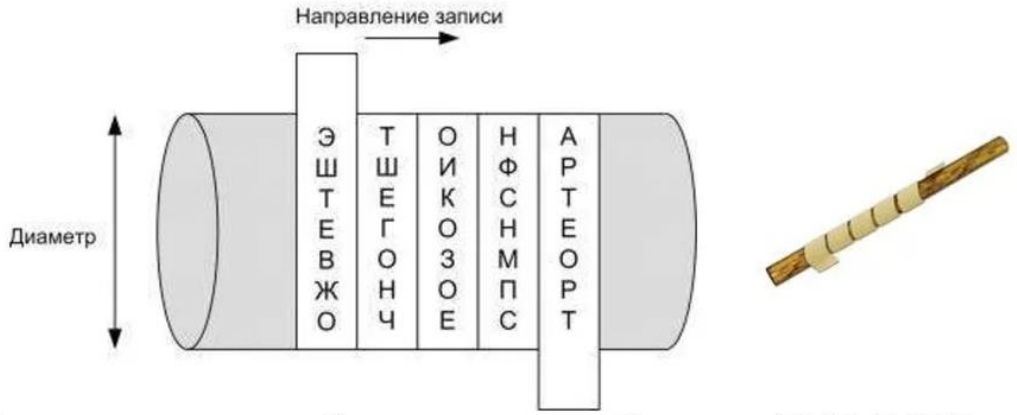
## Шифр «Сцитала» (Scytale)




В результате преобразования сообщения **ЭТО НАШ ШИФРТЕКСТ, ЕГО НЕВОЗМОЖНО ПРОЧЕСТЬ** при использовании шифра «скитала» получится **ЭШТЕВ ЖОТШЕ ГОНЧО ИКОЗО ЕНФСН МПСАР ТЕОРТ**.

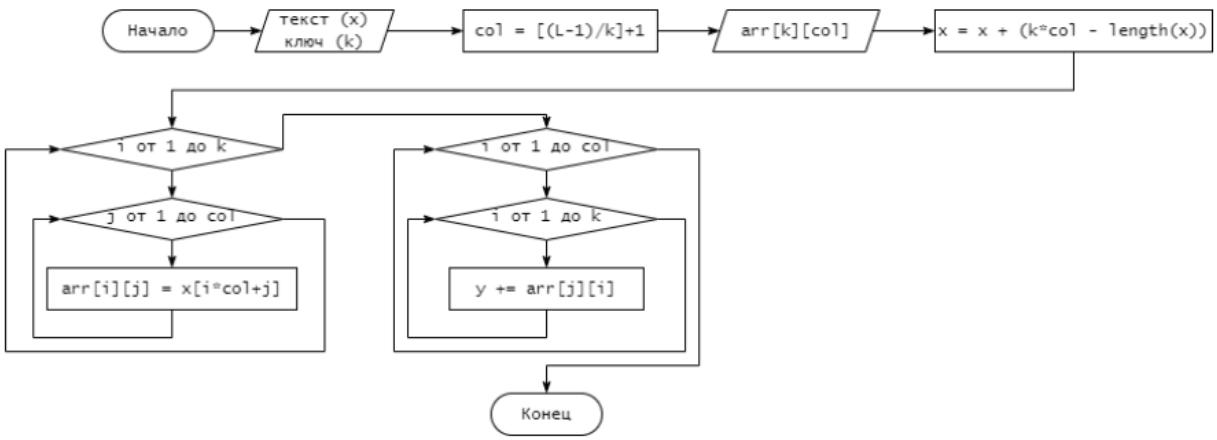
**Характеристика:**

- Ключ: диаметр палочки или количество граней
- Тип шифра: перестановка
- Сложность атаки грубой силы «BruteForce»: O(L), где L – длина шифротекста

**Алгоритм шифрования:**

1) первые $n$ символов выписываются в первую строку слева направо (в примере выше: «*ЭТОШИ*»);
2) следующие $n$ символов выписываем во вторую строчку пока её не заполним и т.д.;
3) если все символы выписаны, а остались незаполненные ячейки, заполняем их пробелами или любыми другими символами по договоренности (например, для сообщения «*НАС АТАКУЮТ*» мы получаем таблицу (см. ниже), где $n = 4$, $m = 3$ и звездочка стоит на месте недостающего символа);
4) если выписаны не все символы, а таблица заполнена, значит, при выборе размеров допущена ошибка;
5) теперь разворачиваем текст по столбцам («*НАУАТЮСАТ_К*»* – в примере ниже)[3][4].

```
_____________________________
  |   |   |   |   |   |
  |__| Н | А | С |__ |__
     | А | Т | А | К |   |
     | У | Ю | Т | * |   |
_____________________________
```



