Programming Homework 2B

Aaryan, CO21BTECH11001

The file named "`findKey_hw2b.py`" is a python program to find the keys and the secret message using a meet-in-the-middle attack.

Here are the steps involved in the program:

1. Read the plaintexts and ciphertexts from the files and convert them to bytes.

2. Use the first (plaintext, ciphertext) pair to find the keys using a meet-in-the-middle attack.

3. In the attack, we prepare two lists as follows:

    a. `plain_to_cipher1` : We iterate over all the possible values of the first key (say k1), which is $[0, 2^{16} - 1]$. Then k1 is expanded to a 128-bit key using the expansion subroutine.
    The plaintext is encrypted using the expanded key and finally, the pair $(cipher1,\ expanded\_key)$ is stored in the list `plain_to_cipher1`.

    b. `final_cipher_to_cipher1` : We iterate over all the possible values of the second key (say k2), which is $[0, 2^{16} - 1]$. Then k2 is expanded to a 128-bit key using the expansion subroutine.
    The final ciphertext is decrypted using the expanded key and finally, the pair $(cipher1,\ expanded\_key)$ is stored in the list `final_cipher_to_cipher1`.

4. Then, both of the above mentioned lists are sorted in increasing order of the ciphertext.

5. To find the keys, we iterate over both of the lists.

    While iterating, if we find a mismatch of the ciphertexts, we increment the pointer of the list corresponding to the lower value of ciphertext. We continue this process until we find a match.

    This step is done in a linear amount of time since both of the lists are sorted.

Time complexity: $O(N * logN)$ where $N = 2^{16}$.

After finding the keys, we find the secret message by decrypting the last ciphertext using the second key and then decrypting this result using the first key.

Note: To run the program, execute the command: "`python3 findKey_hw2b.py`".

Keys (hexadecimal string format):

Plain to cipher key: "b294df5a0b9f7dd7e26de7bd9e0af1ad"
Cipher to cipher key: "1694c35a7003c61f8fd5e70594684e53"
(excluding the quotes)

Secret message: "paddlingcanoeist" (excluding the quotes).