Introduction to cryptology
Exercises#2

2019-03-21

Exercise 1: Hash function generic attacks

Q. 1:

1. Give the definition of a first preimage attack.
2. Describe an algorithm computing a first preimage of a given target.
3. Estimate its average-case complexity

Q. 2:

1. Give the definition of a second preimage attack.
2. Describe an algorithm computing a second preimage of a given target.
3. Estimate its average-case complexity

Q. 3:

1. Give the definition of a collision attack.
2. Describe an algorithm computing a collision. You may use any abstract data structure of your choice, but you must mention the assumptions made on the cost of its elementary operations.
3. Estimate its average-case complexity

Exercise 2: Birthday attacks for CBC and CTR modes

In the following, $E : \{0,1\}^{\kappa} \times \{0,1\}^n \to \{0,1\}^n$ is a block cipher.

Q. 1: Give the definitions of the CBC and CTR modes.

We make the simplifying hypothesis that if $F \star \to \{0,1\}^n$ is a "random function" with arbitrary domain (that is, all the outputs of F are uniformly and independently drawn at random from $\{0,1\}^n$), then the expected number of colliding pairs in the finite sequence $F(x_0)$, $F(x_1), \ldots,$ $F(x_{N-1})$ when all x_is are distinct is $\approx N^2/2^n$.

Q. 2: How long should the above sequence be for one to hope to have one collision among its elements with high probability?

Q. 3: Suppose one wishes to distinguish between the above sequence and the keystream produced by E in counter mode. Using the fact that $E(k, \cdot)$ is invertible for any k, what can you say about collisions in this keystream? How long should the sequence be for one to distinguish the two cases with high probability?

Q. 4: Given the sequence of ciphertext blocks of a single message encrypted with CBC, what can be deduced about the plaintext blocks if two ciphertext blocks are equal? Does this property still holds if the sequence is made of the concatenation of encryptions of more than one message?

Q. 5: How many blocks need to be encrypted for one to observe two equal ciphertext blocks with high probability?

Q. 6: Based on your answers to the above questions, give a recommendation for the maximal number of blocks that should be encrypted with CTR or CBC with a single key. Explain why changing the key may indeed prevent the attacks.