Пример:

Открытый текст: Сообщение, которое хотим зашифровать (36 символов)

Ключ: 7

Алгоритм:

Сначала определим количество столбцов: ((Длина текста - 1) / ключ) + 1 = ((36 – 1) / 7) + 1 = 6.

Записываем наш открытый текст по строкам.

| | | | | | |
|---|---|---|---|---|---|
| С | о | о | б | щ | е |
| н | и | е | , | _ | к |
| о | т | о | р | о | е |
| _ | х | о | т | и | м |
| _ | з | а | ш | и | ф |
| р | о | в | а | т | ь |
| * | * | * | * | * | * |
| | | | | | |

Так как это лента, то читаем по столбцам: Сно__р*оитхзо*оеооав*б,ртша*щ_оиит*екемфь*.

**Ответ:** Сно__роитхзооеооавб,ртшащ_оиитекемфь

**Алгоритм дешифрования:**

Мы знаем, что ключ = 7, тогда можно читать через каждые 6 символов или же воспользоваться формулой ((длина текста - 1) / ключ) и восстановить таблицу.

Записываем наш шифротекст по столбцам, ответ читаем по строкам.

| | | | | | |
|---|---|---|---|---|---|
| С | о | о | б | щ | е |
| н | и | е | , | _ | к |
| о | т | о | р | о | е |
| _ | х | о | т | и | м |
| _ | з | а | ш | и | ф |
| р | о | в | а | т | ь |
| * | * | * | * | * | * |

**Атака «BruteForce»**

Атака заключается в полном переборе. Перебирается от 2 до длины текста до тех пор, пока не получим осмысленный текст.

## Шифр Цезаря

**Описание:**

Шифрование основано на использовании таблицы замен: в одну строку таблицы записываются буквы алфавита, а в другую – тот же алфавит, но сдвинутый влево на выбранное значение смещения. Символ, находящийся под символом исходного алфавита, – это заменяющий символ в шифротексте.

**Характеристика:**

- Ключ: смещение
- Тип шифра: замена (аддитивный шифр замены)
- Сложность атаки грубой силы «BruteForce»: O(A), где A – мощность алфавита

**Алгоритм шифрования:**

Записываем исходный алфавит. Под ним записываем алфавит для шифрования сдвигая буквы на число равное ключу. Смотрим на исходный алфавит, записываем букву из алфавита для шифрования (пробелы и знаки пунктуации не заменяются или добавляются в алфавит и также сдвигаются), получаем шифротекст.

Пусть

- $p$ — номер в алфавите той буквы, которая была взята из открытого текста (plain text);
- $c$ — номер в алфавите той буквы, которая была взята из шифрованного текста (cipher text) буквы;
- $n$ — количество имеющихся в алфавите букв, мощность алфавита;
- $k$ — ключ, сдвиг (отрицательное число — сдвиг влево; ноль — отсутствие сдвига; положительное число — сдвиг вправо).

- шифрование:

$$c = (p + k) \mod n;$$

Пример:

Открытый текст: КРИПТОГРАФИЯ

Ключ: 3

Алгоритм:

Составляем алфавит для шифрования.

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

Сопоставляем буквы. Получаем шифротекст – НУМТХЖУГЧМВ

**Алгоритм дешифрования:**

Мы знаем, что ключ = 3, сдвигаем исходный алфавит на значение равное ключу. Под ним записываем исходный алфавит. Сопоставляем буквы. Получаем ответ.

Пусть

- $p$ — номер в алфавите той буквы, которая была взята из открытого текста (plain text);
- $c$ — номер в алфавите той буквы, которая была взята из шифрованного текста (cipher text) буквы;
- $n$ — количество имеющихся в алфавите букв, мощность алфавита;
- $k$ — ключ, сдвиг (отрицательное число — сдвиг влево; ноль — отсутствие сдвига; положительное число — сдвиг вправо).

