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\_\_\_\_\_\_\_\_\_\_\_СІДНЕНКО Д.В.

**Перевiрив:** старший викладач кафедри 33

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DES mode | Key | Open Text | Cipher Text | Cipher Text(with  changes) |
| ECB | C2C1E96A4BF  EGJGEARGUB  ERGUIABGAG  VBSGEYHGBS  GVBANEGHDH  G | Leonardo da  Vinci =>  Neonardo da  Vinck | 4f52c7dbd53ba  e6b52033a27b3  53edb068b60db  1aae41b92 | 00b3b6eb25e78  59952033a27b3  53edb0b83c92b  ae439cea3 |
| CBC | C2C1E96A4BF  EGJGEARGUB  ERGUIABGAG  VBSGEYHGBS  GVBANEGHDH  G | Leonardo da  Vinci =>  Neonardo da  Vinck | e433a2e62d6b1  9efdb368f772b9  67320c1609b82  573cd3b5 | c0ec366610931  81df115b42bb6  19cbc26ab9289  0ce772d0d |
| CFB | C2C1E96A4BF  EGJGEARGUB  ERGUIABGAG  VBSGEYHGBS  GVBANEGHDH  G | Leonardo da  Vinci =>  Neonardo da  Vinck | 184e2a29edf40  28d47b50822a7  7e4cb90b | 1a4e2a29edf40  28d5a71ada7ce  652bf6cf |
| OFB | C2C1E96A4BF  EGJGEARGUB  ERGUIABGAG  VBSGEYHGBS  GVBANEGHDH  G | Leonardo da  Vinci =>  Neonardo da  Vinck | 184e2a29edf40  28dd176658d64  c5fcbb91 | 1a4e2a29edf40  28dd176658d64  c5fcbb93 |
| CTR | C2C1E96A4BF  EGJGEARGUB  ERGUIABGAG  VBSGEYHGBS  GVBANEGHDH  G | Leonardo da  Vinci =>  Neonardo da  Vinck | 184e2a29edf40  28d55ef796487  772daf4a | 1a4e2a29edf40  28d55ef796487  772daf48 |

**Висновок**

Цей текст містить шифрований вміст, який було зашифровано за допомогою різних режимів шифрування DES (Data Encryption Standard). DES є стандартом шифрування, який використовується для захисту конфіденційності даних. Режими шифрування, які використовуються тут, включають ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback) і CTR (Counter).

ECB (Electronic Codebook):

**ECB (Electronic Codebook):**

У режимі ECB кожен блок даних шифрується незалежно один від одного.

Розмір блоку вхідних даних та шифротексту дорівнює розміру ключа, який для DES становить 64 біти.

Під час шифрування однакові блоки вхідних даних перетворюються на однакові блоки шифротексту.

Однакові блоки даних у вихідному шифротексті можуть розпізнаватись, що дозволяє атакувачам використовувати цю інформацію для аналізу даних.

**CBC (Cipher Block Chaining):**

У режимі CBC перед кожним блоком даних вхідного тексту використовується вектор ініціалізації (IV), який XOR-юється з блоком перед шифруванням.

Розмір блоку даних та шифротексту також дорівнює розміру ключа, тобто 64 біти.

Цей режим має властивість дифузії, що робить його більш стійким до атак на визначення зразків.

Для CBC потрібно додатково передавати вектор ініціалізації, що збільшує обсяг передачі даних.

**CFB (Cipher Feedback):**

У режимі CFB використовується режим зворотного зв'язку, де блок шифрується, а потім XOR-юється з наступним блоком даних перед шифруванням.

Розмір блоку даних та шифротексту визначається обраною довжиною зворотного зв'язку, а не розміром ключа.

Цей режим дозволяє передавати менше інформації про структуру вихідного тексту, але може призвести до помилок при неправильній ініціалізації.

**OFB (Output Feedback):**

У режимі OFB вихід шифрується, а не вхід, і отриманий результат застосовується для шифрування наступного блоку даних.

Розмір блоку даних та шифротексту також визначається довжиною зворотного зв'язку, а не розміром ключа.

OFB надає незалежність від ініціалізації, але не дозволяє коректно декодувати повідомлення при втраті даних.

**CTR (Counter):**

У режимі CTR використовується лічильник, який генерує послідовність значень для XOR-ювання з вхідними даними.

Розмір блоку даних та шифротексту також дорівнює розміру ключа.

Цей режим дозволяє паралельне шифрування та декодування даних.

Щоб відрізнити ці режими один від одного, можна звернути увагу на спосіб, яким обробляється вихідний шифротекст. Кожен режим має свої особливості в генерації та обробці цього шифротексту, що дозволяє їм відрізнятися один від одного. Також, враховуючи, що деякі режими вимагають вектора ініціалізації або мають власні правила для генерації шифрованих блоків, можна визначити конкретний режим за цими параметрами.

Можна ідентифікувати режим шифрування, аналізуючи, як зміни в першому символі відкритого тексту впливають на весь шифротекст. Наприклад:

ECB буде мати обмежені зміни, що впливають лише на окремі блоки.

CBC та CFB продемонструють зміни у всьому шифротексті, але з різною ступенем поширення змін.

OFB і CTR виявлять більш локалізовані зміни, залежно від точного механізму шифрування в кожному режимі.