МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ІКТА

кафедра ЗІ



З В І Т

до лабораторноїроботи №3

з курсу: «Основи криптографічного захисту інформації»

на тему: «КРИПТОГРАФІЯ І СТЕГАНОГРАФІЯ

Використання шифрів гамування та Віженера для захисту текстової інформації»

**Виконав:** ст. гр. УІ-42

Симоненко Д.С.

**Прийняв:** Шандра З.А.

Львів – 2017

**Завдання:**

1. Для шифрування методом гамування вручну зашифрувати і розшифрувати заданий текст на вибраному ключі (створитисамостійно) і перевірити результат шифрування з використаннямпрограми LAB\_RAB.exe . Показати процедуру шифрування/розшифрування, переваги методу, вимоги до ключа.

2. Для шифрування шифром Віжене равручну з використанням аналітичного виразу або таблиці Віженера зашифрувати і розшифрувати заданий текст (див.варіантизавдань) на вибраному ключі (створити самостійно) і перевірити результат шифрування з використанням програми LAB\_RAB.exe . Показати процедуру шифрування, переваги методу, вимоги до ключа. Чи можна цей метод шифруваннярозглядати як метод багатоалфавітної підстановки?

**В8. ISO collaborates with the Electrotechnical Commission**

5. Примітка. Для виконання роботи потрібно запустити програму LAB\_RAB.exe. Порядок роботи і теоретичні відомості з методів шифрування можна подивитися в пункті меню Help. В якості абетки використати табл. ASCII-кодів. Максимальна кількість знаків ключа 9. Символи ключів можна задати в опції «ключі».

**Виконання:**

1. Гамування

ISO collaborates with the Electrotechnical Commission

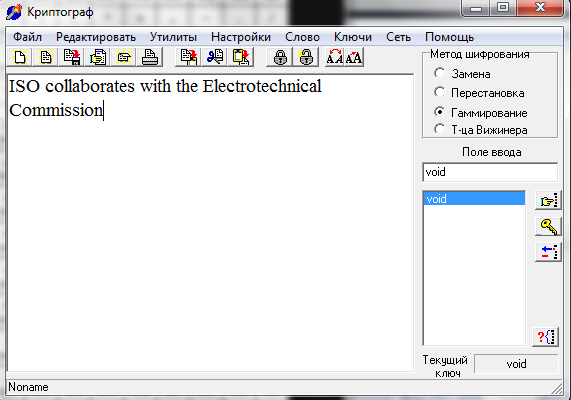
Voidvoidvoidvoidvoidvoidvoidvoidvoidvoidvoidvoidvoidv

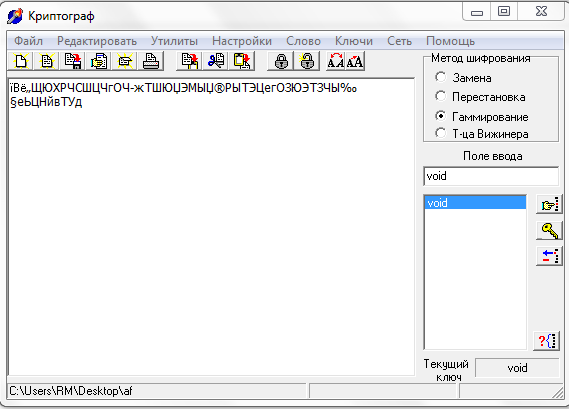
їВё„ЩЮХРЧСШЦЧгОЧ–жТШЮЏЭМЫЏ®РЫТЭЦегОЗЮЭТЗЧЫ‰§еЬЦНйвТУд

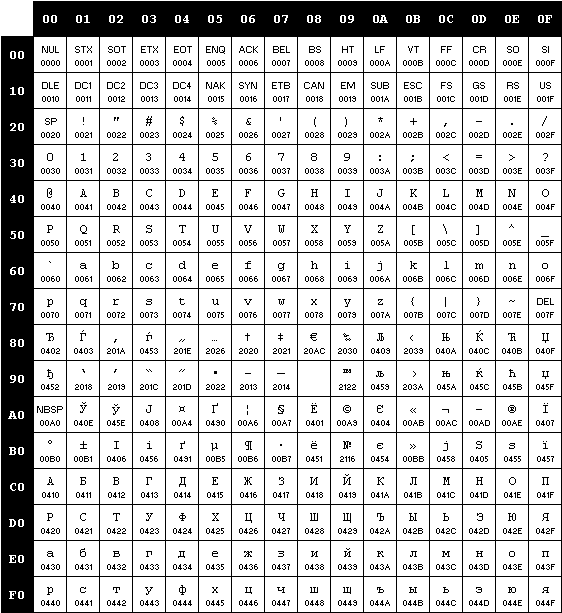
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I | S | O | SP | c | o | l | l | a | b | o | r | a | t | e | s | SP | w |
| 0049 | 0053 | 004F | 0020 | 0063 | 006F | 006C | 006C | 0061 | 0062 | 006F | 0072 | 0061 | 0074 | 0065 | 0073 | 0020 | 0077 |
| v | o | i | d | v | o | i | d | v | o | i | d | v | o | i | d | v | o |
| 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F |
| 0457 | 0412 | 0451 | 201E | 0429 | 042E | 0425 | 0420 | 0427 | 0421 | 0428 | 0426 | 0427 | 0433 | 041E | 0427 | 2014 | 0436 |
| ї | B | ё | „ | Щ | Ю | Х | Р | Ч | С | Ш | Ц | Ч | г | О | Ч | – | ж |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | t | h | SP | t | h | e | SP | E | l | e | c | t | r | o | t | e | c |
| 0069 | 0074 | 0068 | 0020 | 0074 | 0068 | 0065 | 0020 | 0045 | 006C | 0065 | 0063 | 0074 | 0072 | 006F | 0074 | 0065 | 0063 |
| i | d | v | o | i | d | v | o | i | d | v | o | i | d | v | o | i | d |
| 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 |
| 0422 | 0428 | 042E | 040F | 042D | 041C | 042B | 040F | 00AE | 0420 | 042B | 0422 | 042D | 0426 | 0435 | 0433 | 041E | 0417 |
| Т | Ш | Ю | Џ | Э | М | Ы | Џ | ® | Р | Ы | Т | Э | Ц | е | г | О | З |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| h | n | i | c | a | l | SP | C | o | m | m | i | s | s | i | o | n |
| 0068 | 006E | 0069 | 0063 | 0061 | 006C | 0020 | 0043 | 006F | 006D | 006D | 0069 | 0073 | 0073 | 0069 | 006F | 006E |
| v | o | i | d | v | o | i | d | v | o | i | d | v | o | i | d | v |
| 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 |
| 042E | 042D | 0422 | 0417 | 0427 | 042B | 2030 | 00A7 | 0435 | 042C | 0426 | 041D | 0439 | 0432 | 0422 | 0423 | 0434 |
| Ю | Э | Т | З | Ч | Ы | ‰ | § | е | Ь | Ц | Н | й | в | Т | У | д |







