Introduction to cryptology
TD#3

2019-W08,...

Exercise 1: Symmetric modes of operation *(Exam '18)*

In the following questions, $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ is a block cipher. We suppose that E is a "good" cipher, in the sense that for every key k, $E(k,\cdot)$ behaves like a random permutation.

Q. 1: In order to encrypt a message m of more than n bits with E, one proposes to use the following mode: pad m so that its length is equal to $l \times n$ for some l; write the resulting message as the concatenation $m_1||\dots||m_l$, with all the blocks m_is being n-bit long; for all i, encrypt the block m_i with the key k and initialization vector c_0 as $c_i = E(k, m_i \oplus c_{i-1})$.

1. What is the name of this mode?
2. Give the decryption procedure, that from $c_0||\dots||c_l$ and k returns $m1||\dots||m_l$.

Q. 2: We recall (briefly) that a good mode of operation must be such that distinguishing the encryption of two messages m and m' of equal length is hard, while being given prior access to chosen-plaintext encryptions.

1. Is the mode of the previous question good if c_0 is set to a constant?
2. Is the mode of the previous question good if c_0 is implemented as a randomly initialized global counter? That is, the value of c_0 used to encrypt the i^{th} message is set to $\mathsf{IV} + i \mod 2^n$, where the initial value of the counter IV is chosen uniformly at random (i.e. $\mathsf{IV} \xleftarrow{\$} \{0,1\}^n$).
3. Is the mode of the previous question good if c_0 is implemented as the encryption (with a key independent from the encryption key of the mode itself) of a global counter initialised to zero? That is, the value of c_0 used to encrypt the i^{th} message is set to $E(k', (i \mod 2^n))$, with $k' \xleftarrow{\$} \{0,1\}^\kappa$ a secret key.

Q. 3: One proposes a variant of the above mode, where the encryption of $m_1||\dots||m_l$ with the key k and initialization vector x_0 is defined for all i as $c_i = m_i \oplus x_i$; $x_i = E(k, x_{i-1})$.

1. Give the decryption procedure for this mode.
2. Based on your knowledge of mode of operations, explain why this is a good mode if x is implemented as a global variable initialized to zero for the first message and not reset between different messages. (For instance, this means that if one starts by encrypting the two two-block messages $m_1||m_2$ and $m'_1||m'_2$, one has $c'_2 = m'_2 \oplus E^4(k,0)$, with $E^4(k,0) = E(k, E(k, E(k, E(k,0))))$.)

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.

Exercise 3: 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