Introduction to cryptology
TD#3

2021-W11,...

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 informally 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 $m_1||\ldots||m_l$, 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 $c_0||\ldots||c_l$ and k returns $m_1||\ldots||m_l$.

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. In all of the following questions, you must either give an efficient attack in a meaningful model or convincingly argue about the security based on your knowledge about modes of operation.

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 $m_1||\ldots||m_l$ 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: Hash functions *(Exam '19)*

In the following questions, $\mathcal{H} : \mathcal{I} \rightarrow \{0,1\}^n$ is a cryptographic hash function, where $\mathcal{I} = \bigcup_{\ell=0}^{2^N} \{0,1\}^\ell$. We recall the two following definitions:

— A *second preimage attack* on $\mathcal{H}$ is an algorithm that on input $m \in \mathcal{I}$ returns $m' \neq m \in \mathcal{I}$ s.t. $\mathcal{H}(m') = \mathcal{H}(m)$.

— A *collision attack* on $\mathcal{H}$ is an algorithm that returns m, $m' \neq m \in \mathcal{I}$ s.t. $\mathcal{H}(m) = \mathcal{H}(m')$.

Q. 1:

1. Give an algorithm for a second preimage attack. What is its expected running time (in function of n) for a perfectly random function $\mathcal{H}$ (no justification is necessary)?
2. What is the average complexity of a collision attack for a perfectly random function $\mathcal{H}$?
3. Give the specifications of a hash function $\mathcal{H}' : \mathcal{I} \rightarrow \{0,1\}^n$ for which every pair of distinct messages forms a collision. Is it possible to efficiently find second preimages for this function?

We informally call a hash function $\mathcal{H}$ *preimage-resistant* (resp. *collision-resistant*) if there is no "efficient" (first or second) preimage attack (resp. collision attack) on $\mathcal{H}$.

Q. 2:

1. Show that an adversary having a black box access to an efficient second preimage attack can perform a "similarly efficient" collision attack[1]. Is the converse true?
2. Is it possible for a hash function to be collision-resistant but not preimage-resistant?
3. Let $\mathcal{H}$ be such that the best collision attack on it is a generic attack. What can you say about the complexity of preimage attacks on $\mathcal{H}$?

[1] If this statement were expressed formally, what we want would be a reduction whose time complexity is polynomial in the inputs.