- дешифрование:

$$p = (c - k) \mod n.$$

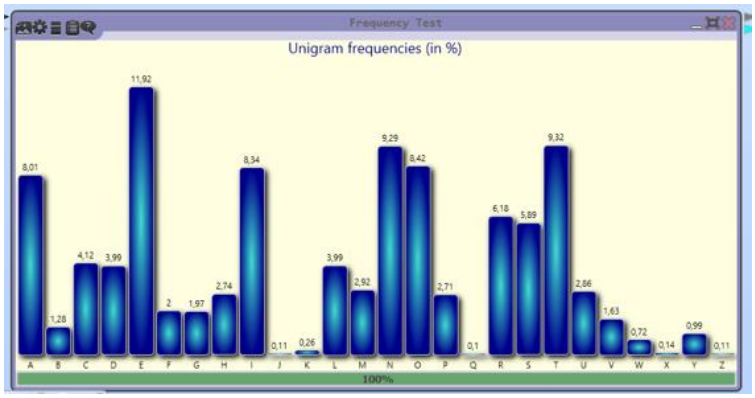
**Атака**

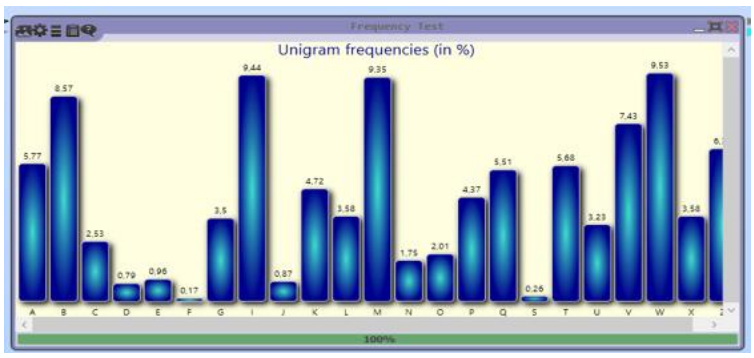
- **«BroutForce»**

  Полный перебор сдвигов. Сдвигаем алфавит и дешефруем сообщение. Сдвигаем до тех пор, пока не получим осмысленный текст. Тем самым находим ключ, который является сдвигом.

- **Частотный анализ**

  По эталонному тексту(требования: текст того же языка, той же тематики, достаточной длины) строим диаграмму частотности букв (гистограмму), потом строим гистограмму по зашифрованному тексту. Сопоставляем две диаграммы, замечаем смещение распределения, определяем сдвиг.




Сдвиг равен 8.

## Шифр моноалфавитной подстановки (Substitution)

**Описание:**

Шифрование основано на использовании таблицы замен: в одну строку таблицы записываются буквы алфавита языка исходного сообщения, а в другую строку – символы, на которые заменяются буквы исходного сообщения.

Первым шагом создания нового алфавита служит удаление всех повторяющихся букв, которые присутствуют в кодовом слове. Затем из алфавита удаляются все буквы кодового слова. На заключительном шаге кодовое слово внедряется в алфавит со смещением первого элемента.

**Характеристика:**

- Ключ: кодовое слово и смещение
- Тип шифра: замена
- Сложность атаки грубой силы «BruteForce»: O(A!), где A – мощность алфавита (проверка всевозможных перестановок)

**Алгоритм шифрования:**

1. Записываем исходный алфавит.
2. Из кодового слова удаляем повторяющиеся буквы.
3. Из исходного алфавита удаляем буквы, содержащиеся в кодовом слове.
4. Берем первые n букв в новом алфавите (n – сдвиг), добавляем кодовое слово, добавляем оставшиеся буквы алфавита (пробелы и знаки пунктуации не заменяются или добавляются в алфавит и также сдвигаются). Получаем алфавит для шифрования.

Пример:

Открытый текст: HELLO WORLD

Ключ: 5 и CRYPTOGRAPHY

Алгоритм:

1. Записываем исходный алфавит.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

2. Из кодового слова удаляем повторяющиеся буквы.

   CRYPTOGRAPHY --> CRYPTOGAH

3. Из исходного алфавита удаляем буквы, содержащиеся в кодовом слове.

