**CCNA Security**

**Глава 7. Лабораторная работа. Изучение методов шифрования**

# Задачи

**Часть 1: Дешифрация предварительно зашифрованного сообщения с помощью шифра Vigenère**

Для дешифрации сообщения используйте шифрованное сообщение, ключ шифра, а также квадрат шифра Vigenère.

**Часть 2. Создание сообщения, зашифрованного с помощью шифра Vigenère, и его дешифрация**

1. Договоритесь с партнером по лабораторной работе о секретном пароле.
2. Создайте секретное сообщение, используя шифр Vigenère и ключ.
3. Обменяйтесь сообщениями и дешифруйте их, используя общий ключ.
4. С помощью интерактивного декодера Vigenère проверьте дешифрацию.

# Общие сведения

В сервисе шифрования паролей Cisco IOS используется собственный алгоритм Cisco, основанный на шифре Vigenère. Vigenère является примером распространенного типа шифрования, который называется многоалфавитной подстановкой.

**Примечание.** В данной лабораторной работе студенты могут работать в парах.

# Необходимые ресурсы

Пользовательское устройство с доступом в Интернет

**Часть 1: Дешифрация предварительно зашифрованного сообщения с помощью шифра Vigenère**



В части 1 необходимо проанализировать зашифрованное сообщение и дешифровать его при помощи ключа шифра и квадрата шифра Vigenère.

**Шаг 1: Изучите шифрованное сообщение.**

Следующее сообщение было зашифровано с помощью шифра Vigenère: **VECIHXEJZXMA**

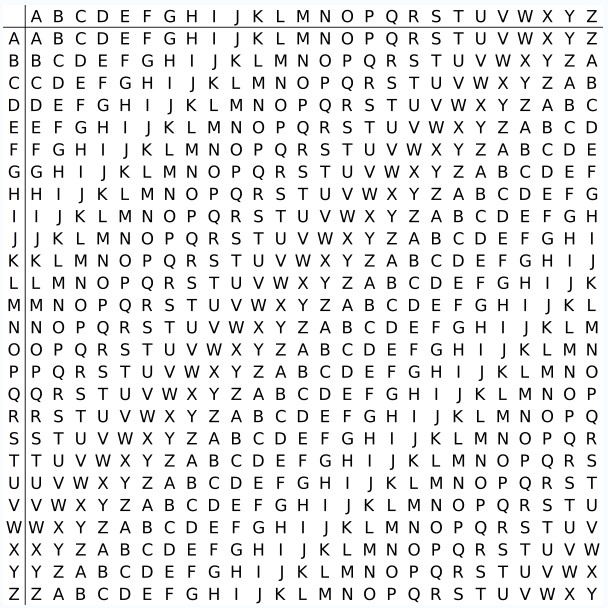
**Шаг 2: Изучите ключевое слово шифра.**

Для шифрования данного сообщения было использовано ключевое слово **TCPIP.** Это же ключевое слово будет использовано для дешифрации сообщения.

**Шаг 3: Изучите структуру квадрата Vigenère.**

Для дешифрации сообщения используется стандартный квадрат или таблица Vigenère вместе с ключевым словом.

Компания Cisco и/или



**Шаг 4: Дешифруйте сообщение, используя ключевое слово и квадрат Vigenère.**

1. С помощью следующей таблицы дешифруйте сообщение. Сначала введите буквы зашифрованного сообщения во второй строке ячеек слева направо.
2. Введите ключевое слово TCPIP в верхней строке, повторяя его буквы до тех пор, пока есть буква ключевого слова для каждой буквы зашифрованного сообщения, даже если в конце ключевое слово будет неполным.
3. Возьмите квадрат или таблицу Vigenère, указанную на шаге 3, и найдите горизонтальную строку, которая начинается с первой буквы ключевого слова (Т). Найдите в этой строке первую букву зашифрованного сообщения (V). Буква в верхней части столбца, где находится буква зашифрованного сообщения, – это первая буква дешифрованного сообщения (С).
4. Повторяйте этот процесс до тех пор, пока не дешифруете сообщение полностью, и введите его в третью строку следующей таблицы.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ключевое слово шифра** | T | C | P | I | P | T | C | P | I | P | T | C |
| **Шифрованное сообщение** | V | E | C | I | H | X | E | J | Z | X | M | A |
| **Дешифрованное сообщение** | C | C | N | A | S | E | C | U | R | I | T | Y |

**Часть 2: Создание сообщения, зашифрованного с помощью шифра Vigenère, и его дешифрация**

В части 2 договоритесь с партнером по лабораторной работе о секретном пароле, который будет использован в качестве общего ключа. Каждый студент из пары создает секретное сообщение, используя шифр Vigenère и ключ. Партнеры обмениваются сообщениями и дешифруют их, используя общий ключ.

**Примечание.** Если вы работаете в одиночку, вы можете выполнить все шаги самостоятельно.

**Шаг 1: Определите ключевое слово шифра.**

Придумайте с партнером и запишите здесь ключевое слово шифра.

\_\_\_\_\_\_\_\_\_\_OFFLINESHE\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Шаг 2: Создайте простое текстовое сообщение и зашифруйте его (каждый из партнеров).**

1. Создайте простое (дешифрованное) текстовое сообщение, которое ваш партнер должен дешифровать.

