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\_\_\_\_\_\_\_\_\_\_\_ІВАНОВ І.В.

Перевiрив: старший викладач кафедри 33

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

| DES mode | key | Open text | (changed text) | CypherText  (open text) | CypherText  (changed text) |
| --- | --- | --- | --- | --- | --- |
| ECB | 0E329232EA6D0D73 | i love cryptology | u love cryptology | 49f79d7d92f505a6900e1a98fd386a97a55346d971c0cb9c | 06fe19266d4f7049900e1a98fd386a97a55346d971c0cb9c |
|  |  | i love cryptologu | 49f79d7d92f505a6900e1a98fd386a97a55346d971c0cb9c | 49f79d7d92f505a6900e1a98fd386a970c8a7687c07a3f78 |
| CBC |  |  | u love cryptology | a85b47bfcc2dd601924c25bf0056d123bfb99221a7dc8360 | 3f4edeb05841195f64148655ecc383bfa1cb64b7f2e72f48 |
|  |  | i love cryptologu | a85b47bfcc2dd601924c25bf0056d123bfb99221a7dc8360 | a85b47bfcc2dd601924c25bf0056d123cd278e5eda52fabb |
| CFB |  |  | u love cryptology | 1137a122f18bce50d9b633e250a7f7e3e5 | 0d37a122f18bce5097fa2fbe1484fac699 |
|  |  | i love cryptologu | 1137a122f18bce50d9b633e250a7f7e3e5 | 1137a122f18bce50d9b633e250a7f7e3e9 |
|  |  | love my mom | iove my mom | 1478bb28a7839713b80602 | 1178bb28a7839713b0c6f8 |
|  | love my mom | love my mon | 1478bb28a7839713b80602 | 1478bb28a7839713b80601 |
| OFB |  |  | u love cryptology | 1137a122f18bce5016c3e2f74e3fba45eb | 0d37a122f18bce5016c3e2f74e3fba45eb |
| i love cryptologu | 1137a122f18bce5016c3e2f74e3fba45eb | 1137a122f18bce5016c3e2f74e3fba45e7 |
| i love crypt0logy | 1137a122f18bce50cd7b32f21d6fc50d43 | 1137a122f18bce5016c3e2f7113fba45eb |
| CTR | u love cryptology | 1137a122f18bce50cd7b32f21d6fc50d43 | 0d37a122f18bce50cd7b32f21d6fc50d43 |
| i love cryptologu | 1137a122f18bce50cd7b32f21d6fc50d43 | 1137a122f18bce50cd7b32f21d6fc50d4f |
| i love crypt0logy | 1137a122f18bce50cd7b32f21d6fc50d43 | 1137a122f18bce50cd7b32f2426fc50d43 |

Таблиця 1.1

Висновок:

* Режим ECB має блоки по 16 біт, тому можна ідентифікувати, якщо при будь-якій зміні відкритого тексту - розмір блоків зашифрованого тексту кратне 16 біт.
* Режим CBC можна ідентифікувати, якщо при зміні першої букви відкритого тексту - шифротекст повністю змінюється.
* Режим CFB можна ідентифікувати, якщо при зміні першої букви відкритого тексту змінюється перші символи зашифрованого тексту, а також середина зашифрованого тексту.
* Режим OFB, CTR можна ідентифікувати, якщо при зміні першого або останнього символу відкритого тексту - шифротекст змінюється на 1 байт символу на початку або в кінці.
* Режими OFB та CTR можна відрізнити, якшо змінити середину відкритого тексту, а саме: при зміні середини відкритого тексту - шифротекст OFB повністю змінюється з моменту зміни символу відкритого тексту, в свою чергу CTR змінює кількість байт відповідну зміненого відкритого тексту.