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | B | | D | E | F | | | I | J | K | L | M | N | | | Q | | S | | U | V | W | X | | Z |

4. Берем первые n букв в новом алфавите (n – сдвиг),

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | D | E | F | I | | | | | | | | | | | | | | | | | | | | |

добавляем кодовое слово,

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | D | E | F | I | C | R | Y | P | T | O | G | A | H | | | | | | | | | | | |

добавляем оставшиеся буквы алфавита (пробелы и знаки пунктуации не заменяются или добавляются в алфавит и также сдвигаются). Получаем алфавит для шифрования.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | D | E | F | I | C | R | Y | P | T | O | G | A | H | J | K | L | M | N | Q | S | U | V | W | X | Z |

Шифруем: HELLO WORLD --> YIGGJ VJMGF

**Алгоритм дешифрования:**

Нам известны смещение и кодовое слово. Составляем по тому же принципу алфавит. Сопоставляем буквы.

**Атака**

- **«BroutForce»**
- **Частотный анализ (Frequency Analysis)**
- **Атака по известному открытому тексту (Known Plaintext Attack)**

Эта атака применяется, когда часть исходного текста (открытого текста) известна криптоаналитику. Зная, какие символы соответствуют известным фрагментам текста, можно частично расшифровать шифр и затем использовать эту информацию для расшифровки оставшейся части сообщения.

Процесс атаки по известному открытому тексту:

- Использование известных фрагментов открытого текста для определения соответствий между шифрованными и открытыми символами.

- Расширение этих соответствий на остальной текст для его полного расшифрования.

## Шифр двойной перестановки (Permutation/Transposition)

**Описание:**

В основе шифра лежит перестановка матричного представления открытого текста. Перестановки можно выполнять по строкам или по столбцам, а также обоими способами.

**Характеристика:**

- Ключ: две перестановки или два кодовых слова
- Тип шифра: перестановка
- Сложность атаки грубой силы «BruteForce»: O(n! * m!), где n и m – длина ключей

**Алгоритм шифрования:**

1. Составляем таблицу. Индексируем ее двумя кодовыми словами по столбцу и строке. Записываем открытый текст по строкам (ОГРАНИЧЕНИЕ НА ТЕКСТ: он должен полностью заполнять таблицу)
2. Переставляем столбцы по возрастанию цифр или в алфавитном порядке.
3. Переставляем строки по возрастанию цифр или в алфавитном порядке.
4. Читаем по строкам, получаем шифротекст.

Пример:

Открытый текст: ПРИМЕРМАРШРУТНЫЙШИФР

Ключ: (5, 4, 3, 1, 2) и (2, 4, 3, 1)

Алгоритм:

1. Записываем текст в матрицу

| | 5 | 4 | 3 | 1 | 2 |
|---|---|---|---|---|---|
| 2 | п | р | и | м | е |
| 4 | р | м | а | р | ш |
| 3 | р | у | т | н | ы |
| 1 | й | ш | и | ф | р |

2. Переставляем столбцы:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 2 | м | е | и | р | п |
| 4 | р | ш | а | м | р |
| 3 | н | ы | т | у | р |
| 1 | ф | р | и | ш | й |

3.Переставляем строки:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | ф | р | и | ш | й |
| 2 | м | е | и | р | п |
| 3 | н | ы | т | у | р |
| 4 | р | ш | а | м | р |

4.Читаем по строкам

Ответ: ФРИШЙМЕИРПНЫТУРРШАМР

**Алгоритм дешифрования:**

Нам известны ключи. Сначала делим строку на блоки, равные количеству столбцов, записываем в строки согласно порядку в ключе. Потом аналогично меняем столбцы. Действие полностью обратное шифрованию.

**Атака**

- **Частотный анализ (Frequency Analysis)**

  **Проблемы:** Метод сложен при использовании двойной перестановки, поскольку комбинация двух перестановок сильно искажает исходный текст, что затрудняет применение этого анализа напрямую.

- **Атака с известным открытым текстом (Known Plaintext Attack)**

  В этой атаке предполагается, что у злоумышленника есть доступ к фрагменту исходного текста и соответствующему фрагменту зашифрованного текста. Это позволяет ему выяснить ключи перестановок. Основные этапы:

  - Идентификация соответствий между фрагментами исходного и зашифрованного текста.
  - Восстановление ключей перестановки путем сравнения позиций символов.

  **Проблемы:** Данная атака требует наличия хотя бы небольшого фрагмента исходного текста, что не всегда доступно.

- **Криптоанализ на основе модели текста**

  Использование моделей текста (например, биграмм или триграмм) может помочь в атаках на шифр двойной перестановки. Например,

вероятностные модели текста позволяют оценить, насколько вероятно, что конкретная перестановка соответствует зашифрованному тексту.

