Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Основы защиты информации»

Отчёт по практическому занятию №4

Студент: Коренчук А.В.

ФИТ 2 курс 2 группа

Преподаватель: Ржеутская Н.В.

Минск 2022 г.

**Практическое занятие №5**

**«Криптографическая защита информации»**

Цель: овладение основными криптографическими алгоритмами симметричного шифрования

**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 поблочно. 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. Paзличают 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.



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 помощью аффинной системы подстановок Цезаря**

В данном методе используется ключ шифрования в виде пары целых чисел (A, K). Число A задает переход при шифровании вперед на A\*J букв, а число K – дополнительное смещение по алфавиту на K букв. Следовательно, аффинную систему подстановок Цезаря можно описать следующей формулой:

(5.1)

где A>=0, K<M, НОД(A,M) = 1, I – значение кода символа в результирующей таблице, J – значение кода символа в исходной таблице.

Например, пусть M = 26, A = 3, K = 5. Тогда, очевидно, НОД (3,26) = 1, и мы получаем следующее соответствие между числовыми кодами букв:

Таблица 5.1– таблица кодов символов

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| J | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 3t+5 | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 1 | 4 | 7 | 10 | 13 | 16 | 19 | 22 | 25 | 2 |

Преобразуя числа в буквы английского языка, получаем следующее соответствие для букв открытого текста и шифр текста:

Таблица 5.2– таблица символов

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| F | I | L | O | R | U | Х | А | D | G | J | М | Р | S | V | Y | В | Е | Н | K | N | Q | Т | W | Z | C |

Функция дешифровки выглядит следующим образом:

(5.2)

**Шифр 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.4.7 изображена таблица с ключевым словом «ДЯДИНА».

Таблица 5.3 – Таблица шифрозамен для шифра Трисемуса



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 «АБРАМОВ», зашифрованное – «ЖЗЦЖУФЙ».

**Шифр Плейфейра**

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8 или 6х6), 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 английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» 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 5х5 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», 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.

**Шифр Вижинера**

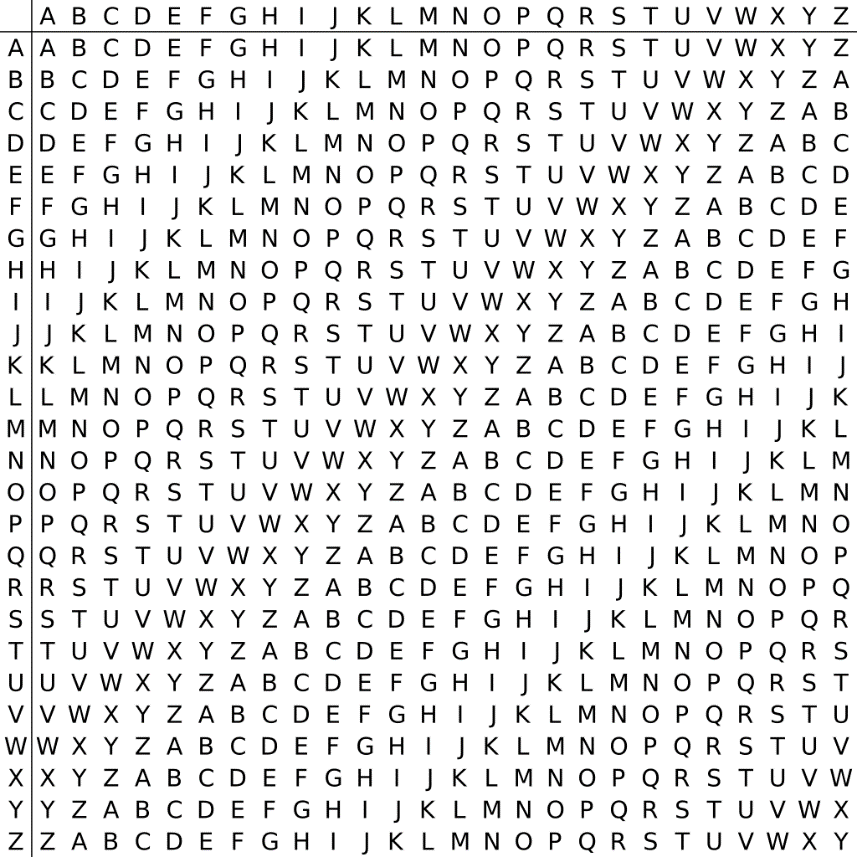
В [шифре Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров 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 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет вид:

