Cryptography and Security 2017

Exercise Sheet 8

Exercise 1 Attack Against the OFB Mode

Assume that someone sends encrypted messages by using AES in the OFB mode of operation with a secret (but fixed) IV value.

1. Show how to perform a known plaintext attack in order to decrypt transmitted messages.
2. Is it better with the CFB mode?
3. What about the CBC mode?

Exercise 2 RC4 Biases

The RC4 pseudorandom number generator is defined by a state and an algorithm which updates the state and produces an output byte. In RC4, a state is defined by

- two indices i and j in $\mathbf{Z}_{256}$;
- one permutation S of $\mathbf{Z}_{256}$.

By abuse of notation we write $S(x)$ for an arbitrary integer x as for $S(x \bmod 256)$. The state update and output algorithm works as follows:

1: $i \leftarrow i + 1$
2: $j \leftarrow j + S(i)$
3: exchange the values at position i and j in table S
4: output $z_i = S(S(i) + S(j))$

1. Assume that the initial S is a random permutation with uniform distribution and that i and j are set to 0.

   What is the probability that $[S(1) \neq 2 \text{ and } S(2) = 0]$?
2. If $S(1) \neq 2$ and $S(2) = 0$ hold, show that the second output z_2 is always 0.
3. In other cases, we assume that $z_2 = 0$ with probability close to $1/256$. Deduce $p = \Pr[z_2 = 0]$. What do you think of this probability?

Exercise 3 Attack on 2K-3DES

1. What are the block length and the key length in DES? What is the *memory* and *time* complexity of the key recovery exhaustive search? Is it a *known plaintext* or a *chosen ciphertext* attack? What is the complexity in terms of *data* (the number of *known plaintexts* or *chosen ciphertexts* pairs needed) ?

2. Double DES is defined by

$$y = \mathsf{DES}_{K_1}\left(\mathsf{DES}_{K_2}(x)\right).$$

Explain how the meet-in-the-middle attack works. What is the *memory* and *time* complexity ? Is it a *known plaintext* or a *chosen ciphertext* attack? What is the complexity in terms of *data* (the number of *known plaintexts* or *chosen ciphertexts* pairs needed) ?

3. Two-key triple DES is defined by

$$y = \mathsf{DES}_{K_1}\left(\mathsf{DES}_{K_2}^{-1}\left(\mathsf{DES}_{K_1}(x)\right)\right).$$

By preparing a dictionary of all $(\mathsf{DES}_k^{-1}(0), k)$ pairs, show that we can break this using many chosen plaintexts and within a time/memory complexity similar to in the previous question.

Hint: Make an exhaustive search on K_1, i.e., guess K_1, do something, then use the dictionary to recover K_2.