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 \_\_\_\_\_\_\_\_\_\_\_\_\_БІЛАЄНКО І.О

21.04.2024

**Перевiрив:** викладач кафедри № 33

капітан \_\_\_\_\_\_\_\_\_\_\_\_Прийма О.О.

Київ – 2024

1. Виконати цикл шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 7f2a9t6u4g2s6k0l4r2t5l9m1bh в HEX форматі.

Відкритий текст - Bubble Shooter HD

Шифротекст - 6251953add3466bea75689ea8f3d2b9daa5d4d99b96bfb30 в HEX форматі.

A screenshot of a computer

Description automatically generated

Дані розшифрування:

Ключ - 7f2a9t6u4g2s6k0l4r2t5l9m1bh в HEX форматі.

Шифротекст - 6251953add3466bea75689ea8f3d2b9daa5d4d99b96bfb30

Відкритий текст - Bubble Shooter HD

A screenshot of a computer

Description automatically generated

1. Виконати цикл шифрування алгоритмом DES у режимі CBC

Дані шифрування:

Ключ - 7f2a9t6u4g2s6k0l4r2t5l9m1bh в HEX форматі.

Вектор ініціалізації (IV) - f27d2cdcadce4a7e в HEX форматі.

Відкритий текст – Idle Mining Empire

Шифротекст - 6642f1c4a15e95a326a908aff9faba92f5e51bee4bee19fc в HEX форматі.

A screenshot of a computer

Description automatically generated

Дані розшифрування:

Ключ - 7f2a9t6u4g2s6k0l4r2t5l9m1bh в HEX форматі.

Вектор ініціалізації (IV) - f27d2cdcadce4a7e в HEX форматі.

Шифротекст - 6642f1c4a15e95a326a908aff9faba92f5e51bee4bee19fc в HEX форматі.

Відкритий текст - Idle Mining Empire

A screenshot of a computer

Description automatically generated

1. Виконати цикл шифрування алгоритмом DES у режимі CFB

Дані шифрування:

Ключ - 7f2a9t6u4g2s6k0l4r2t5l9m1bh в HEX форматі.

Вектор ініціалізації (IV) - f27d2cdcadce4a7e в HEX форматі.

Відкритий текст - Solitaire Mahjong Classic

Шифротекст - d6c6786dba87e4409dc5e589a2669e53e73a4413cab1337fb18c в HEX форматі.

A screenshot of a computer

Description automatically generated

Дані розшифрування:

Ключ - 7f2a9t6u4g2s6k0l4r2t5l9m1bh в HEX форматі.

Вектор ініціалізації (IV) - f27d2cdcadce4a7e в HEX форматі.

Шифротекст - d6c6786dba87e4409dc5e589a2669e53e73a4413cab1337fb18c в HEX форматі.

Відкритий текст - Solitaire Mahjong Classic

A screenshot of a computer

Description automatically generated

**Висновок:**

Після проведення експериментів з DES у режимах CFB, CBC та ECB, я зробив кілька висновків:

1. **ECB**:
   * Цей режим простий у реалізації та розумінні, але не забезпечує високого рівня безпеки.
   * Дані, які мають однакове значення, під час шифрування у тому ж самому блоку, отримують однаковий шифротекст, що може викликати проблеми з конфіденційністю.
2. **CBC**:
   * Режим CBC використовує попередній блок шифротексту для шифрування наступного блоку, що робить його стійким до атак на патерни та підсаджування даних.
   * Він забезпечує високий рівень конфіденційності, оскільки навіть однакові блоки даних будуть мати різний шифротекст.
3. **CFB**:
   * У режимі CFB кожен блок шифрується, а потім використовується для шифрування наступного блоку даних.
   * Він дозволяє передавати блоки будь-якого розміру, що може бути корисним у певних сценаріях.

Загалом, режими CBC і CFB забезпечують вищий рівень безпеки порівняно з ECB, оскільки вони уникнуть багатьох проблем, пов'язаних з патернами у шифрованому тексті та можливістю атак. Режим CBC, зокрема, виявився найбільш ефективним для забезпечення конфіденційності даних.