ATTACKATDOWN

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

LEMONLEMONLE

Таблица 5.4 – Таблица шифрозамен для шифра Вижинера



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

# **Задание для выполнения**

Зашифровать сообщение с использованием шифра Цезаря, Трисемуса, Плейфейра и Вижинера и полученного секретного ключа (по номеру варианта и ключевому слову «Защита»). В качестве сообщения использовать свою Фамилию Имя Отчество.

**Шифр Цезаря**

Необходимо зашифровать сообщение «Коренчук Андрей Васильевич» с помощью шифра Цезаря и ключа k=13. Исходный алфавит русского языка представлен в таблице 7.2.

Таблица 7.2 – алфавит русского языка и его смещение на один символ

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

Следовательно, сообщение «Коренчук Андрей Васильевич», зашифрованное с использованием шифра Цезаря и заданного ключа k=13, будет иметь следующий вид: «Чыэсьдач Мърэсц Омюхшихсод».

**Шифр Трисемуса**

Необходимо зашифровать сообщение «Коренчук Андрей Васильевич» с помощью шифра Трисемуса и ключевого слова «Защита». Под ней

Таблица 7.3 – Таблица Трисумеса

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| з | а | щ | и | т | б |
| в | г | д | е | ё | ж |
| й | к | л | м | н | о |
| п | р | с | т | у | ф |
| х | ц | ч | ш | ъ | ы |
| ь | э | ю | - | - | - |

Следовательно, сообщение «Коренчук Андрей Васильевич», зашифрованное с использованием шифра Трисемуса и заданного ключевого слова «Защита», будет иметь следующий вид: «Рфцмуюр Гулцмп Йгчесмйею».

**Шифр Плейфейра**

Необходимо зашифровать сообщение «Коренчук Андрей Васильевич» с помощью шифра Плейфейра и ключевого слова «Защита». Промежуточная биграмма имеет «ко-ре-нч-ук-ан-др-ей-ва-си-ль-ев-ич».

Таблица 7.4 -Таблица Плейфейра

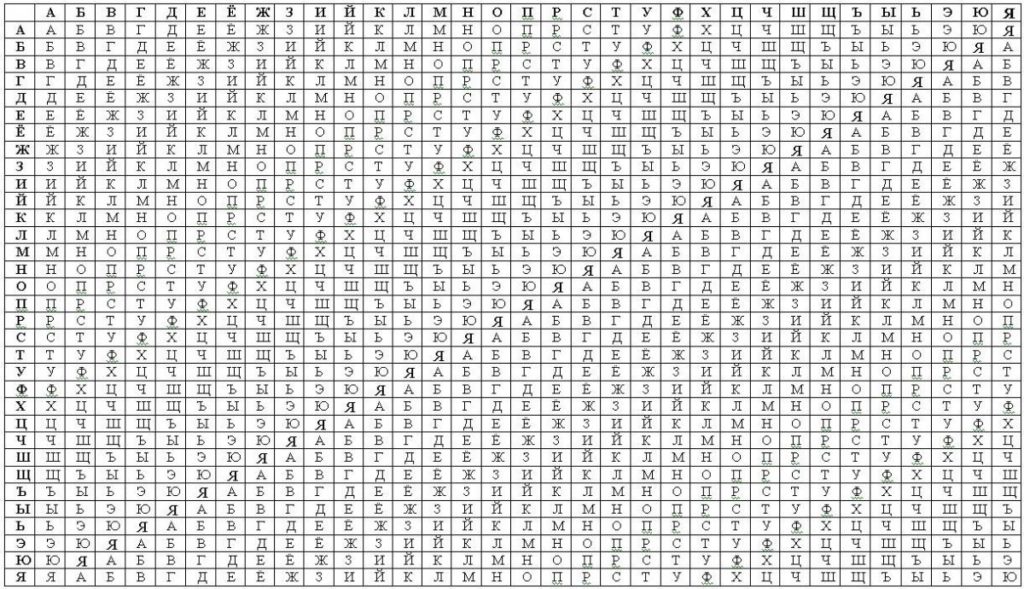
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| з | а | щ | и | т | б | в | г |
| д | е | ж | й | к | л | м | н |
| о | п | р | с | у | ф | х | ц |
| ч | ш | ъ | ы | ь | э | ю | я |

