**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**

**ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ**

КАФЕДРА КІБЕРБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія 2»

**ДОСЛІДЖЕННЯ КРИПТОСТІЙКОСТІ DES**

**Виконав:** курсант 314 навчальної групи

ст. солдат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Є.КОНДРАТЕНКО

.04.2024

**Перевiрив:** викладач кафедри № 33

капітан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.ПРИЙМА

.04.2024

Київ – 2024

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DES mode** | **Key** | **Open text** | **Cypher text** | **Open text with change** | **Cypher text with change** |
| **CBC** | **DR358643135607cf** | **У берлозі шум та гамір** | **3cbc37fb13f087702019f0e7dc69a90fe926e3a01fe3e523** | **1) В берлозі шум та гамір**  **2)В берлозі шум та гамін** | **1)0cc0428683e4a054c320d4c01c360f672baa78bc94744b56**  **2) 3cbc37fb13f087702019f0e7dc69a90f52f05fb69e941165** |
| **CFB** | **DR358643135607cf** | А з чорниці чи ожинки | **dbaccf5a6c70598de03df7aeba43e1be8f3265b34a** | **1) І з чорниці чи ожинки**  **2) А з чорниці чи ожинка** | **1) cdaccf5a6c70598de3ece43b1eec35e96ca9766e7a**  **2) dbaccf5a6c70598de03df7aeba43e1be8f3265b342** |
| **OFB** | **DR358643135607cf** | А коли настане нічка | **dbacc6441072398d60c15b26a6d2b02c2b320e27** | **1) І коли настане нічка**  **2) І коли настане нічка** | **1) cdacc6441072398d60c15b26a6d2b02c2b320e27**  **2)cdacc6441072398d60c15b26a6d2b02c2b320e29** |
| **CTR** | **DR358643135607cf** | І на білому коні | **cdacc14a0b7f4f8be538ceeec06d69db** | **1) А на білому коні**  **2) І на білому коня** | **1) dbacc14a0b7f4f8be538ceeec06d69db**  **2) dbacc14a0b7f4f8be538ceeec06d69c2** |
| **ECB** | **DR358643135607cf** | **У небесній вишин** | **cdf24f2c4734007c052ccbf5c9b8a4ac7fc24cc847acabaa** | **1)В небесній вишині**  **2)У небесній вишиня** | **1)5cc8c36f8293a8a2052ccbf5c9b8a4ac7fc24cc847acabaa**  **2)cdf24f2c4734007c052ccbf5c9b8a4ac793b724ab63e5c6e** |

Висновок:

За допомогою стандартного шифрування даних DES (Data Encryption Standard ), якиз шифрує дані в блоках розміром 64 біти кожен, що 64 біти звичайного тексту надходять як вхідні дані для DES, який створює 64 біти зашифрованого тексту. Опрацювавши кожен із режимів DES, можна сказати, що режими CBC та CFB придатні для аутентифікації даних. Режим CFB підходить для шифрування ключів, цей режим зазвичай використовується для шифрування окремих символів, а режим OFB нерідко застосовується для шифрування супутникових системах зв'язку.

Отже зміни, які застосовують до текст, впливають на кінцевий шифротекст у залежності від обраного типу шифрування і режиму. Якщо у режимі ЕСВ замінити першу букву у відкритому тексті, то відбудеться повна зміна блока шифрування,тож весь блок шифрування буде різним. А зміна першої букви у режимах СВС, CFB, OFB, CTR вплине лише на змінений блок шифрування.