- Создание статистической модели на основе обычного текста (например, вероятности появления биграмм).
- Применение перестановок к зашифрованному тексту и оценка вероятностей в соответствии с моделью.
- Поиск перестановок, которые дают текст с максимально правдоподобной структурой.

**Проблемы:** Требует значительных вычислительных ресурсов и данных для обучения модели.

- **Брутфорс (Перебор)**

## Шифр Виженера (Vigenere)

**Описание:**

Многоалфавитная перестановка с использованием ключевого слова. Можно сказать, что это несколько шифров Цезаря.

**Характеристика:**

- Ключ: кодовое слово
- Тип шифра: полиалфавитная замена
- Сложность атаки грубой силы «BruteForce»: O(A^k), где A – мощность алфавита, k – длина ключа

**Алгоритм шифрования:**

1. Делим текст на отрезки равные длине ключа.
2. Составляем таблицу замен. В первый столбец записывается ключевое слово, в строку каждой букве дописывается алфавит по порядку, получается некий сдвиг.
3. Буква открытого текста – это столбец, буква ключевого слова – строка. Находим пересечение, заменяем.

Пример:

Открытый текст: ПРИМЕРШИФРАВИЖЕНЕРА

Ключ: КЛЮЧ

Алгоритм:

1. Делим текст на отрезки:

| | | | |
|---|---|---|---|
| п | р | и | м |
| к | л | ю | ч |

| | | | |
|---|---|---|---|
| е | р | ш | и |
| к | л | ю | ч |

| | | | |
|---|---|---|---|
| ф | р | а | в |
| к | л | ю | ч |

| | | | |
|---|---|---|---|
| и | ж | е | н |
| к | л | ю | ч |

| | | | |
|---|---|---|---|
| е | р | а | |
| к | л | ю | |

2. Производим замену (для первого отрезка). Получаем ПРИМ = ШЪЖВ

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

3. Шифруем весь текст, получаем ШЪЖВПЪЦЯЭЪЮЩТСГГПЪЮ

**Алгоритм дешифрования:**

1. Делим текст на отрезки равные длине ключа.

2. Составляем таблицу замен. В первый столбец записывается ключевое слово, в строку каждой букве дописывается алфавит по порядку, получается некий сдвиг.
3. Буква ключа – это строка, буква шифротекста – это буква в строке, которая указывает на столбец. Находим столбец, записываем букву.

**Атака**

- **Атака полного перебора (Brute Force Attack):**
- **Атака Касиски (Kasiski Examination):**

  Эта атака основана на поиске повторяющихся подстрок в зашифрованном тексте. Повторяющиеся подстроки предполагают использование одного и того же ключа в некоторых местах, что позволяет определить длину ключа. Определив длину ключа, можно провести частотный анализ по каждому сдвигу. Это значительно снижает сложность взлома шифра.
- **Анализ частот (Frequency Analysis):**

  Как только известна длина ключа, зашифрованный текст можно разбить на несколько подмножеств, каждое из которых зашифровано одним и тем же символом ключа. Для каждого подмножества проводится частотный анализ, как в случае с шифром Цезаря, чтобы определить наиболее вероятный символ ключа для каждого подмножества.
- **Атака методами статистического анализа (Statistical Analysis):**

  В некоторых случаях, можно использовать различные статистические методы, такие как анализ биграмм или триграмм, для предсказания частей ключа, особенно если длина ключа известна или предполагается.

## Шифр Хилла (Hill)

**Описание:**

Шифр Хилла основан на матричном преобразовании текста. Перед шифрованием необходимо каждому символу алфавита следует сопоставить код равный порядковому номеру символа в алфавите. Затем коды символов открытого текста записываются в матрицу размером n × m и создается шифрующая матрица n × n. Для шифрования матрица открытого текста умножается на шифрующую матрицу и вычисляется остаток от деления значения элементов матрицы-произведения на число символов выбранного алфавита. Для расшифровки необходимо шифротекст умножить на матрицу, которая является мультипликативной инверсией по отношению к шифрующей для выбранного алфавита.

