EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Midsem Exam : 25 points March 1, 2018

1. (5 points) Prove that if $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Solution: See proof of Theorem 2.10 in Katz/Lindell.

2. (5 points) If a private-key encryption scheme Π is perfectly indistinguishable, prove that it is perfectly secret.

Solution: This proof was done in class. Check your lecture notes.

3. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a keyed pseudorandom permutation (the first argument is the key). Consider the keyed function $F' : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined for all $x, x' \in \{0,1\}^n$ by

$$F'_k(x\|x') = F_k(x)\|F_k(x \oplus x').$$

   (a) (1 point) Prove that F'_k is a permutation for all $k \in \{0,1\}^n$.

Solution: Since the domain and range of F'_k are equal to the finite site $\{0,1\}^{2n}$, it is enough to show that F'_k is one-to-one. That is, for all $X, Y \in \{0,1\}^{2n}$ we have to show that $X \neq Y \implies F'_k(X) \neq F'_k(Y)$.
Let $X = x\|x'$ and $Y = y\|y'$ where $x, x', y, y' \in \{0,1\}^n$. Given $X \neq Y$, either $x \neq y$ or $x' \neq y'$. If $x \neq y$, then $F_k(x) \neq F_k(y)$ as F_k is a permutation. This implies that the **first** n bits of $F'_k(X)$ and $F'_k(Y)$ are different. Hence $F'_k(X) \neq F'_k(Y)$.
If $x = y$, then $x' \neq y'$. Then $x \oplus x' = y \oplus x' \neq y \oplus y'$. Then $F_k(x \oplus x') \neq F_k(y \oplus y')$ since F_k is a permutation. This implies that the **last** n bits of $F'_k(X)$ and $F'_k(Y)$ are different. Hence $F'_k(X) \neq F'_k(Y)$.

   (b) (4 points) Prove that F'_k is **not** a pseudorandom permutation.

Solution: Let $0_{2n} = \underbrace{000\cdots000}_{2n \text{ times}}$ and $0_n = \underbrace{000\cdots000}_{n \text{ times}}$.
The distinguisher queries the oracle on 0_{2n}.

- If the oracle is responding to queries using F'_k, then its response is $F'_k(0_{2n}) = F_k(0_n)\|F_k(0_n \oplus 0_n) = F_k(0_n)\|F_k(0_n)$.
- If the oracle is responding to queries using an $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ which was uniformly chosen from $\texttt{Perm}_{2n}$, then its response is $f(0_{2n})$ which can take any value in $\{0,1\}^{2n}$ with probability $\frac{1}{2^{2n}}$.

Let $y \in \{0,1\}^{2n}$ be the response to the query on input 0_{2n}. The distinguisher outputs 1 if the first n bits of y are equal to the last n bits of y. If not, the distinguisher outputs 0.

The $\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] = 1$. But $\Pr\left[D^{f(\cdot)}(1^n) = 1\right] = \frac{2^n}{2^{2n}} = \frac{1}{2^n}$. The latter follows from the observation that there are exactly 2^n bitstrings in $\{0,1\}^{2n}$ whose first n bits are equal to the last n bits.
Thus $\left|\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| = 1 - \frac{1}{2^n}$ which is not negligible. Since D is a polynomial time distinguisher, F'_k is not a pseudorandom permutation.

4. (5 points) Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom permutation. Suppose messages of size dn bits have to be encrypted where $d > 1$. The message m is divided into d blocks of n bits each where m_i is the ith block. Consider the mode of operation in which a uniform value $\texttt{ctr} \in \{0,1\}^n$ is chosen, and the ith ciphertext block c_i is computed as $c_i := F_k(\texttt{ctr} + i + m_i)$. The value $\texttt{ctr}$ is sent in the clear, i.e. the eavesdropper observes $\texttt{ctr}, c_1, c_2, c_3, \ldots, c_d$. The sum $\texttt{ctr} + i + m_i$ is calculated modulo 2^n ensuring that the argument of F_k belongs to $\{0,1\}^n$. Show that this scheme does **not** have indistinguishable encryptions in the presence of an eavesdropper.

Solution: The adversary observes $\texttt{ctr}, c_1, c_2, \ldots, c_d$ where $d > 1$. Let the messages m_0, m_1 chosen by the adversary be given by

$$m_0 = \begin{bmatrix} m_{0,1} & m_{0,2} & \cdots & m_{0,d} \end{bmatrix},$$
$$m_1 = \begin{bmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,d} \end{bmatrix}.$$

The blocks in m_0 are chosen as $m_{0,i} = (2^n - i) \bmod 2^n$. This implies that the ith block of the ciphertext corresponding to m_0 is given by

$$c_i = F_k\left(\texttt{ctr} + i + 2^n - i \bmod 2^n\right) = F_k(\texttt{ctr}).$$

So all the ciphertext blocks (after $\texttt{ctr}$) are equal when m_0 is transmitted.

The first two blocks in m_1 are chosen as $m_{1,1} = (2^n - 1) \bmod 2^n$ and $m_{1,2} = (2^n - 1) \bmod 2^n$. The remaining message blocks $m_{1,3}$ to $m_{1,d}$ are arbitrarily chosen. This implies that the first two blocks of the ciphertext corresponding to m_1 are given by

$$c_1 = F_k\left(\texttt{ctr} + 1 + 2^n - 1 \bmod 2^n\right) = F_k(\texttt{ctr}),$$
$$c_2 = F_k\left(\texttt{ctr} + 2 + 2^n - 1 \bmod 2^n\right) = F_k(\texttt{ctr} + 1).$$

As F_k is a permutation, the first two ciphertext blocks (after $\texttt{ctr}$) are alway not equal when m_1 is transmitted.

Let the adversary's estimate of b be given by $b' = \mathcal{A}(\texttt{ctr}, c_1, c_2, \ldots, c_d)$. The adversary determines b' as follows:

$$\mathcal{A}(\texttt{ctr}, c_1, c_2, \ldots, c_d) = \begin{cases} 0 & \text{if } c_1 = c_2, \\ 1 & \text{if } c_1 \neq c_2. \end{cases}$$

By our construction, $b' = b$ irrespective of the value of `ctr`. So the adversary succeeds with probability 1 which is not bounded by $\frac{1}{2} + \texttt{negl}(n)$. The existence of such an adversary (which operates in polynomial time) shows that the scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

5. (5 points) Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ 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 $t = F_k(m_1) \| F_k\left(F_k(m_2)\right)$.

Solution: Suppose the adversary queries the tag generation algorithm $\texttt{Mac}_k(\cdot)$ on messages $m_1 \| m_2$ and $m_1' \| m_2'$ where $m_1, m_2, m_1', m_2' \in \{0,1\}^n$ and $m_1 \neq m_1'$, $m_2 \neq m_2'$.

Let $t = F_k(m_1) \| F_k\left(F_k(m_2)\right)$ and $t' = F_k(m_1') \| F_k\left(F_k(m_2')\right)$ be the tags returned by the tag generation algorithm. The query set is given by $\mathcal{Q} = \{m_1 \| m_2, m_1' \| m_2'\}$.

Consider the message $m_1 \| m_2'$. By our assumptions, this message is not in $\mathcal{Q}$. The adversary presents the tag $t'' = F_k(m_1) \| F_k\left(F_k(m_2')\right)$ for $m_1 \| m_2'$ by combining the first n bits of t with the last n bits of t'. Thus the adversary succeeds in generating a tag for a message not in the query set Q with probability 1.