**ЗВІТ ЗА ПРАКТИКУ З ПРЕДМЕТУ “ПРИКЛАДНА КРИПТОЛОГІЯ”**

**ЗА 22.04.2024**

**ПАЛІЙ М.В.**

**314 ГРУПА**

| **DES mode** | **KEY** | **OPEN txt** | **CHAGED txt** | **CYPHERtxt** | **CYPHERtxt** |
| --- | --- | --- | --- | --- | --- |
| ***CBC*** | 2B7E151628AED2A6 | **you make life** | you make lift | cd0f0462d28f61ad1e2ab777a40b7018 | cd0f0462d28f61adf91c5f3e0d4727b0 |
| 2B7E151628AED2A6 | **you make life** | dou make life | cd0f0462d28f61ad1e2ab777a40b7018 | 161cad92153fee73b0529ce1c44e960b |
| ***CFB*** | 2B7E151628AED2A6 | **you make life** | you make lift | 7e43b64f2954007c5439806c64 | 7e43b64f2954007c5439806c75 |
| 2B7E151628AED2A6 | **you make life** | dou make life | 7e43b64f2954007c5439806c64 | 6343b64f2954007c354868f154 |
| ***OFB*** | 2B7E151628AED2A6 | **you make life** | you make lift | 7e43b64f2954007cc7ed96b9a2 | 7e43b64f2954007cc7ed96b9b3 |
| 2B7E151628AED2A6 | **you make life** | dou make life | 7e43b64f2954007cc7ed96b9a2 | 6343b64f2954007cc7ed96b9a2 |
| ***CTR*** | 2B7E151628AED2A6 | **you make life** | you make lift | 7e43b64f2954007ca552b3bf68 | 7e43b64f2954007ca552b3bf79 |
| 2B7E151628AED2A6 | **you make life** | dou make life | 7e43b64f2954007ca552b3bf68 | 6343b64f2954007ca552b3bf68 |
| ***ECB*** | 2B7E151628AED2A6 | **you make life** | you make lift | ad2d3ea777bc81f7ef2b606b34e6b415 | ad2d3ea777bc81f79bdfce40c3fc5128 |
| 2B7E151628AED2A6 | **you make life** | dou make life | ad2d3ea777bc81f7ef2b606b34e6b415 | d87bbc901572cd18ef2b606b34e6b415 |

**Висновок:**

Після аналізу таблиці можна зробити кілька висновків:

Заміна першої та останньої букв у текстах впливає на кінцевий шифротекст у залежності від типу шифрування і режиму. Наприклад, у режимі ECB заміна першої букви у відкритому тексті призведе до повної зміни блока шифрування, тому весь блок шифрування буде різним. У режимах CBC, CFB, OFB та CTR зміна першої букви вплине лише на відповідний блок шифрування.

Отже, таблиця демонструє різні результати шифрування в різних режимах та різницю у величині шифртексту в залежності від режиму шифрування та довжини відкритого тексту.