**Характеристика:**

- Ключ: шифрующая матрица
- Тип шифра: линейная замена
- Сложность атаки грубой силы «BruteForce»: O(A^k^2), где A – мощность алфавита, k – длина ключа

**Алгоритм шифрования:**

1. Каждому символу алфавита сопоставляем порядковый номер начиная с 0.
2. Составляем таблицу матрицу, записываем построчно. Выбираем шифрующую матрицу, которая имеет мультипликативную инверсию себя.
3. Перемножаем матрицы. Берем остаток от деления на число мощности алфавита.
4. Получаем шифротекст

Пример:

Открытый текст: HILLCIPHEREXAMPLES

Ключ: матрица 3 на 3. [[6, 24, 1],[13, 16 10],[20, 17, 15]]

Алгоритм:

1. Каждому символу алфавита сопоставляем порядковый номер начиная с 0.

| a | b | c | d | e | f | g | h | i | j | k | l | m | n |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

| o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

2. Составляем таблицу матрицу, записываем построчно. Выбираем шифрующую матрицу, которая имеет мультипликативную инверсию себя.

| | | |
|---|---|---|
| 7 | 8 | 11 |
| 11 | 2 | 8 |
| 15 | 7 | 4 |
| 17 | 4 | 23 |
| 0 | 12 | 15 |
| 11 | 4 | 18 |

×

| | | |
|---|---|---|
| 6 | 24 | 1 |
| 13 | 16 | 10 |
| 20 | 17 | 15 |

Шифрующая матрица

3. Перемножаем матрицы. Берем остаток от деления на число мощности алфавита.

| | | |
|---|---|---|
| 366 | 483 | 552 |
| 252 | 432 | 151 |
| 261 | 540 | 145 |
| 614 | 863 | 402 |
| 456 | 447 | 345 |
| 478 | 634 | 321 |

≡

| | | |
|---|---|---|
| 2 | 15 | 18 |
| 18 | 16 | 21 |
| 1 | 20 | 15 |
| 16 | 5 | 12 |
| 14 | 5 | 7 |
| 10 | 10 | 9 |

(mod26)

Шифротекст: CPSSQVBUPQFMOFHKKJ.

**<u>Алгоритм дешифрования:</u>**

1. Каждому символу алфавита сопоставляем порядковый номер начиная с 0.
2. Составляем таблицу матрицу, записываем построчно. Считаем мультипликативную инверсию шифрующей матрицы.
3. Перемножаем матрицы. Берем остаток от деления на число мощности алфавита.
4. Получаем открытый текст

<u>Пример:</u>

Открытый текст: CPSSQVBUPQFMOFHKKJ

Ключ: матрица 3 на 3. [[6, 24, 1],[13, 16 10],[20, 17, 15]] –инверсия--> [[8, 5, 10],[21, 8, 21],[21, 12, 8]]

Алгоритм:

1. Каждому символу алфавита сопоставляем порядковый номер начиная с 0.

| a | b | c | d | e | f | g | h | i | j | k | l | m | n |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

| o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

2. Составляем таблицу матрицу, записываем построчно. Считаем мультипликативную обратную матрицу к матрице-ключу.

| | | |
|---|---|---|
| 2 | 15 | 18 |
| 18 | 16 | 21 |
| 1 | 20 | 15 |
| 16 | 5 | 12 |
| 14 | 5 | 7 |
| 10 | 10 | 9 |

×

| | | |
|---|---|---|
| 8 | 5 | 10 |
| 21 | 8 | 21 |
| 21 | 12 | 8 |

Дешифрующая матрица (обратная)

3. Перемножаем матрицы. Берем остаток от деления на число мощности алфавита.

| | | |
|---|---|---|
| 709 | 346 | 479 |
| 921 | 470 | 684 |
| 743 | 345 | 550 |
| 485 | 264 | 361 |
| 364 | 194 | 301 |
| 479 | 238 | 382 |

≡

| | | |
|---|---|---|
| 7 | 8 | 11 |
| 11 | 2 | 8 |
| 15 | 7 | 4 |
| 17 | 4 | 23 |
| 0 | 12 | 15 |
| 11 | 4 | 18 |

(mod26)

Шифротекст: HILLCIPHEREXAMPLES

**Атака**

- **Атака грубой силы (Brute Force Attack)**
- **Атака на основе известного открытого текста (Known Plaintext Attack)**

Эта атака предполагает, что злоумышленник имеет доступ к паре открытый текст - шифротекст. Используя эти пары, он может создать систему линейных уравнений для восстановления ключевой матрицы.

