МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**РЕЖИМИ РОБОТИ ШИФРУ DES**

Дата 24.04.2024

**Виконав:** курсант 314 навчальної групи

старший солдат\_\_\_\_\_\_\_\_\_\_\_КОКУРА І.В.

**Перевiрив:** старший викладач кафедри 33

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DES mode | Key | Open text | Cipher text | Cipher text/ |
|  |  |  |  |  |
| ECB | 34242343234231 | Actions speak louder than words  ->  Bctions speak louder than words | 538a95e9ec13668baa552ee690d167b02da8ec8c822c22fcd625333e8c0a5fb6 | 122a9617ff4e217eaa552ee690d167b02da8ec8c822c22fcd625333e8c0a5fb6 |
| CBC | 34242343234231 | Actions speak louder than words  ->  Bctions speak louder than words | 37071f147545e825ff17db5979a7c127f04913db9dfe0d07415a37af2f89a506 | fb86348aeda2a17982da25b18c88c56943bb322c85b3616a86690fbe7b4a877c |
| CFB | 34242343234231 | Actions speak louder than words  ->  Bctions speak louder than words | f267e44a536d750742a6a076e5f132810688ae4408bb93b20f7ed87e953912 | f167e44a536d7507e9f3d980e4c1da8155ee898e95bfce9eb8338d5c8e6a88a7da |
| OFB | 34242343234231 | Actions speak louder than words  ->  Bctions speak louder than words | f267e44a536d750786182bad35e667acbdf38df2dc8bcb2f40f9c6c854562e | f267e44a536d750786182bad35e667acbdf38df2dc8bcb2f40f9c6c854622e |
| CTR | 34242343234231 | Actions speak louder than words  ->  Bctions speak louder than words | f267e44a536d7507a699d08cb009b9246fec19708aadaadc719823b58b0e80 | f167e44a536d7507a699d08cb009b9246fec19708aadaadc719823b58b0e807fd7 |

На основі аналізу таблиці, можна зробити такі висновки про різні режими шифрування DES:

**1. ECB (Electronic Codebook Mode)**

Опис: Зміна першого символу відкритого тексту привела до зміни тільки першого блоку шифротексту. Решта блоків залишилася незмінною.

Висновок: ECB не забезпечує сильну залежність між різними частинами шифротексту, оскільки кожен блок шифрується незалежно. Це може дозволити атакувальнику легше визначити використовуваний текст або частину ключа при наявності достатньої кількості шифротексту.

**2. CBC (Cipher Block Chaining Mode)**

Опис: Зміна в першому символі відкритого тексту вплинула на весь наступний шифротекст.

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

**3. CFB (Cipher Feedback Mode)**

Опис: Зміна в першому символі вплинула на перший блок шифротексту, проте наступні блоки залишились незмінними.

Висновок: CFB дозволяє шифрувати дані у реальному часі без буферизації блоків, проте відкритий до атак зі зміною даних.

**4. OFB (Output Feedback Mode)**

Опис: Зміна в першому символі відкритого тексту не спричинила жодних змін у шифротексті, окрім останнього блоку.

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

**5. CTR (Counter Mode)**

Опис: Зміна в першому символі відкритого тексту вплинула на весь наступний шифротекст, але лише у 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 ідентифікувати режим шифрування, аналізуючи, як зміни в першому символі відкритого тексту впливають на весь шифротекст. Наприклад:

ECB буде мати обмежені зміни, що впливають лише на окремі блоки.

CBC та CFB продемонструють зміни у всьому шифротексті, але з різною ступенем поширення змін.

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