

Минск 2022

**Практическое занятие №5**

**Тема «****Криптографическая защита информации»**

**Цель**: Овладение навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.

**Теоретическое введение**

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Помимо этого, современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей.

В англоязычной литературе зашифрование / расшифрование – enciphering / deciphering.

Классификация алгоритмов шифрования

1. Симметричные (с секретным, единым ключом, одноключевые, single-key).

1.1. Потоковые:

· с одноразовым или бесконечным ключом (infinite-key cipher);

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

1.2.1. Шифры перестановки (permutation, P-блоки);

1.2.2. Шифры замены (substitution, S-блоки):

· моноалфавитные;

· полиалфавитные;

2. Асимметричные (с открытым ключом, public-key):

· Диффи-Хеллман DH (Diffie, Hellman);

· Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);

· Эль-Гамаль (ElGamal).

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в 3 этапа:

– отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);

– отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;

– получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется по блокам. Блочные шифры бывают двух основных видов:

– шифры перестановки (transposition, permutation, P-блоки);

– шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Различают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

– моноалфавитные (код Цезаря);

– полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например, в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций.



Рисунок 5.1 – Принцип замены

Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

В современных криптографических системах, как правило, используют оба способа шифрования (замены и перестановки). Такой шифратор называют составным (product cipher). Oн более стойкий, чем шифратор, использующий только замены или перестановки.

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания – другой (секретный). Эти ключи различны и не могут быть получены один из другого.

Схема обмена информацией такова:

– получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);

– отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;

– получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

**Шифрование с использованием системы Цезаря:**

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

http://kriptografea.narod.ru/13.png

http://kriptografea.narod.ru/14.png

где x — символ открытого текста

y — символ шифрованного текста

n — мощность алфавита (кол-во символов)

k — ключ.



Рисунок 5.2 – Алфавит

Пример:

Таблица 5.1 Шифр Цезаря

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сообщение** | | **Н** | **И** | **К** | **О** | **Л** | **А** | **Е** | **В** | **А** | **Е** | **В** | **Г** | **Е** | **Н** | **И** | **Я** |
| **Номер 1** | 15 | 10 | 12 | 16 | 13 | 1 | 6 | 3 | 1 | 6 | 3 | 4 | 6 | 15 | 10 | 33 |
| **Номер 1 + 19** | 1 | 29 | 31 | 2 | 32 | 20 | 25 | 22 | 20 | 25 | 22 | 23 | 25 | 1 | 29 | 19 |
| **Шифр** | **А** | **Ы** | **Э** | **Б** | **Ю** | **Т** | **Ч** | **Ф** | **Т** | **Ч** | **Ф** | **Х** | **Ч** | **А** | **Ы** | **С** |

Ответ: «Аыэбютчфт чфхчаыс», ключ 19

**Шифрование с использованием системы Трисемуса:**

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.5.2 изображена таблица с ключевым словом «ЗАЩИТА».

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **З** | **А** | **Щ** | **И** | **Т** | **Б** | **В** | **Г** |
| **Д** | **Е** | **Ж** | **Й** | **К** | **Л** | **М** | **Н** |
| **О** | **П** | **Р** | **С** | **У** | **Ф** | **Х** | **Ц** |
| **Ч** | **Ш** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |

Рисунок 5.2 – Таблица шифрозамен для шифра Трисемуса с ключевым словом «ЗАЩИТА»

Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца.

Например, исходное сообщение «НИКОЛАЕВА ЕВГЕНИЯ», зашифрованное – «ЦЙУЧФЕПМЕ ПМНПЦЙГ».

**Шифрование с использованием системы Виженера:**

В [шифре Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 32 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 32 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет вид:

НИКОЛАЕВАЕВГЕНИЯ(16)

Человек, посылающий сообщение, записывает ключевое слово («ЗАЩИТА») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

ЗАЩИТАЗАЩИТАЗАЩИ(16)

