Introduction to Modern Cryptography
Homework 2

Jie Feng[*]
jokerfeng2010@gmail.com
Information Security Institute
Johns Hopkins University

September 24, 2013

[*]I'm getting loving *cryptography*

Ex 3.1 Prove Proposition 3.7
Proof of Proposition 3.7-1:

Given polynomial $p(n)$, we have that $h(n) = p(n) \cdot 2$ is polynomial too. Since $\mathsf{negl}_1(n)$ *and* $\mathsf{negl}_2(n)$ are negligible functions, by **DEFINITION 3.5**, we get:

- there exists an N_1 such that for all integers $n > N_1$ it holds that $\mathsf{negl}_1(n) < \frac{1}{h(n)}$.
- there exists an N_2 such that for all integers $n > N_2$ it holds that $\mathsf{negl}_2(n) < \frac{1}{h(n)}$.

Let $N = max(N_1, N_2)$, we have: for all integers $n > N$ it holds that $\mathsf{negl}_1(n) < \frac{1}{h(n)}$ *and* $\mathsf{negl}_2(n) < \frac{1}{h(n)}$.

Hence we get: for all integers $n > N$ it holds that $\mathsf{negl}_1(n) + \mathsf{negl}_2(n) < \frac{1}{h(n)} \cdot 2 = p(n)$.

Finally, we have: $\mathsf{negl}_3(n) = \mathsf{negl}_1(n) + \mathsf{negl}_2(n)$ is negligible.

Proof of Proposition 3.7-2:

Given polynomial $q(n)$, we have that $h(n) = q(n) \cdot p(n)$ is polynomial too. Since $\mathsf{negl}_1(n)$ is negligible functions, by **DEFINITION 3.5**, we get:

- there exists an N such that for all integers $n > N$ it holds that $\mathsf{negl}_1(n) < \frac{1}{h(n)}$.

Hence we get: for all integers $n > N$ it holds that $\mathsf{negl}_4(n) = p(n) \cdot \mathsf{negl}_1(n) < p(n) \cdot \frac{1}{h(n)} = p(n) \cdot \frac{1}{q(n) \cdot p(n)} = p(n)$.

Finally, we have: $\mathsf{negl}_4(n) = p(n) \cdot \mathsf{negl}_1(n)$

Ex 3.3 Prove that Definition 3.9 cannot be satisfied if Π can encrypt arbitrary length messages and the adversary is *not* restricted to output equal length messages in experiment $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$.
Proof:

In **DEFINITION 3.8**, we have:

A private-key encryption scheme is a tuple of *probabilistic polynomial-time algorithms* (Gen, Enc, Dec).

Since Enc is *polynomial-time algorithm*, we know that it can only produce *polynomial-length* output if given *polynomial-length* input. Otherwise, the algorithm of Enc is not a polynomial one.

Suppose Enc is used to encrypt a single bit, then the length of the ciphertext is polynomial. Let $q(n)$ be a polynomial upper-bound on the length of the ciphertext.

If Π can encrypt arbitrary length messages and the adversary is not restricted to output equal length messages in experiment $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}$, then consider an adversary who outputs $m_0 \in \{0,1\}$ *and* $m_1 \in \{0,1\}^{q(n)+2}$.

In the third step of **the adversarial indistinguishability experiment** $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}(n)$, the adversary can guess b' in the following means:

1. if *ciphtertext* c's length is bigger than or equal to $q(n)$ then output $b' = 1$.
2. if *ciphtertext* c's length is smaller than $q(n)$ then output $b' = 0$.

So, how is the probability of that guess? Let's calculate.

There are $2^{q(n)+2}$ different plaintexts of length $q(n) + 2$.

Since it holds that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$, thus it should hold that $\mathsf{Enc}(m_0) \neq \mathsf{Enc}(m_1), \forall m_0, m_1 \in 0, 1^*$.

So, there are at most $2^1 + 2^2 + \cdots + 2^{q(n)-1}$ different ciphertexts which are encrypted from plaintext $m \in \{0, 1\}^{q(n)+2}$ with length smaller than $q(n)$.

Let P be the probability that a plaintext of length $q(n) + 2$ is encrypted to a ciphertext with length smaller to $q(n)$.

So $P \leq \frac{2^1+2^2+\cdots+2^{q(n)-1}}{2^{q(n)+2}} = \frac{2^{q(n)}-2}{2^{q(n)+2}} < \frac{1}{4}$.

By definition of **the adversarial indistinguishability experiment**, m_0 *and* m_1 are both get encrypted at probability $\frac{1}{2}$.

1. If m_0 gets encrypted.

   Since the upper-bound on the length of the ciphertext when Enc is used to encrypt a single bit is $q(n)$, so the probability of that the length of ciphtertext is smaller than $q(n)$ is 1.

   At this situation, we will always guess $b' = 0$, thus the probability to win the guess is 1 when m_0 gets encrypted.

2. If m_1 gets encrypted.

   When the length of the ciphertext is bigger than or equal to $q(n)$, we will always guess $b' = 1$, and we are right. When the length of the ciphertext is smaller than $q(n)$, we will always guess $b' = 0$, and we are wrong.

   Since the length of the ciphertext which is bigger than or equal to $q(n)$ is at probability of $1 - P$. So, the probability to win the guess is $1 - P$ when m_1 gets encrypted.

So, the probability to win the game is $Pr[\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}(n) = 1] = \frac{1+1-p}{2} = 1 - \frac{p}{2} > 1 - \frac{1}{4} = \frac{3}{4} > \frac{1}{2} + \mathsf{negl(n)}$.

Thus Definition 3.9 cannot be satisfied.

Ex 3.4 Answer:

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a fixed-length private-key encryption scheme.

Let $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ be the scheme we need, define Π' as follows:

1. Gen' takes as input the security parameter n and outputs a key k, $k \leftarrow \mathsf{Gen}(1^n)$.

2. Enc' takes as input a key k and a plaintext message $m \in \{0,1\}^l$ where $l < l(n)$. Then generate message m' by first padding m with a single bit 1, then padding with bits 0 until the length reaches $l(n)$. After that, encrypt the new message m' with Gen from Π and output ciphertext c.

3. Dec' takes as input a key k and a ciphertext c. First uses Dec and key k to decrypt the ciphtertext and get padded message m', then removes the zeros together with the first 1 at the tail of the m' and output the message m.

In **the adversarial indistinguishability experiment** $\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}(n)$. The adversary can output messages m_0 *and* m_1 where $|m_0| < l(n)$ *and* $|m_1| < l(n)$.

Then the adversary receives the ciphertext c which is encrypted by one of the two padded messages m_0 *and* m_1 of the same length.

Thus the scheme satisfies Definition 3.9.