МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

Дата 20.04.2024

Виконав: курсант 314 навчальної групи

старший солдат\_\_\_\_\_\_\_\_\_\_\_БУХОВЦЕВ Г.І.

Перевiрив: старший викладач кафедри 33

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

| DES mode | key | Open text | (changed text) | CypherText  (open text) | CypherText  (changed text) |
| --- | --- | --- | --- | --- | --- |
| ECB | 0E329232EA6D0D90 | Слава Україні | злава Україні | 829cd2e6b974d2931ff4dbb7f025994d | 53c3e5bfb574b23a1ff4dbb7f025994d |
| Слава Україну | 829cd2e6b974d2931ff4dbb7f025994d | 829cd2e6b974d293fda949e2783ecc85 |
| CBC | злава Україні | e90415927fb518c079640f4b59a2445e | c727c2fe038443d3f0e4eb6a05454dd4 |
| Слава Україну | e90415927fb518c079640f4b59a2445e | e90415927fb518c0c36c57338a8306a5 |
| CFB | злава Україні | 9192a238c2cc7ec2999bb9f3f7 | 8792a238c2cc7ec2222faf54af |
| Слава Україну | 9192a238c2cc7ec2999bb9f3f7 | 9192a238c2cc7ec2999bb9f3e2 |
| OFB | злава Україні | 9192a238c2cc7ec23f758c80c7 | 8792a238c2cc7ec23f758c80c7 |
| Слава Україну | 9192a238c2cc7ec23f758c80c7 | 9192a238c2cc7ec23f758c80d2 |
| CTR | злава Україні | 9192a238c2cc7ec266a22d55f2 | 8792a238c2cc7ec266a22d55f2 |
| Слава Україну | 9192a238c2cc7ec266a22d55f2 | 9192a238c2cc7ec266a22d55e7 |

Таблиця 1.1

Висновок:

* Режим ECB має блоки по 16 біт, що дозволяє встановити, що при будь-якій зміні відкритого тексту розмір блоків зашифрованого тексту буде кратним 16 бітам.
* Режим CBC можна ідентифікувати, оскільки при зміні першої букви відкритого тексту шифротекст повністю змінюється.
* Режим CFB можна впізнати, оскільки при зміні першої букви відкритого тексту змінюються перші символи зашифрованого тексту, а також середина зашифрованого тексту.
* Режими OFB і CTR можна впізнати, оскільки при зміні першого або останнього символу відкритого тексту шифротекст змінюється на 1 байт символу на початку або в кінці.
* Режими OFB і CTR можна відрізнити, якщо змінити середину відкритого тексту: при зміні середини відкритого тексту шифротекст OFB повністю змінюється з моменту зміни символу відкритого тексту, у той час як у режимі CTR змінюється кількість байтів, що відповідають зміненому відкритому тексту.