E0 235 : Cryptography	**Question Set**
Tutorial 1	
Instructor: Arpita Patra	*Feb 08, 2016*

Question 1

Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space M, every $m, m' \in M$, and every $c \in C$:

$$\mathsf{Pr}[\ M = m \mid C = c\ ] = \mathsf{Pr}[\ M = m' \mid C = c\ ].$$

Question 2

When using the one-time pad (Vernam's cipher) with the key $k = 0^l$, it follows that $\mathsf{Enc}_k(m) = k \oplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^l$ (i.e., to have Gen choose k uniformly at random from the set of non-zero keys of length l). Is this an improvement? In particular, is it still perfectly secret? Prove your answer. If your answer is positive, explain why the one-time pad is not described in this way. If your answer is negative, reconcile this with the fact that encrypting with 0^l doesn't change the plaintext.

Question 3

Let G be a pseudorandom generator where $|G(s)|\ >\ 2 \cdot |s|$.

(a) Define $G'(s) \overset{def}{=} G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?

(b) Define $G'(s) \overset{def}{=} G(s_1 \cdots s_{n/2})$, where $s = s_1 \cdots s_n$. Is G' necessarily a pseudorandom generator?

Question 4

Definition 1 A private-key encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions in the presence of an eavesdropper, or is EAV-secure, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function $negl$ such that, for all n,

$$\mathsf{Pr}\ \left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq 1/2 + negl(n)$$

where the probability is taken over the randomness used by $\mathcal{A}$ and the randomness used in the experiment (for choosing the key and the bit b, as well as any randomness used by Enc). $\diamondsuit$

Prove that the above definition (Definition 5) cannot be satisfied if Π can encrypt arbitrary length messages and the adversary is not restricted to output equal length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

Hint: Let $q(n)$ be a polynomial upper-bound on the length of the ciphertext when Π is used to encrypt a single bit. Then consider an adversary who outputs $m_0 \in \{0,1\}$ and a uniform $m_1 \in \{0,1\}^{q(n)+2}$.

Question 5

Let F be a pseudorandom permutation, and define a fixed-length encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ as follows: On input $m \in \{0,1\}n/2$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}n/2$ of length $n/2$ and computes $c := F_k(r||m)$. Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

Question 6

Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $l(n) = n+1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

(a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

(b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

(c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Question 7

Consider the following MAC for messages of length $l(n) = 2n - 2$ using a pseudorandom function F: On input a message $m_0||m_1$ (with $|m_0| = |m_1| = n - 1$) and key $k \in \{0,1\}^n$, algorithm Mac outputs $t = F_k(0||m_0)||F_k(1||m_1)$. Algorithm Vrfy is defined in the natural way. Is $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ secure? Prove your answer.

Question 8

Let F be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)

(a) To authenticate a message $m = m_1, \cdots, m_l$, where $m_i \in \{0,1\}^n$, compute $t := F_k(m_1) \oplus \cdots \oplus F_k(m_l)$.

(b) To authenticate a message $m = m_1, \cdots, m_l$, where $m_i \in \{0,1\}^{n/2}$, compute $t := F_k(\langle 1 \rangle ||m_1) \oplus \cdots \oplus F_k(\langle l \rangle ||m_l)$.

Question 9

Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is insecure: Gen outputs a uniform $k \in \{0,1\}^n$. To authenticate a message $m_1||m_2$ with $|m_1| = |m_2| = n$, compute the tag $F_k(m_1)||F_k(F_k(m_2))$.

Practice Problems

Question 1

For any function $g : \{0,1\}^n \to \{0,1\}^n$, define $g^{\$}(\cdot)$ to be a probabilistic oracle that, on input 1^n, chooses uniform $r \in \{0,1\}^n$ and returns $\langle r, g(r)\rangle$. A keyed function F is a *weak pseudorandom* function if for all PPT algorithms D, there exists a negligible function $negl$ such that:

$$| \mathsf{Pr}\left[D^{F_k^{\$}(\cdot)}(1^n) = 1\right] - \mathsf{Pr}\left[D^{f_k^{\$}(\cdot)}(1^n) = 1\right] | \le negl(n)$$

where $k \in \{0,1\}^n$ and $f \in Func_n$ are chosen uniformly.

(a) Prove that if F is pseudorandom then it is weakly pseudorandom.

(b) Let F' be a pseudorandom function, and define

$$F_k(x) \stackrel{def}{=} \begin{cases} F'_k(x) & \text{if } x \text{ is even} \\ F'_k(x+1) & \text{if } x \text{ is odd} \end{cases}$$

Prove that F is weakly pseudorandom, but not pseudorandom.

Question 2

Prove that the following modifications of basic CBC-MAC do not yield a secure MAC (even for fixed-length messages):

A random initial block is used each time a message is authenticated. That is, choose uniform $t_0 \in \{0,1\}^n$, run basic CBC-MAC over the "message" $t_0, m_1, \cdots, m_l$, and output the tag $\langle t_0, t_l\rangle$. Verification is done in the natural way.

Question 3

For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case.

(a) The message space is $M = \{\ 0, \cdots, 4\ \}$. Algorithm Gen chooses a uniform key from the key space $\{\ 0, \cdots, 5\ \}$. $\mathsf{Enc}_k(m)$ returns $[k + m \bmod 5]$, and $\mathsf{Dec}_k(c)$ returns $[c - k \bmod 5]$.

(b) The message space is $M = \{m \in \{0,1\}^l |$ the last bit of m is $0\ \}$. Gen chooses a uniform key from $\{0,1\}^{l-1}$. $\mathsf{Enc}_k(m)$ returns ciphertext $m \oplus (k||0)$, and $\mathsf{Dec}_k(c)$ returns $c \oplus (k||0)$.

Question 4

Let Π be an arbitrary encryption scheme with $|K| < |M|$. Show an $\mathcal{A}$ for which $\mathsf{Pr}\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] > 1/2$. Hint: It may be easier to let $\mathcal{A}$ be randomized.

Question 5

In the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

(a) Let G be a pseudorandom generator with expansion factor $l(n) > 2n$. Define $G'(s) \stackrel{def}{=} G(s)||G(s+1)$. Is G' necessarily a pseudorandom generator?

(b) Let $G : \{0,1\}^k \to \{0,1\}^n$ be a PRG. $G' : \{0,1\}^{k+l} \to \{0,1\}^{n+l}$ defined by

$$G'(x||x') = G(x)||x'$$

where $x \in \{0,1\}^k$ and $x' \in \{0,1\}^l$.

Question 6

Prove or refute: An encryption scheme with message space M is perfectly secret if and only if for every probability distribution over M and every $c_0, c_1 \in C$ we have

$$\mathsf{Pr}[\ C = c_0\ ] = \mathsf{Pr}[\ C = c_1\ ].$$

Question 7

Assuming the existence of a pseudorandom function, prove that there exists an encryption scheme that has indistinguishable multiple encryptions in the presence of an eavesdropper (i.e.COA-secure), but is not CPA-secure

Question 8

Let F be a length-preserving pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

(a) $F'_k(x) \stackrel{def}{=} F_k(0||x)||F_k(1||x)$

(b) $F'_k(x) \stackrel{def}{=} F_k(0||x)||F_k(x||1)$

References

1. Jonathan Katz, Yehuda Lindell : Introduction to Modern Cryptography, Second Edition