1. Шифр Віженера

ISO collaborates with the Electrotechnical Commission

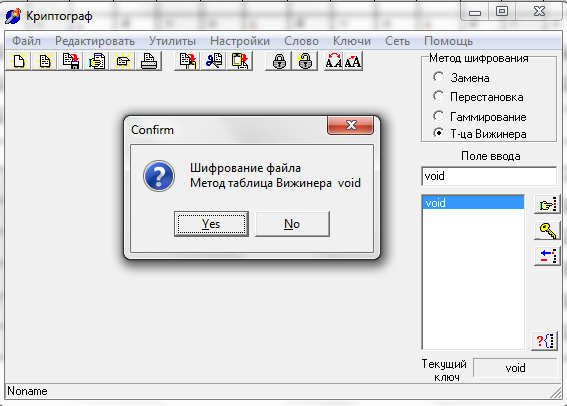
Voidvoidvoidvoidvoidvoidvoidvoidvoidvoidvoidvoidvoidv

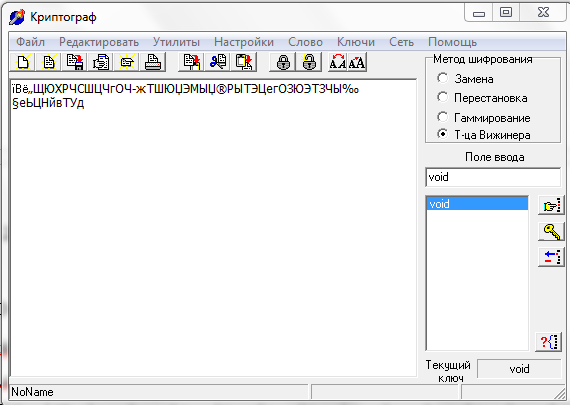
їВё„ЩЮХРЧСШЦЧгОЧ–жТШЮЏЭМЫЏ®РЫТЭЦегОЗЮЭТЗЧЫ‰§еЬЦНйвТУд

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I | S | O | SP | c | o | l | l | a | b | o | r | a | t | e | s | SP | w |
| 0049 | 0053 | 004F | 0020 | 0063 | 006F | 006C | 006C | 0061 | 0062 | 006F | 0072 | 0061 | 0074 | 0065 | 0073 | 0020 | 0077 |
| v | o | i | d | v | o | i | d | v | o | i | d | v | o | i | d | v | o |
| 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F |
| 0457 | 0412 | 0451 | 201E | 0429 | 042E | 0425 | 0420 | 0427 | 0421 | 0428 | 0426 | 0427 | 0433 | 041E | 0427 | 2014 | 0436 |
| ї | B | ё | „ | Щ | Ю | Х | Р | Ч | С | Ш | Ц | Ч | г | О | Ч | – | ж |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | t | h | SP | t | h | e | SP | E | l | e | c | t | r | o | t | e | c |
| 0069 | 0074 | 0068 | 0020 | 0074 | 0068 | 0065 | 0020 | 0045 | 006C | 0065 | 0063 | 0074 | 0072 | 006F | 0074 | 0065 | 0063 |
| i | d | v | o | i | d | v | o | i | d | v | o | i | d | v | o | i | d |
| 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 |
| 0422 | 0428 | 042E | 040F | 042D | 041C | 042B | 040F | 00AE | 0420 | 042B | 0422 | 042D | 0426 | 0435 | 0433 | 041E | 0417 |
| Т | Ш | Ю | Џ | Э | М | Ы | Џ | ® | Р | Ы | Т | Э | Ц | е | г | О | З |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| h | n | i | c | a | l | SP | C | o | m | m | i | s | s | i | o | n |
| 0068 | 006E | 0069 | 0063 | 0061 | 006C | 0020 | 0043 | 006F | 006D | 006D | 0069 | 0073 | 0073 | 0069 | 006F | 006E |
| v | o | i | d | v | o | i | d | v | o | i | d | v | o | i | d | v |
| 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 | 006F | 0069 | 0064 | 0076 |
| 042E | 042D | 0422 | 0417 | 0427 | 042B | 2030 | 00A7 | 0435 | 042C | 0426 | 041D | 0439 | 0432 | 0422 | 0423 | 0434 |
| Ю | Э | Т | З | Ч | Ы | ‰ | § | е | Ь | Ц | Н | й | в | Т | У | д |





**Висновки:**

Дослідив використання шифрів гамування та Віженера для захисту текстової

Інформації.