CS:6160 CRYPTOLOGY

TUTORIAL 3

Instructions

- These questions are part of your tutorial. We will keep adding more questions.

(1) Question 3.20 : Consider a stateful variant of CBC-mode encryption where the sender just increments IV by 1 each time a message is encrypted rather than choose an IV at random each time. S.T. that the scheme is not CPA-secure.

(2) Let $\Pi = (Gen, Enc, Dec)$ be the stateless CTR mode of encryption and $\tilde{\Pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$ be the encryption scheme that is identical to Π except that a truly random function is used in place of F_k. P.T.

$$|Pr[PrivK^{cpa}_{\mathcal{A},\Pi}(n) = 1] - Pr[PrivK^{cpa}_{\mathcal{A},\tilde{\Pi}}(n) = 1]| \leq negl(n).$$

(3) Question 3.21: What is the effect of a single-bit error in the ciphertext when using the CBC, OFB, and CTR modes of operation?

(4) Question 3.22: What is the effect of a dropped ciphertext block (e.g: if the transmitted block $c_1, c_2, c_3, \ldots$ is received as $c_1, c_3, \ldots$) when using CBC, OFB, CTR modes?

(5) Let F be a PRF. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. In each case Gen outputs a uniform $k \in \{0,1\}^n$ and $[i]_2$ denotes the $\frac{n}{2}$-bit binary encoding of i.

(a) To authenticate a message $m = m_1 \ldots m_\ell$, where $m_i \in \{0,1\}^n$, compute

$$t := F_k(m_1) \oplus \ldots F_k(m_\ell).$$

(b) To authenticate a message $m = m_1 \ldots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, compute

$$t := F_k([1]_2||m_1) \oplus \ldots F_k([\ell]_2||m_\ell).$$

(c) To authenticate a message $m = m_1 \ldots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, choose uniform $r \leftarrow \{0,1\}$ and compute

$$t := (r, F_k(r) \oplus F_k([1]_2||m_1) \oplus \ldots F_k([\ell]_2||m_\ell)).$$

(6) Let $\Pi = (Gen, MAC, Verify)$ be a secure MAC that uses canonical verification. Prove that Π is a strong MAC.

(7) Question 4.13 : We explore what happens when the basic CBC-MAC construction is used with messages of different lengths.
- Say the sender and receiver do not agree on the message length in advance, but the sender is careful to only authenticate messages of length $2n$. Show that an adversary can forge a valid tag on a message of length $4n$.
- Say the receiver only accepts 3-block messages, but the sender authenticates messages of any length a multiple of n. Show that an adversary can forge a valid tag on a new message.

(8) Question 4.14 : Prove that the following modifications of basic CBC-MAC do not yield a secure MAC (even for fixed-length messages):
- MAC outputs all blocks $t_1, \ldots, t_\ell$ rather than t_ℓ. ($Verify$ only checks whether t_ℓ is correct.)
- A random initial block is used each time a message is authenticated.

(9) Show that appending the message length to the end of the message before applying basic CBC-MAC does not result in a secure MAC for arbitrary-length messages.

(10) Question 4.25: Let F be a strong pseudorandom permutation, and define the following fixed-length encryption scheme: On input a message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, Enc chooses a uniform $r \in \{0,1\}^{n/2}$ and $c := F_k(m \circ r)$. Prove that this scheme is CCA-secure, but is not an authenticated encryption scheme.

November 1, 2022; Dept of CSE, IIT Hyderabad