\_\_\_\_\_YOURSUMMARY\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Воспользуйтесь следующей таблицей для шифрования сообщения. Введите здесь нешифрованное сообщение и ключевое слово шифра, но не показывайте их партнеру.
2. В таблице Vigenère найдите строку, которая начинается с первой буквы ключевого слова шифра. Затем в верхней части столбца таблицы найдите первую букву, которую необходимо зашифровать. Ячейка, в которой строка таблицы (буква ключа) и столбец (буква сообщения) пересекаются, содержит первую букву зашифрованного сообщения. Повторяйте процесс до тех пор, пока не зашифруете сообщение полностью.

**Примечание.** Таблица рассчитана на сообщения длиной до 12 символов. При желании вы можете создать более длинные сообщения. Шифрование и дешифрование сообщений не чувствительны к регистру.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ключевое слово шифра** | O | F | F | L | I | N | E | E | S | H | E |  |
| **Шифрованное сообщение** | M | T | Z | C | A | H | Q | Q | S | Y | C |  |
| **Дешифрованное сообщение** | Y | O | U | R | S | U | M | M | A | R | Y |  |

**Шаг 3: Дешифруйте сообщение партнера.**

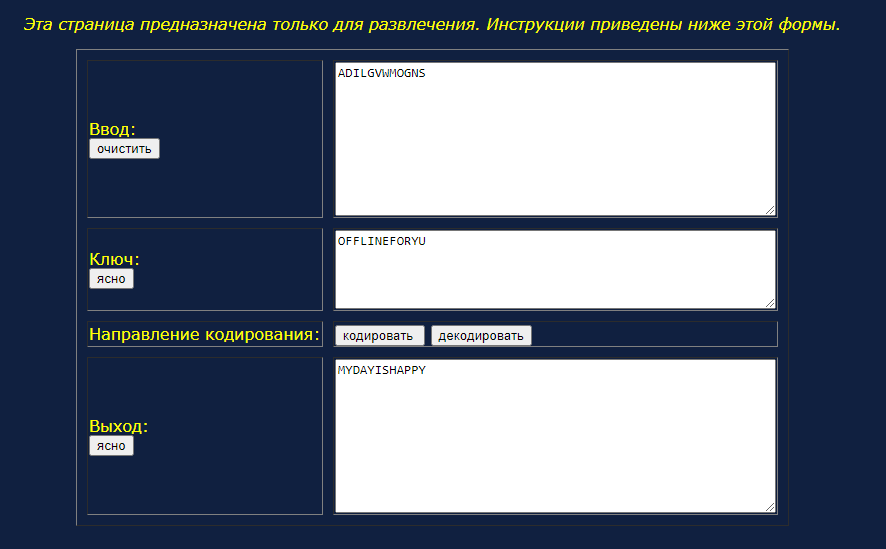
1. Воспользуйтесь следующей таблицей для дешифрования сообщения, которое зашифровал ваш партнер.

Введите зашифрованное сообщение и ключевое слово шифра.

1. Используйте процедуру, описанную в части 1, шаг 4.

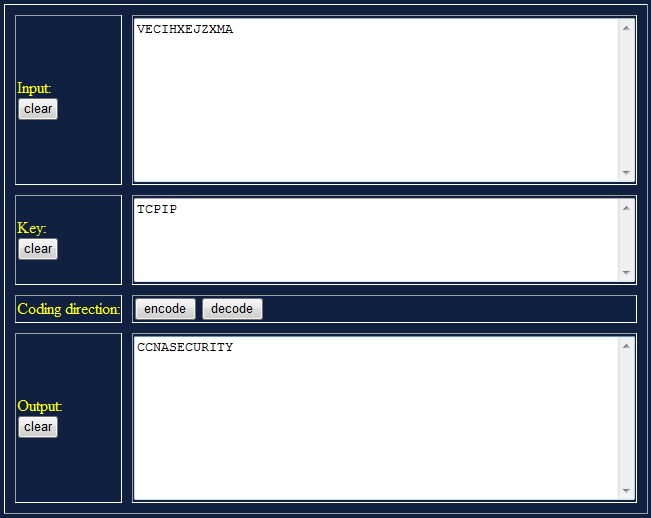
**Примечание.** Таблица рассчитана на сообщения длиной до 12 символов. При желании вы можете создать более длинные сообщения.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ключевое слово шифра** | O | F | F | L | I | N | E | F | O | R | Y | U |
| **Шифрованное сообщение** | A | D | I | L | G | V | W | M | O | G | N | S |
| **Дешифрованное сообщение** | M | Y | D | A | Y | I | S | H | A | P | P | Y |



**Шаг 4: Используйте интерактивный инструмент дешифрования для подтверждения результата дешифрования.**

1. Поиск в Интернете по фразе Vigenère decode покажет, что существует множество различных инструментов для шифрования и дешифрования. Многие из них являются интерактивными.
2. Один из них находится по адресу [http://sharkysoft.com/vigenere/1.0/.](http://sharkysoft.com/vigenere/1.0/) Введите на этом сайте зашифрованное сообщение партнера в верхней части экрана, а ключ шифра в середине. Нажмите **Decode**, чтобы увидеть исходный текст сообщения. Вы также можете использовать этот инструмент для шифрования сообщений.
3. В следующем примере для дешифрации шифрованного сообщения из части 1 используется инструмент Sharky’s Vigenère Cipher.



# Вопросы для повторения

1. Можно ли использовать шифр Vigenère для дешифрования сообщений вручную без использования компьютера?

\_\_\_Да. У получателя должно быть зашифрованое сообщение и ключивое слово и копия шифра Vigenère \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Найдите в Интернете инструменты взлома шифра Vigenère. Считается ли шифр Vigenère криптостойкой системой шифрования, которую сложно взломать?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_ Криптографический алгоритм считается безусловно стойким\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_