Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическое задание №4.1**

**Тема «Криптографическая защита информации»**

Руководитель: Ржеутская Н. В.

Выполнил:

Студент 2 курса 8 группы ФИТ

Солодкий Денис Викторович

Минск 2022

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

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

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).

Шифр Цезаря

Это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Ключ: 13 Сообщение: Солодкий ДВ

Исходный алфавит:   
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Шифрованный алфавит:  
МНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛ

Зашифрованное сообщение: **ЭЪЧЪПШХЦ ПО**

Шифр Трисемуса

Представляет собой усовершенствованный шифр Цезаря, то есть шифр подстановки. По алгоритму шифрования, каждый символ сообщения смещается на символ, отстающий от данного на некоторый шаг.

Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы.

Функция: k = p, k – смещение, p – позиция буквы в сообщении  
Сообщение: Солодкий ДВ

Алфавит:



Зашифрованное сообщение: **СПНСЗПОР ЛК**

Шифр Плейфейра

Представляет собой ручную симметричную технику шифрования, в которой впервые использована замена биграмм. Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в шифре подстановки.

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу.

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.

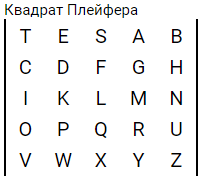
Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила.

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Ъ», зашифровываем новую пару символов и продолжаем.
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.

Ключ: test Сообщение: Solodkiy DV

Разобьём сообщение на биграммы: So lo dk iy DV

Используем ключ «test», тогда матрица примет вид:



Зашифр. сообщение: TQ IQ KP MV CW

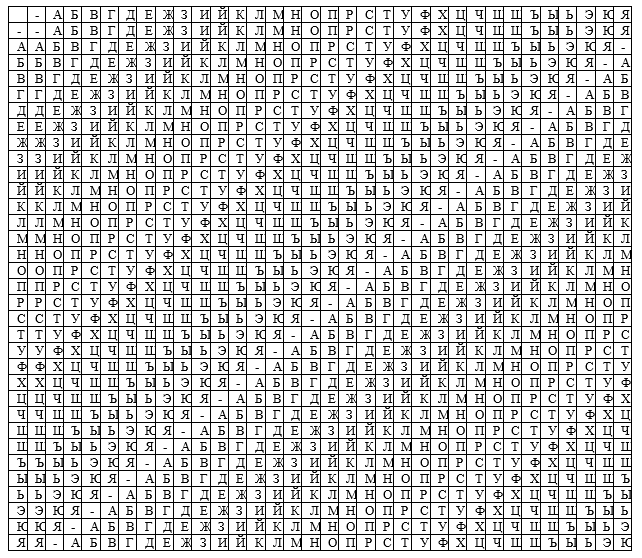
Шифр Вижинера

Представляет собой метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены.

Ключ: Защита Сообщение: Солодкий ДВ

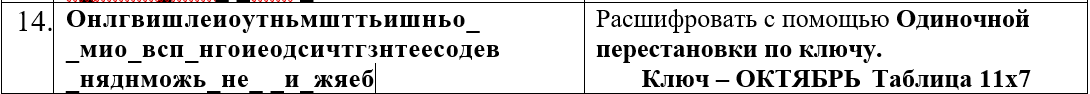
При шифровке Вижинера ключ записывается заново, пока не будет достигнута длина сообщения.

Полученная ключевая фраза: ЗащитаЗащ  
 Солодкий ДВ



Зашифрованное сообщение: щоечцкрй эк

**Расшифровать сообщение:**



Ключом к расшифрованию методом одиночной перестановки по ключу служит слово (в нашем случае «Октябрь»). Заданное сообщение: «Онлгвишлеиоутньмшттьишньо\_\_мио\_всп\_нгоиеодсичтгзнтеесодев\_няднможь\_не\_ \_и\_жяеб», размерность 11х7.

Для этого нам надо написать ключевое слово в алфавитном виде и указать порядок нумерациями (таблица 1). В исходной таблице расставляем цифры по возрастанию, чтобы ключевое слово было выстроено в ряд по алфавиту и используем для этого **таблицу 1**. Вписываем буквы по горизонтали, которые в заданном сообщении (таблица 2).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| О | К | Т | Я | Б | Р | Ь |

Таблица 1 – Порядок букв

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Б** | **К** | **О** | **Р** | **Т** | **Ь** | **Я** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **О** | **Н** | **Л** | **Г** | **В** | **И** | **Ш** |
| **Л** | **Е** | **И** | **О** | **У** | **Т** | **Н** |
| **Ь** | **М** | **Ш** | **Т** | **Т** | **Ь** | **И** |
| **Ш** | **Н** | **Ь** | **О** | **\_** | **\_** | **М** |
| **И** | **О** | **\_** | **В** | **С** | **П** | **\_** |
| **Н** | **Г** | **О** | **И** | **Е** | **О** | **Д** |
| **С** | **И** | **Ч** | **Т** | **Г** | **З** | **Н** |
| **Т** | **Е** | **Е** | **С** | **О** | **Д** | **Е** |
| **В** | **\_** | **Н** | **Я** | **Д** | **Н** | **М** |
| **О** | **Ж** | **Ь** | **\_** | **Н** | **Е** | **\_** |
| **\_** | **И** | **\_** | **Ж** | **Я** | **Е** | **Б** |

Таблица 2 – Исходная таблица

Для расшифрования сообщения при одиночной перестановке по ключу, расставляем буквы ключевого слова «Октябрь» с нумерациями (таблица 1) и вписываем сообщение по столбцам используя **таблицу 2**.

Расшифрованное сообщение: **лишь очень немногие живут сегодняшним днем большинство готовится жить позднее.**

Вывод: для защиты информации используется шифровка – процесс приведения исходного текста в набор символов, определяемых некоторым правилом. Существует множество методов шифровки. У каждой шифровки есть дешифровка – процесс приведения набора символов в исходный текст, зная ключ или последовательность действий. Овладел основными криптографическими алгоритмами симметричного шифрования.