**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**

**ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ**

КАФЕДРА КІБЕРБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія 2»

**СТАНДАРТ ШИФРУВАННЯ ДАНИХ DES**

**Виконав:** курсант 314 навчальної групи

мол. с-нт \_\_\_\_\_\_\_\_\_\_\_\_\_ І.МАРТИНЮК

.04.2024

**Перевiрив:** викладач кафедри № 33

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

.04.2024

Київ – 2024

**ЗМІСТ**

1. РЕЖИМИ РОБОТИ АЛГОРИТМУ DES ............................................................. 3

2.АНАЛІЗ РОБОТИ РЕЖИМІВ .............................................................................. 4

3. ВИСНОВОК ........................................................................................................... 5

1. **РЕЖИМИ РОБОТИ АЛГОРИТМУ DES**

**DES** (*Data Encryption Standard*) — це симетричний алгоритм шифрування певних даних, стандарт шифрування.

Для DES рекомендовано декілька режимів:

• **ECB** (electronic code book) – режим «електронної кодової книги» (проста заміна);

• **CBC** (cipher block chaining) – режим зчеплення блоків;

• **CFB** (cipher feed back) - режим зворотного зв'язку за шифротекстом;

• **OFB** (output feed back) – режим зворотного зв'язку по виходу;

• **CTR** (counter Mode) — це режим шифрування, який працює, перетворюючи блочний шифр на потоковий.

1. **АНАЛІЗ РОБОТИ РЕЖИМІВ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Encryption mode** | **Key** | **Open text** | **Encrypted text** | **Open text w/ changes** | **Encrypted text w/ changes** |
| ECB | AC14881488AB | White pride! | a35d3d8153df101923a34af77f501dce | White pride? | a35d3d8153df1019b5b388055b1bc940 |
| CBC | AC14881488AB | White pride! | 282f02f0a79ff3095f8df67806465130 | White pride? | 282f02f0a79ff309f720c5628160697c |
| CFB | AC14881488AB | White pride! | 5bcb865a0393f7fc8fe96c6d | White pride? | 5bcb865a0393f7fc8fe96c73 |
| OFB | AC14881488AB | White pride! | 5bcb865a0393f7fcfb09211a | White pride? | 5bcb865a0393f7fcfb092104 |
| CTR | AC14881488AB | White pride! | 5bcb865a0393f7fc246febfe | White pride? | 5bcb865a0393f7fc246febe0 |

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

**Опис:** Зміна одного символу в оригінальному відкритому тексті ("!" на "?") спричинила значні зміни в шифротексті. Ці зміни виявилися тільки в кінцевій частині шифротексту.

**Висновок:** ECB шифрує кожен блок даних незалежно, тому зміни у вхідних даних прямо впливають на відповідні блоки шифротексту, що може дозволити аналіз патернів для визначення використаних даних або ключа.

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

**Опис:** Зміна символу також вплинула на кінцеву частину шифротексту. Оскільки в CBC попередній блок шифротексту використовується для шифрування наступного, ці зміни є локалізованими.

**Висновок:** Завдяки використанню попереднього шифротексту у якості частини вектору ініціалізації, CBC може бути більш стійким до атак на відтворення, але все ще можливі залежності між блоками.

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

**Опис:** Лише останні цифри в шифротексті змінилися при зміні в останньому символі відкритого тексту.

**Висновок:** CFB використовує попередній шифротекст для шифрування наступного блоку, тому зміни в останньому символі відкритого тексту мають вплив на кінцевий шифротекст.

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

**Опис:** Тут також відбулись зміни лише в останніх символах шифротексту.

**Висновок:** Оскільки OFB використовує шифротекст лише для генерації ключового потоку, будь-які зміни в відкритому тексті відображаються лише у відповідній частині шифротексту, що підвищує стійкість до помилок.

**5. CTR (Counter Mode)**

**Опис:** Зміни в шифротексті знову обмежені кінцевою частиною.

**Висновок:** В CTR використовується лічильник для генерації ключового потоку, тому зміни в останньому символі відкритого тексту відображаються відповідно в шифротексті, зберігаючи стійкість до помилок та атак.

1. **ВИСНОВОК**

Визначити режим шифрування можна, аналізуючи, як зміни в останньому символі відкритого тексту впливають на шифротекст:

**ECB** покаже зміни в конкретних блоках, які відповідають зміненому відкритому тексту.

**CBC, CFB, OFB, і CTR** продемонструють зміни в кінцевих блоках, причому ступінь впливу та характер змін може допомогти визначити конкретний режим.