**Описание атаки:**

- Собираются пары известного открытого текста и соответствующего шифротекста.
- Составляется система линейных уравнений вида C=KPC = KPC=KP, где CCC — матрица шифротекста, KKK — ключевая матрица, а PPP — матрица открытого текста.
- Решая эту систему уравнений, злоумышленник может определить ключевую матрицу KKK.

## Шифр ADFGVX

**Описание:**

Шифрование осуществляется в два этапа. На первом этапе сначала задается матрица-ключ 6 × 6, заполненная произвольно символами алфавита и цифрами от 0 до 9. Индексами строк и столбцов этой матрицы служат буквы A, D, F, G, V, X. Далее каждый символ открытого текста кодируется парой буквенных индексов, на пересечении которых в матрице-ключе он находится. На втором этапе задается кодовое слово для перестановки столбцов, а затем ранее закодированный открытый текст переписывается построчно в матрицу с числом столбцов, равным длине ключевого слова. В завершение столбцы этой матрицы переставляются в соответствии с лексикографическим порядком букв ключевого слова и итоговый шифротекст образуется конкатенацией строк этой матрицы.

**Характеристика:**

- Ключ: кодовое слово или последовательность цифр
- Тип шифра: комбинированный (замена и перестановка)
- Сложность атаки грубой силы «BruteForce»: O(36! * k!), где 36 – квадрат размерности матрицы, k – длина ключа

**Алгоритм шифрования:**

1. Составить матрицу и кодировать каждый символ открытого текста. Таблица индексируется буквами ADFGVX.
2. Каждая буква кодируется парой букв. Индекс строки и индекс столбца.
3. Записать получившийся шифр в таблицу, которая индексируется кодовым словом. Производится перестановка.
4. Читаем по столбцам. Получаем шифротекст

Пример:

Открытый текст: CIPHEREXAMPLE

Ключ: OURKEY

Алгоритм:

1. Составить матрицу и кодировать каждый символ открытого текста. Таблица индексируется буквами ADFGVX.

| | a | d | f | g | v | x |
|---|---|---|---|---|---|---|
| a | a | b | c | d | e | f |
| d | g | h | i | j | k | l |
| f | m | n | o | p | q | r |
| g | s | t | u | v | w | x |
| v | y | z | 0 | 1 | 2 | 3 |
| x | 4 | 5 | 6 | 7 | 8 | 9 |

2. Каждая буква кодируется парой букв. Индекс строки и индекс столбца. Получится последовательность: AFDFFGDDAVFXAVGXAAFAFGDXAV
3. Записать получившийся шифр в таблицу, которая индексируется кодовым словом. Производится перестановка.

| **o** | **u** | **r** | **k** | **e** | **y** |
|---|---|---|---|---|---|
| **3** | **5** | **4** | **2** | **1** | **6** |
| a | f | d | f | f | g |
| d | d | a | v | f | x |
| a | v | g | x | a | a |
| f | a | f | g | d | x |
| a | v | | | | |

=>

| **e** | **k** | **o** | **r** | **u** | **y** |
|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** |
| f | f | a | d | f | g |
| f | v | d | a | d | x |
| a | x | a | g | v | a |
| d | g | f | f | a | x |
| | | a | | v | |

4. Получаем шифротекст

Выписать текст по столбцам и сформировать шифротекст: FFADFVXG ADAFADAGFFDVAVGXAX.

**Алгоритм дешифрования:**

1. Исходя из знания ключа, заполняем таблицу по столбцам.
2. Читаем текст по строкам. Разбиваем получившийся текст по парам. Первая буква – это индекс строки, вторая – столбца. Смотрим пересечение. Декодируем.

**Атака**

- **Атака грубой силы (Brute Force)**
- **Атака частотного анализа**

Эта атака использует частотный анализ на первом этапе подстановки. После того как сообщение шифруется подстановочной таблицей, можно попытаться определить вероятные соответствия символов путем анализа частот встречаемости символов в шифрованном тексте и сравнения их с известными частотами букв в языке. Однако из-за транспозиции эта атака становится сложнее, так как необходимо сначала правильно восстановить порядок символов.

- **Криптоанализ с известным открытым текстом (Known Plaintext Attack)**