МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**ДОСЛІДЖЕННЯ КРИПТОСТІЙКОСТІ DES**

**Виконав:** курсант 314 навчальної групи

ст. солдат \_\_\_\_\_\_\_\_\_\_\_ЛУТЧЕНКО О.Т.

**Перевiрив:** викладач кафедри № 33

майор\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ПРИЙМА О.О.

Київ – 2024

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DES mode | Key | Open text | Cypher text | Open text(with change) | Cypher text(with change) |
| ECB | 1234AB  CC5654345 | я живу у Києві | 2789d505f2d4f6b5  8fd1190af9723772 | 1. с живу у Києві  2.я живу у Києву | 1. 900e04a58fe2fb9b  8fd1190af9723772  2. 2789d505f2d4f6b5  07ffab9f8a27806b |
| CBC | 1234AB  CC5654345 | я живу у Києві | 4428027fa2ea8325  874e641efad4a86d | 1. с живу у Києві  2.я живу у Києву | 1. 37d665ad9b08750a  f6003ed864d95be8  2. 4428027fa2ea8325  aabcf7eefe48292e |
| СFB | 1234AB  CC5654345 | я живу у Києві | 9039d76896349c7  8a13462ab7b5e | 1. с живу у Києві  2.я живу у Києву | 1. 9e39d76896349c78  929c22e85fa0  2. 9039d76896349c78  a13462ab7b4b |
| OFB | 1234AB  CC5654345 | я живу у Києві | 9039d76896349c7  8be98dec9ee88 | 1. с живу у Києві  2.я живу у Києву | 1. 9e39d76896349c78  be98deс9ee88  2. 9039d76896349c78  be98dec9ee9d |
| CTR | 1234AB  CC5654345 | я живу у Києві | 9039d76896349c7  8ac59e2864f38 | 1. с живу у Києві  2.я живу у Києву | 1. 9e39d76896349c78  ac59e2864f38  2. 9039d76896349c78  ac59e2864f2d |

**ВИСНОВКИ:**

В режимі ECB(Еlectronic Сode Вook) текст ділиться на блоки. В результаті виходить послідовність блоків. Тому при заміні тексту в першому чи останньому блоці у відкритому тексті замінюється перший чи останній блок шифротексту.

В режимі CBC(Сipher Вlock Сhaining) текст ділиться на блоки. Блоки шифруються шляхом зчеплення 1 блока з 2; 1 та 2 з 3; 1, 2 та 3 з 4; 1, 2, 3, 4 з 5. Алгоритм використовує попередній блок шифротексту для шифрування наступного блоку, тому навіть невеликі зміни у відкритому тексті призведуть до значних змін у шифротексті. Тому при зміні тексту в першому блоці у відкритому тексті - міняється весь шифротекст, а при зміні тексту в останньому блоці - міняється останній блок шифротексту.

В режимі СFB(Сipher Feed Вack) текст ділиться на блоки. Заміна першої літери відкритого тексту призведе до зміни першої літери шифротексту, але не вплине на наступні літери. Процес шифрування залежить від блоку шифрування, тому зміна лише однієї літери вплине лише на одну літеру шифротексту.

В режимі OFB(Output Feed Back) текст ділиться на блоки. Дзеркальне відображення у зашифрованому тексті робить дзеркально відбитий біт у відкритому тексті на тому самому місці. Тому якщо замінити першу чи останню літеру відкритого тексту, це призведе до зміни першого чи останнього блоку шифротексту. OFB генерує ключі, які використовуються для шифрування наступних блоків, тому зміна одного біту відкритого тексту змінить один біт шифротексту, але не вплине на інші блоки.

В режимі CTR(Сounter) текст ділиться на блоки. Режим робить із блочного шифру потоковий, тобто генерує послідовність, до якої застосовується операція XOR з текстом повідомлення. Тому якщо змінити першу або останню літеру відкритого тексту, це призведе до зміни тільки одного біту на початку чи в кінці в шифротексті. Така зміна буде розповсюджуватися по блоку зашифрованого тексту, але не вплине на інші блоки.