Следовательно, сообщение «Коренчук Андрей Васильевич», зашифрованное с использованием шифра Плейфейра и заданного ключевого слова «Защита», будет иметь следующий вид: «ду-пж-дя-ьу-ге-ож-жк-щг-ый-кэ-ам-зы».

**Шифр Вижинера**

Необходимо зашифровать сообщение «Коренчук Андрей Васильевич» с помощью шифра Вижинера и ключевого слова «Защита». Промежуточный ключ имеет вид «защитазащитазащитазащитазащ» (человек, посылающий сообщение, записывает ключевое слово («защита») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста).

Таблица 7.5-Таблица Виженера



Следовательно, сообщение «КоренчукАндрейВасильевич»

защитазащитазащитазащитаза

, зашифрованное с использованием шифра Виженера и заданного ключевого слова «Защита», будет иметь следующий вид: «тойначык щццрмй ыидиуьюкыч».

# **Индивидуальное задание**

Расшифровать следующие сообщения.

Таблица 7.6-Вариант выполнения задания

|  |  |  |  |
| --- | --- | --- | --- |
| № варианта | Сообщение | Способ | Ключ |
| 13 | \_яетож\_нксучнтуотдеыужбьатйдны\_,  с\_ао\_о\_яс,\_ндк,е\_иаиу\_ккддндаруто\_  а\_еди.в\_нта\_ \_ахе:\_ | Расшифровать с помощью **Одиночной перестановки по ключу** | Счастье  (Таблица  12х7) |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **с** | **ч** | **а** | **с** | **т** | **ь** | **е** |
| 3 | 6 | 1 | 4 | 5 | 7 | 2 |
| Е | Ж | \_ | Т | О | \_ | Я |
| С | Н | Н | У | Ч | Т | К |
| Т | Ы | У | Д | Е | У | О |
| Ь | Й | Ж | А | Т | Д | Б |
| \_ | \_ | Н | , | С | А | Ы |
| О | С | О | \_ | Я | , | \_ |
| Д | Е | \_ | К | , | \_ | Н |
| И | К | И | У | \_ | К | А |
| Н | Р | Д | Д | А | У | Д |
| \_ | Е | Т | А | \_ | Д | О |
| В | Т | И | \_ | Н | А | . |
| А | : | \_ | Х | Е | \_ | \_ |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| а | е | с | с | т | ч | ь |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| \_ | я | е | т | о | ж | \_ |
| н | к | с | у | ч | н | т |
| у | о | т | д | е | ы | у |
| ж | б | ь | а | т | й | д |
| н | ы | \_ | , | с | \_ | а |
| о | \_ | о | \_ | я | с | , |
| \_ | н | д | к | , | е | \_ |
| и | а | и | у | \_ | к | к |
| д | д | н | д | а | р | у |
| т | о | \_ | а | \_ | е | д |
| и | . | в | \_ | н | т | а |
| \_ | \_ | а | х | е | : | \_ |

Результат: Есть один важный секрет: нужно идти туда, куда хочется, а не туда, куда якобы надо.

**Вывод:** в ходе лабораторной работы были изучены основные криптографические алгоритмы симметричного шифрования.