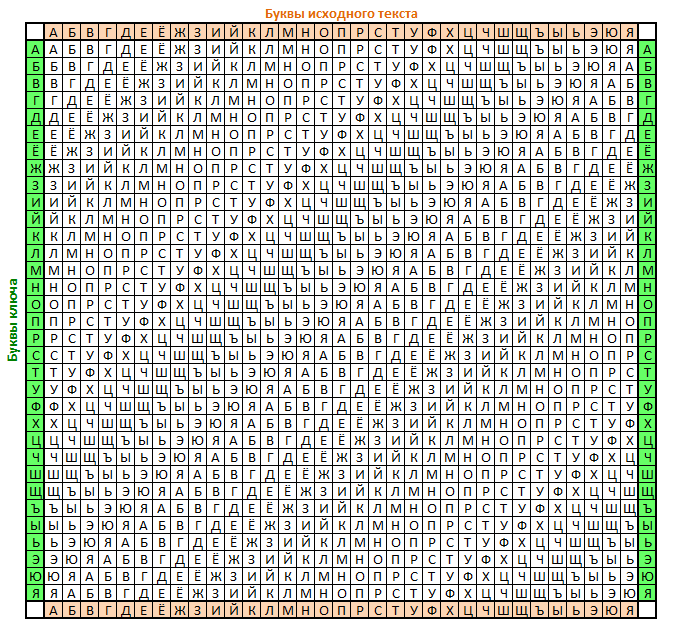


Рисунок 5.3 – Таблица Виженера для русского алфавита

Первый символ исходного текста Т зашифрован последовательностью З, которая является первым символом ключа. Первый символ З шифрованного текста находится на пересечении строки З и столбца Т в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста Р получается на пересечении строки А и столбца Р. Остальная часть исходного текста шифруется подобным способом.

*Исходный текст: НИКОЛАЕВАЕВГЕНИЯ*

*Ключ:* ЗАЩИТАЗАЩИТАЗАЩИ

*Зашифрованный текст: ХИДЧЮАМВЩНФГМНВЗ*

**Шифрование с использованием системы Плейфера:**

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в русских текстах обычно «Е» и «Ё» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 4х8 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Николаева Евгения» становится «НИ КО ЛА ЕВ АЕ ВГ ЕН ИЯ», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».

2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении.

Пример: Используем ключ «ЗАЩИТА», тогда матрица примет вид:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **З** | **А** | **Щ** | **И** | **Т** | **Б** | **В** | **Г** |
| **Д** | **Е** | **Ж** | **Й** | **К** | **Л** | **М** | **Н** |
| **О** | **П** | **Р** | **С** | **У** | **Ф** | **Х** | **Ц** |
| **Ч** | **Ш** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |

Рисунок 5.4 – Таблица шифрозамен для шифра Плейфера с ключевым словом «ЗАЩИТА»

НИ КО ЛА ЕВ АЕ ВГ ЕН ИЯ

Зашифруем сообщение «Николаева Евгения»

1. Биграмма НИ формирует прямоугольник, заменяем её на ЙГ.  
2. Биграмма КО формирует прямоугольник, заменяем её на ДУ.  
3. Биграмма ЛА расположена в одном столбце, заменяем её на ЕБ.  
4. Биграмма ЕВ формирует прямоугольник, заменяем её на МА.  
5. Биграмма АЕ расположена в одном столбце, заменяем её на ЕП.  
6. Биграмма ВГ формирует прямоугольник, заменяем её на ГЗ.  
7. Биграмма ЕН формирует прямоугольник, заменяем её на ЖД.

8. Биграмма ИЯ формирует прямоугольник, заменяем её на ГЫ.  
Получаем зашифрованный текст «ЙГ ДУ ЕБ МА ЕП ГЗ ЖД ГЫ»

Таким образом сообщение «Николаева Евгения» преобразуется в «ЙГДУЕБАМЕПГЗЖДГЫ»

Расщифровка:

Ключ: «**ПРАВИТЕЛЬ**», зашифрованный текст «**ъгчгл кыпргл бгнщзг»**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **П** | **Р** | **А** | **В** | **И** | **Т** | **Е** | **Л** |
| **Ь** | **Б** | **Г** | **Д** | **Ж** | **З** | **Й** | **К** |
| **М** | **Н** | **О** | **С** | **У** | **Ф** | **Х** | **Ц** |
| **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Э** | **Ю** | **Я** |

Рисунок 5.5 – Таблица шифрозамен для шифра Трисемуса с ключевым словом «**ПРАВИТЕЛЬ**»

Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца.

Например, исходное сообщение «**ъгчгл кыпргл бгнщзг**», зашифрованное – «САМАЯ ЛУЧШАЯ РАБОТА».

Вывод: в ходе этой практической работы, мы получили навыки работы с методами шифрования для криптографической защиты информации при передаче и хранении данных.