**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія 2»

**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 314 навчальної групи старший солдат\_\_\_\_Р.ДІДКОВСЬКИЙ

20.04.2024

**Перевiрив:** викладач кафедри №33

капітан \_\_\_\_\_\_\_\_\_\_\_\_\_\_О.ПРИЙМА

Київ – 2024

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DES mode | Key | Open Text | Changed Text | CipherText  (Open Text) | CipherText\*  (Changed Text) |
| ECB | 14A7D67818CA18DB | I cadet Didkovskiy! | I cadet Didkovskiy!F | d0968b2236aebc7cd2beb02fbf246e86edd5cf824d331a19 | d0968b2236aebc7cd2beb02fbf246e86e45cc93479e901b1 |
| 12cadet Didkovskiy! | 1bda800debceaa13d2beb02fbf246e86edd5cf824d331a19 |
| CTR | 14A7D67818CA18DB | I cadet Didkovskiy! | I cadet Didkovskiy!F | fdcbfd3f51ad6a7fef81aa2b3e20f9d8fa7bf9 | fdcbfd3f51ad6a7fef81aa2b3e20f9d8fa7bf948 |
| 12cadet Didkovskiy! | 85d9fd3f51ad6a7fef81aa2b3e20f9d8fa7bf9 |
| CBC | 14A7D67818CA18DB | I cadet Didkovskiy! | I cadet Didkovskiy!F | 10fd458653068dac41e67112bc32cec00bfca6871ea4dd70 | 10fd458653068dac41e67112bc32cec0191e10b710e85905 |
| 12cadet Didkovskiy! | e376768c180395d7ead5d92681e1963a333d73c2e9ba2d93 |
| CFB | 14A7D67818CA18DB | I cadet Didkovskiy! | I cadet Didkovskiy!F | fdcbfd3f51ad6a7f257cd7066e576d9427366f | fdcbfd3f51ad6a7f257cd7066e576d9427366f44 |
| 12cadet Didkovskiy! | 85d9fd3f51ad6a7f428f28d6169c49cd38f44c |
| OFB | 14A7D67818CA18DB | I cadet Didkovskiy! | I cadet Didkovskiy!F | fdcbfd3f51ad6a7fb6f77be04bcdc547fd8492 | fdcbfd3f51ad6a7fb6f77be04bcdc547fd849258 |
| 12cadet Didkovskiy! | 85d9fd3f51ad6a7fb6f77be04bcdc547fd8492 |

**Висновок:**

ECB (Режим електронної кодової книги): ECB не міцно пов'язує різні частини шифротексту, оскільки кожен блок обробляється окремо, що може полегшити атаки на розшифрування.

CBC (Режим зв’язування блоків шифру): CBC забезпечує сильну залежність між відкритим текстом та шифротекстом, що забезпечує високу стійкість та лавинний ефект.

CFB (Режим зворотного зв’язку шифру): CFB дозволяє шифрування в реальному часі, але вразливий до атак зі зміною даних через його особливості.

OFB (Режим зворотного зв’язку вихідного сигналу): OFB забезпечує стійкість до помилок і не поширює їх на інші блоки.

CTR (Режим лічильника): CTR ефективний та швидкий в застосуванні через паралельність процесу шифрування та дешифрування.