МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**РЕЖИМ РОБОТИ DES**

Дата 20.04.2024

Виконав: курсант 314 навчальної групи

cтарший солдат\_\_\_\_\_КОНОНУЧЕНКО A.В.

Перевiрив: старший викладач кафедри 33

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DES mode | Key | Open text | Cipher text | Cipher text |
| ECB | A45325FDE345682 | cadet of the 314th group  ->  vadet of the 314th group | fadce94b24c695fc9f41601170d003bf12631e74261554d68712998b7636c35e | 1261965b9646e6889f41601170d003bf12631e74261554d68712998b7636c35e |
| CBC | A45325FDE345682 | cadet of the 314th group  ->  vadet of the 314th group | 1dacbe5e2e729bc399cb60f3562141c857684d7d023dca6dc88a731efc4f0eb9 | 75334df12788884ccb9798f6bdcab24c2468968ec318c0a6cb3c8df6261d03c6 |
| CFB | A45325FDE345682 | cadet of the 314th group  ->  vadet of the 314th group | 43d0c19e63048be3549657056018131573ccb7c29c3fb3eb | 56d0c19e63048be3244b2caf495d1f0277fd42ffb4af5247 |
| OFB | A45325FDE345682 | cadet of the 314th group  ->  vadet of the 314th group | 43d0c19e63048be3e1e25f8f68499a2f55b0b7b5fb091ab7 | 56d0c19e63048be3e1e25f8f68499a2f55b0b7b5fb091ab7 |
| CTR | A45325FDE345682 | cadet of the 314th group  ->  vadet of the 314th group | 43d0c19e63048be39874eecd0f5c35299ea09f57e73dcd0c | 56d0c19e63048be39874eecd0f5c35299ea09f57e73dcd0c |

Висновок:

1. ECB (Режим електронної кодової книги)

Опис: Зміна першого символу відкритого тексту викликала зміну лише в першому блоку шифротексту. Решта блоків залишилася без змін.

Висновок: ECB не створює сильного зв’язку між різними частинами шифротексту, оскільки кожен блок шифрується окремо. Це може спростити завдання атакуючого при спробі визначити використовуваний текст або частину ключа, якщо він має достатньо шифротексту.

1. CBC (Режим зв’язування блоків шифру)

Опис: Зміна першого символу відкритого тексту вплинула на весь наступний шифротекст.

Висновок: В режимі CBC весь шифротекст сильно залежить від змін у відкритому тексті, що забезпечує більшу стійкість до спроб розшифрування та реалізує принцип лавинного ефекту.

1. CFB (Режим зворотного зв’язку шифру)

Опис: Зміна першого символу вплинула на перший блок шифротексту, але наступні блоки залишились без змін.

Висновок: CFB дозволяє шифрувати дані в реальному часі без буферизації блоків, але він вразливий до атак зі зміною даних.

1. OFB (Режим зворотного зв’язку вихідного сигналу)

Опис: Зміна першого символу відкритого тексту не викликала жодних змін у шифротексті, окрім останнього блоку.

Висновок: OFB забезпечує високу стійкість до помилок у шифротексті і не дозволяє розсипати помилки на інші блоки.

1. CTR (Режим лічильника)

Опис: Зміна першого символу відкритого тексту вплинула на весь наступний шифротекст, але лише в відповідних блоках.

Висновок: CTR дозволяє паралельне шифрування і дешифрування, що робить його відносно швидким та ефективним у великих системах.

Визначення режиму шифрування на основі змін в шифротексті

Можна визначити режим шифрування, аналізуючи, як зміни в першому символі відкритого тексту впливають на весь шифротекст. Наприклад:

ECB матиме обмежені зміни, що впливають лише на окремі блоки.

CBC та CFB покажуть зміни в усьому шифротексті, але з різним ступенем поширення змін.

OFB і CTR виявлять більш локалізовані зміни, залежно від конкретного механізму шифрування в кожному режимі.