МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**Тема № 2**. Електронна комунікаційна мережа об’єкта кіберзахисту як джерело ознак кіберінциденту.

**Заняття № 3/18**. Реалізація алгоритму шифрування DES

**РОБОТА З WEB-ДОДАТКОМ CYBERCHEF.IO**

**Виконав:** курсант навчальної групи 314

солдат\_\_\_\_\_\_\_\_\_\_МАКСИМЕНКО Р.Р.

20.04.2024

**Перевiрив:** викладач кафедри №33

капітан \_\_\_\_\_\_\_\_\_\_\_\_\_\_ПРИЙМА О.О.

Київ – 2024

| DES mode | Key | Open Text | Changed Text | CipherText  (Open Text) | CipherText\*  (Changed Text) |
| --- | --- | --- | --- | --- | --- |
| ECB | 14A7D67818CA18AD | I love Odessa | I love Odessm | 30c0b00d5f4cb55082af42b446d05543 | 30c0b00d5f4cb550a655f57ca9fa734c |
| K love Odessa | 30c0b00d5f4cb55082af42b446d05543 | 6f853a85c131bd2c82af42b446d05543 |
| CTR | 14A7D67818CA18AD | I love Odessa | I love Odessp | 1d6d55f25e14d051350a7c2b59b8 | 1d6d55f25e14d051350a7c2b48b8 |
| L love Odessa | 1d6d55f25e14d051350a7c2b59b8 | 186d55f25e14d051350a7c2b59 |
| CBC | 14A7D67818CA18AD | I love Odessa | I love Odesst | 6f2b7b9417f28f7d8b54307341280192 | 6f2b7b9417f28f7de29c4f7323f3a71a |
| A love Odessa | 6f2b7b9417f28f7d8b54307341280192 | 969d21135c7080c0978aabaea2d60a2c |
| CFB | 14A7D67818CA18AD | I love Odessa | I love Odessr | 1d6d55f25e14d051b6e3d5565a | 1d6d55f25e14d051b6e3d55649 |
| J love Odessa | 1d6d55f25e14d051b6e3d5565a | 1e6d55f25e14d0515d7725ca4b |
| OFB | 14A7D67818CA18AD | I love Odessa | I love Odessy | 1d6d55f25e14d0514561c01a42 | 1d6d55f25e14d0514561c01a5a |
| C love Odessa | 1d6d55f25e14d0514561c01a42 | 176d55f25e14d0514561c01a42 |

**ВИСНОВОК**

У ході проведення аналізу режимів шифрування EBC та CBC виявлено:

Обидва режими використовують блоки шифрування фіксованого розміру 64 біти та симетричне шифрування.

Головна відмінність режимів, це те, що режим EBC шифрує блоки незалежно один від одного тобто однакові блоки відкритого тексту, будуть мати однакові блоки шифртексту

| DES mode | Key | Open Text | Changed Text | CipherText  (OT) | Cipher Text  (CT) |
| --- | --- | --- | --- | --- | --- |
| ECB | 14A7D67818CA18AD | I love Odessa and | I love Odessa ans | 30c0b00d5f4cb5508b0bd543406b158edbd74723569e50eb | 30c0b00d5f4cb5508b0bd543406b158e403231935d4ea48 |

| DES mode | Key | Open Text | Changed Text | CipherText  (OT) | Cipher Text  (CT) |
| --- | --- | --- | --- | --- | --- |
| ECB | 14A7D67818CA18AD | I love Odessa and | I love Odesfa and | 30c0b00d5f4cb5508b0bd543406b158edbd74723569e50eb | 30c0b00d5f4cb55070a5dad97e1073e7dbd74723569e50eb |

У режимі CBC кожен блок відкритого тексту комбінується з попереднім блоком шифртексту, що робить кожен блок унікальним, а також режим вимагає обов’язкове використання вектору ініціалізації розмір якого дорівнює розміру блоку

| DES mode | Key | IV | Open Text | Changed Text | CipherText  (OT) | CipherText  (CT) |
| --- | --- | --- | --- | --- | --- | --- |
| CBC | 14A7D67818CA18AD | 305840986309727 | I love Odessa and | I love Odessa ans | ac99141bd41da6a5fe7a937552c60d85ba6a6c6470427c32 | ac99141bd41da6a5fe7a937552c60d85edd88defed7f03fb |
| I love Odesaa and | ac99141bd41da6a5b180c8e4aceb6ad2835cf2531b34ef82 |

Отже, ми бачимо, що в режимі EBC при зміні 2 блоку відкритого тексту змінюється тільки 2 блок шифртексту, а в режимі CBC при зміні 2 блоку відкритого тексту змінюється 2 та наступний блок шифртексту