Segurança de Dados - Assignment 3

Pedro Malainho PG61005

1.

A. The answer is in the decrypt function of Q1.py within the zip file.

B. The answer is in the key_generator function of Q1.py within the zip file.

C. A Key Derivation Function (KDF) enables both parties to securely derive the same key from a shared secret, but it introduces challenges such as securely exchanging the secret, managing KDF parameters (e.g., salt and iterations), and preventing key reuse or performance issues.

2.

Since we knew there were four words — "STOP," "START," "REMOVE," and "TRANSFER" — I started by filtering the encrypted file, creating a dictionary in which I separated the hexadecimal values by their size in bytes (4, 5, 6, and 8).

I then used this dictionary to find the key. Knowing that three keys were used and that, after applying a set to my dictionary, I obtained 12 encrypted words, I assumed that there was a keystream to encrypt the four words, repeated three times.

To discover the possible keystreams, I used the largest encrypted word, "TRANSFER," with 8 bytes. All I had to do was apply the XOR operation between the three encrypted words with that size and "TRANSFER" in bytes, thus obtaining three keys, which I could then use to decrypt the remaining messages.

As keystreams que obti foram:

- 41875ec8d07cefea
- 400088bb4a42bab2
- c9b3e8e63b1ea3

Encrypted	Keystream	Decrypted
9ae7a7b6	41875ec8d07cefea	STOP
12d31198	400088bb4a42bab2	STOP
1354c7eb	c9b3e8e63b1ea3f7	STOP
1354c9e91e	41875ec8d07cefea	START
9ae7a9b46f	c9b3e8e63b1ea3f7	START
12d31f9a84	400088bb4a42bab2	START
13c213878639	41875ec8d07cefea	REMOVE
9bf6a5a96d5b	c9b3e8e63b1ea3f7	REMOVE
1245c5f41c07	400088bb4a42bab2	REMOVE
1452c9f51904ffe0	400088bb4a42bab2	TRANSFER
15d51f86833aaab8	41875ec8d07cefea	TRANSFER
9de1a9a86858e6a5	c9b3e8e63b1ea3f7	TRANSFER

3.

To discover the plaintext, I used crib-dragging on the six ciphertexts, as we know that they were all encrypted using the same keystream. I started with guesses such as letters, then words, and when several different texts at the same offset produced readable fragments, I confirmed the guess. I repeated this until I had reconstructed the complete plaintext. This results in a **result.txt** file that recorded all attempts, and the last line has the plaintext of ciphertext 6:
"OBJETIVOSDEDESENVOLVIMENTOSUSTENTAVEL"