Task 3: Analyze the time and memory complexity of the attack compared with the naive exhaustive key search.

a) What is the key space for the mini block cipher*?*

The key space represents the number of possible keys. It is calculated 2 to the key length/size power. For mini block cipher such as Mini-AES is 2^{16} equals to 65,536 possible keys. [1]

b) Image the mini block cipher is executed twice to generate a cipher text. It is called double mini cipher block. We need a key in 32 bits. The first 16 to the first mini block cipher, the remaining 16 to the second mini block cipher. The meet in the middle attack is to match the state for the first encryption of mini block cipher and the second decryption mini block. How many operations are needed to such attack?

This plain text attack generally targets block cipher that uses multiple rounds of encryption. This can help reduce the number of brute-force permutations required to decrypt text that was encrypted by more than one key. [2]

In a double mini block cipher, the message/plaintext is encrypted two times using two different 16-bit keys (For example $\mathbf{K_1}$ & $\mathbf{K_2}$).

- Each Mini block has a 16-bit key
- The full key is 32 bits which splits into two 16-bit keys).
- For Key 1 we can try all 2^{16} possible values. The Transitional state is stored after Encryption
- For Key 2, we can try all 2^{16} possible values. Check if the decryption results match.

The total number of operations is $2^{16}+2^{16} = 2^{16+1}=\underline{\mathbf{2^{17}}}$ which equals to about 131,072. This is way more efficient than the brute attack which would use 2^{32} operations

c) If we do exhaustive key search for the double mini block cipher, how many operations are needed?

The formula for the keys is if key length for each of the two keys is k, then the total number of possible keys for each is 2^k. Since are working with a double mini block there are two keys involved.

In order to calculate the number of operations we first start with the keys. Since there are 2 keys we would need the combinations of k_1 and k_2, we need $2^k + 2^k = 2^{2k}$ operations.

Sample Calculations:

- Let's assume for the first use case that the key size k=6 bits for a double mini block cipher.
  - $2^{2k}=2^{2\times6}=2^{12}=4{,}096$ operations

- Let's assume for the second use case the key size k=8 bits for a double mini block cipher.
    - $2^{2k}=2^{2\times8}=2^{16}=65{,}536$ operations

[3]

d) What is the tradeoff for the MITM attack (speed, memory, etc.)?

After a deep analysis of the upside to a MITM attack, it has some efficiencies that are better than an exhaustive key search. For Instance, the speed of processing a MITM is much faster than brute (exhaustive key search). There are some drawbacks. MITM requires a bit more storage and is a complex solution when dealing with larger key possibilities.

Resources

[1][Stanford-URL]
[2][MIT Hands-on 6: Cryptography and Certificates - URL
[3] Jean - Philippe Aumasson,
Serious Cryptography: A Practical Introduction to Modern Encryption 2017 (Chapter 4)
https://theswissbay.ch/pdf/Books/Computer%20science/Cryptography/SeriousCryptography.pdf