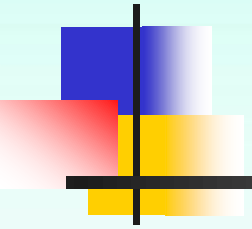
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Практ. 4 2022 КІБ-19

ШИФР ВИЖЕНЕРА

I.2.2 Шифр Виженера (Vigenere, 1585)

Идея→ задается вектор $\boldsymbol{K}$ ключей $(\boldsymbol{m} < \boldsymbol{n})$ – секретное кодовое слово

$$\boldsymbol{K} = \begin{bmatrix} \boldsymbol{k}_0 \\ \boldsymbol{k}_i \\ \boldsymbol{k}_{m-1} \end{bmatrix} \qquad \boldsymbol{k}_i = \boldsymbol{s}_l \in \mathbb{Z}_{\boldsymbol{n}}!$$

Шифрование $\rightarrow \boldsymbol{c}_t = \left(\boldsymbol{s}_t + \boldsymbol{k}_{t(mod\ \boldsymbol{m})}\right) \boldsymbol{mod\ n}$

Дешифрование $\rightarrow \boldsymbol{s}_i = \left(\boldsymbol{c}_t - \boldsymbol{k}_{t(mod\ \boldsymbol{m})}\right) \boldsymbol{mod\ n}$

I.2.2 Шифр Виженера. Пример

К = СУПЕРКЛЮЧ

М= ПРИВІТ_СТУДЕНТИ_КІБ

М= *ПРИВІТ_СТ УДЕНТИ_КІ Б*

k_0 = С → 20; s_0 = П → 18;

c_0 = (20+18) mod 31 = 7; c_0 = 7 → Є

С = ЄИЩЗЯШЛПН ІШХУЗНЛІЕ У

Общий подход

Использовать словарь аддитивного шифра.
Создать СЕКРЕТНОЕ слово (6 символов).
Модифицировать программу аддитивного шифра для шифра Виженера.

ШИФР ПЛЕЙФЕРА

Шифр Плейфера

Идея→ задается $\boldsymbol{m * m}$ матрица $\boldsymbol{K}$ ключей $(\boldsymbol{m * m \geq n})$

$$\begin{bmatrix} \boldsymbol{k_{0,0}} & \boldsymbol{\dots} & \boldsymbol{k_{0,m}} \\ & \boldsymbol{k_{i,j}} & \\ \boldsymbol{k_{m,0}} & & \boldsymbol{k_{m,m}} \end{bmatrix} \qquad \boldsymbol{k_{i,j} = s_l \in \mathbb{Z}_n!}$$

Каждый $\boldsymbol{k_{i,j}}$ есть символ алфавита.

Размещение $\boldsymbol{k_{i,j}}$ в матрице $\boldsymbol{K}$ собственно и есть секретный ключ.

Мощность $\boldsymbol{\|K\| = (m * m)!}$

Открытый текст $\boldsymbol{s_0, s_1, s_2, s_3, \dots}$ разбивается на пары символов $\mathbf{S_1, S_2}$.

$$\mathbf{S_1} \rightarrow \boldsymbol{k_{i_1,j_1}} \quad \mathbf{S_2} \rightarrow \boldsymbol{k_{i_2,j_2}}$$

Шифр Плейфера

Шифрование. Для каждой пары символов находим шифросимволы:

Если $i1 = i2, j1 \neq j2 \rightarrow$
$\boldsymbol{c}_1 = \boldsymbol{k}_{i_1, j_1+1\,(mod\ m)}$, $\boldsymbol{c}_2 = \boldsymbol{k}_{i_1, j_2+1\,(mod\ m)}$

Если $i1 \neq i2, j1 = j2 \rightarrow$
$\boldsymbol{c}_1 = \boldsymbol{k}_{i_1+1\,(mod\ m), j_1}$, $\boldsymbol{c}_2 = \boldsymbol{k}_{i_2+1\,(mod\ m), j_1}$

Если $i1 \neq i2, j1 \neq j2 \rightarrow$
$\boldsymbol{c}_1 = \boldsymbol{k}_{i_1, j_2}$, $\boldsymbol{c}_2 = \boldsymbol{k}_{i_2, j_1}$

Шифр Плейфера. Пример

K =

А	Б	Ґ	Д	Ж	З
В	Г	Е	Є	І	Ї
Й	К	Н	О	С	Т
Л	М	П	Р	У	Ф
Х	Ц	Щ	Ь	_	.
Ч	Ш	Ю	Я	И	,

М= ПРИВІТ_СТУДЕНТИ_КІБ

М= ПР ИВ ІТ _С ТУ ДЕ НТ И_ КІ Б.

С = РУЧІ….СЇ …….. ОЙ …..

Общий подход

В открытом тексте используется 36 символов: украинские большие буквы и спецсимволы

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З
И	І	Ї	Ь	Й	К	Л	М	Н	О
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Щ	Ю	Я	_	.	,				

Общий подход

1. Формирование ключевой матрицы

Матрица ***K*** размерности **6 * 6** выбирается в соответствии с вариантом задания.

При формировании матрицы необходимо учесть кодировку украинских символов.

Общий подход

2. Функция шифрования.
def *encrypt_message* (message)
…..
return (ciphertext)
message – исходное сообщение
ciphertext – зашифрованное сообщение

!!!! Проверки исходного сообщения:

1. Четное число символов.
2. Нет символов не из принятого множества.
3. Нет двух одинаковых символов, идущих подряд.

Общий подход

3. Функция дешифрования.
def *decrypt_message* (ciphertext)
…..
return (planetext)
ciphertext – зашифрованное сообщение
planetext – расшифрованное сообщение

!!!! Проверки исходного сообщения:

1. Четное число символов.
2. Нет символов не из принятого множества.
3. Нет двух одинаковых символов, идущих подряд.

Задание

1. Генерация ключевой матрицы (см. вариант)
2. Ввод текста открытого сообщения (см. вариант)
3. Шифрование.
4. Вывод шифрограммы.
5. Дешифрация.
6. Вывод расшифрованного сообщения.
7. Сравнение исходного текста и расшифрованного.
8. Вывод о работе

СУПЕР Задание

Задано открытое сообщение и соответствующая шифрограмма.

Найти ключевую матрицу *K*

END # 4