**Вопросы к лабораторной работе №4**

1. В чем заключается основная идея криптографических преобразований на основе шифров замены?

Сущность подстановочного шифрования состоит в том, что исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

1. Привести классификационные признаки и дать сравнительную характеристику разновидностям подстановочных шифров.

1. Моноалфавитные (простые подстановочные) шифры:

- В таких шифрах каждая буква открытого текста заменяется одной и той же буквой или символом в зашифрованном тексте.

2. Полиграммные шифры:

- В этих шифрах сочетания нескольких символов (биграмм, триграммы и т. д.) заменяются другими сочетаниями.

3. Омофонические (многозвучные) шифры:

- В таких шифрах каждая буква открытого текста может быть заменена одним из нескольких символов.

4. Полиалфавитные шифры:

- Эти шифры используют несколько алфавитов для шифрования, применяя разные подстановки в зависимости от позиции символа в тексте или ключа.

1. Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?

Для русского и белорусского алфавитов, состоящих из 33 и 32 букв соответственно, можно создать 32 различные разновидности шифра Цезаря, где сдвиг будет варьироваться от 1 до 32 (или от 1 до 31 для белорусского языка).

Таким образом, для русского языка можно создать 32 различные разновидности шифра Цезаря, а для белорусского - 31.

1. Найти ключ шифра, с помощью которого получен шифртекст: «byajhvfwbjyyfzgjcktljdfntkmyjcnm».
2. Расшифровать (с демонстрацией каждого шага алгоритма) текст Сi = «qrscqcocqclc», зашифрованный аффинным шифром Цезаря при N = 26, а = 3, b = 5.

Y = a\*x + bmodN

venividicici

1. Зашифровать и расшифровать свою фамилию (на основе кириллицы), используя аффинный шифр Цезаря.
2. Можно ли использовать в качестве ключевого в шифре Виженера слово, равное по длине открытому тексту? Обосновать ответ.

Да, можно использовать в качестве ключа в шифре Виженера слово, равное по длине открытому тексту. Основное преимущество использования ключа, равного по длине открытому тексту, заключается в том, что каждая буква ключа будет использоваться для шифрования соответствующей буквы открытого текста. Это приводит к созданию множества различных шифрованных текстов, что делает криптоанализ сложнее.

1. По какому признаку можно определить, что текст зашифрован шифром Плейфера?

Одним из характерных признаков, по которому можно определить, что текст зашифрован шифром Плейфера, является наличие символов, расположенных в парах. В шифре Плейфера каждая пара букв открытого текста заменяется парой других букв из шифрового алфавита в соответствии с определенными правилами. Поэтому зашифрованный текст будет содержать много пар символов, что отличает его от текста, зашифрованного моноалфавитным шифром. Кроме того, текст, зашифрованный шифром Плейфера, может содержать определенные характерные биграммы или триграммы, которые встречаются с намного большей частотой, чем другие комбинации букв, что может быть использовано для его идентификации. Таким образом, наличие парных символов и характерных биграмм или триграмм в тексте может указывать на то, что он зашифрован шифром Плейфера.

1. Имеются ли предпочтения в выборе размеров таблицы Трисемуса для виртуального алфавита мощностью 40: 4×10; 10×4; 5×8; 8×5; 2×20; 20×2?

Важно, чтобы таблица была эффективно заполнена символами из алфавита, чтобы обеспечить наиболее эффективное шифрование и минимизировать вероятность повторений символов в таблице. Таблицы размером 5x8 и 8x5 позволяют более равномерно распределить символы алфавита по ячейкам.

1. Охарактеризовать основные виды атак на шифры.

**Атака с известным шифртекстом (ciphertext only attack).** Предполагается, что противник знает алгоритм шифрования, у него имеется набор перехваченных шифрограмм, но он не знает секретный ключ.

**Атака с выбором шифртекста (chosen cipher text attack**). Криптоаналитик имеет возможность выбрать необходимое количество шифрограмм и получить соответствующие им открытые тексты. Используя полученные данные, он может попытаться восстановить секретный ключ.

**Адаптивная атака с выбором шифртекста (adaptive chosen ciphertext attack).** Криптоаналитик имеет возможность выбирать новые шифрограммы для расшифрования с учетом того, что ему известна некоторая информация из предыдущих сообщений.

**Атака с известным открытым текстом (known plaintext attack).** То же, что и предыдущая, но противник для некоторых шифрограмм получает в свое распоряжение соответствующие им открытые тексты.

**Атака с выбором открытого текста (chosen plaintext attack).** Криптоаналитик обладает некоторыми открытыми текстами и соответствующими шифртекстами. Кроме того, он имеет возможность зашифровать несколько предварительно выбранных открытых текстов (до начала атаки).

**Атака на основе связанных ключей (related key attack).** Криптоаналитик знает не сами ключи, а некоторые различия (соотношения) между ними; реальные криптосистемы используют разные ключи, связанные известным соотношением, например, для каждого нового сообщения предыдущее значение ключа увеличивается на единицу или преобразуется на основе операции сдвига.

**Атака с выбором ключа (chosen key attack).** Криптоаналитик задает часть ключа, а на оставшуюся часть ключа выполняет атаку на основе связанных ключей.

1. Сравнить криптостойкость шифра Цезаря и шифра Виженера.

Шифр Цезаря очень уязвим для частотного анализа, поскольку каждая буква открытого текста заменяется на одну и ту же букву шифрованного текста. Это позволяет криптоаналитику анализировать частоту появления букв и проводить атаки на основе известной статистики языка.

Шифр Виженера усложняет криптоанализ, поскольку каждая буква открытого текста может быть заменена разными символами в зависимости от позиции в тексте и ключа. Это затрудняет проведение частотного анализа и других классических методов криптоанализа.

Шифр Цезаря имеет очень ограниченное ключевое пространство, поскольку ключом является только число от 1 до N (N – мощность алфавита). Это означает, что всего существует N возможных вариантов шифра, что делает его очень уязвимым для перебора ключа.

В отличие от этого, шифр Виженера использует ключевое слово, которое может быть длинным и случайным. Это создает значительно большее ключевое пространство, что делает шифр Виженера гораздо более стойким к атакам перебора ключа.

1. Охарактеризовать основные методы взлома подстановочных шифров.

• полный перебор ключей (лобовая атака, bruteforce attack);

• атака по словарю, перебор ключей по словарю (dictionary attack); применяется часто для взлома паролей;

• частотный криптоанализ – метод взлома шифра, основывающийся на предположении о существовании зависимости между частотой появления символов алфавита в открытых сообщениях и соответствующих шифрозамен в шифрограммах.