Crypto Engineering - verifying crypto primitives and security protocols
2016/2017

C. Ene

Exercices

Exercise 1
Let $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme, such that the sets of messages (plaintexts) $\mathcal{M}$, cyphertexts $\mathcal{C}$ and keys $\mathcal{K}$ are $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1, 2\}$. The encryption function is described by the table below:

		m		
	$\mathcal{E}(k,m)$	0	1	2
	0	2	1	0
k	1	1	2	0
	2	2	0	1

i.e., for example $\mathcal{E}(0, 2) = 0$ and $\mathcal{E}(1, 1) = 2$.

- Give the corresponding decryption function.
- Is this cryptosystem perfectly secure? Why or why not?

Exercise 2
We recall that a family of distributions $\mathcal{E}$ is called **polynomial-time constructible**, if there is a ppt-algorithm $\Psi_{\mathcal{E}}$, such that the output of $\Psi_{\mathcal{E}}(\eta)$ is distributed identically to $\mathcal{E}_\eta$. We use $\oplus$ to denote the usual bitwise xor over equal-length bitstrings, e.g. $0011 \oplus 1110 = 1101$, and $01 \oplus 00 = 01$.
Given two families of distributions $\mathcal{D}$ and $\mathcal{E}$, such that for any η, both $\mathcal{D}_\eta$ and $\mathcal{E}_\eta$ are distributions over strings of length η, we define $\mathcal{D} \oplus \mathcal{E}$ by

$$(\mathcal{D} \oplus \mathcal{E})_\eta = [x \xleftarrow{R} \mathcal{D}_\eta; y \xleftarrow{R} \mathcal{E}_\eta : \ (x \oplus y)].$$

Prove or disprove the following assertions (where $\approx$ is the computational indistingushability relation over distributions):

- If $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}$ is polynomial-time constructible, then $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$.
- If $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$ then $\mathcal{D}^0 \approx \mathcal{D}^1$.
- If $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$ and $\mathcal{D}^0, \mathcal{D}^1, \mathcal{E}^0, \mathcal{E}^1$ are all polynomial-time constructible, then $(\mathcal{D}^0 \oplus \mathcal{E}^0) \approx (\mathcal{D}^1 \oplus \mathcal{E}^1)$.
- If $(\mathcal{D}^0 \oplus \mathcal{E}^0) \approx (\mathcal{D}^1 \oplus \mathcal{E}^1)$ then $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$.

Exercise 3
We recall the definitions of the following hardness assumptions:

1) Assumption DL: $\mathbf{Adv}^{DL}(\mathcal{A})$ is negligible for any ppt-algorithm $\mathcal{A}$, where

$$\mathbf{Adv}^{DL}(\mathcal{A}) = Pr\Big[r = x \mid x \overset{R}{\leftarrow} \mathbb{Z}_q; r \overset{R}{\leftarrow} \mathcal{A}(\eta, q, g, g^x)\Big].$$

2) Assumption CDH: $\mathbf{Adv}^{CDH}(\mathcal{A})$ is negligible for any ppt-algorithm $\mathcal{A}$, where

$$\mathbf{Adv}^{CDH}(\mathcal{A}) = Pr\Big[r = g^{xy} \mid x \overset{R}{\leftarrow} \mathbb{Z}_q; y \overset{R}{\leftarrow} \mathbb{Z}_q; r \overset{R}{\leftarrow} \mathcal{A}(\eta, q, g, g^x, g^y)\Big].$$

3) Assumption $SCDH$: $\mathbf{Adv}^{SCDH}(\mathcal{A})$ is negligible for any ppt-algorithm $\mathcal{A}$, where

$$\mathbf{Adv}^{SCDH}(\mathcal{A}) = Pr\Big[r = g^{x^2} \mid x \overset{R}{\leftarrow} \mathbb{Z}_q; r \overset{R}{\leftarrow} \mathcal{A}(\eta, q, g, g^x)\Big].$$

4) Assumption DDH: $\mathbf{Adv}^{DDH}(\mathcal{A})$ is negligible for any ppt-algorithm $\mathcal{A}$, where

$$\begin{aligned}\mathbf{Adv}^{DDH}(\mathcal{A}) = Pr\Big[b' = 1 \mid x \overset{R}{\leftarrow} \mathbb{Z}_q; y \overset{R}{\leftarrow} \mathbb{Z}_q; b' \overset{R}{\leftarrow} \mathcal{A}(\eta, q, g, g^x, g^y, g^{xy})\Big] \\ - Pr\Big[b' = 1 \mid x \overset{R}{\leftarrow} \mathbb{Z}_q; y \overset{R}{\leftarrow} \mathbb{Z}_q; r \overset{R}{\leftarrow} \mathbb{Z}_q; b' \overset{R}{\leftarrow} \mathcal{A}(\eta, q, g, g^x, g^y, g^r)\Big].\end{aligned}$$

It is assumed that we have an efficient (polynomial) way: 1) to perform the group operation, 2) to compute the inverse of any element, 3) to test if two elements are equal or not, 4) to compute the square root of any element.
Prove that: 1) CDH implies DL; 2) CDH implies $SCDH$; 3) $SCDH$ implies CDH; 4) DDH implies CDH.

Exercise 4
ElGamal encryption scheme for a cyclic group G of order q and generator g, is defined by the following algorithms $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ where $||$ denotes concatenation:

- $\mathcal{K}() = x \leftarrow^R \mathbb{Z}_q;\ sk \leftarrow x;\ pk \leftarrow g^x; return\ (sk, pk)$
- $\mathcal{E}(pk, m) = r \leftarrow^R \mathbb{Z}_q;\ return\ (pk^r \times m)\ ||\ g^r.$
- $\mathcal{D}(sk, c1||c2) = return\ c1/(c2^{sk}).$

Prove that ElGamal is IND-CPA secure if we assume the hardness of DDH.

Exercise 5
In this exercice, $||$ denotes concatenation, and $|\cdot|$ denotes the lentgh. A one-way function is a function that is easy to compute but hard to invert. Formally, $f : \{0,1\}^* \mapsto \{0,1\}^*$ is a one-way function, if for all probabilistic polynomial-time families of adversaries $\mathcal{A}$ the following probablity:

$$p(k) \overset{def}{=} Pr[f(x') = y \mid x \overset{R}{\leftarrow} \{0,1\}^k; y \leftarrow f(x); x' \overset{R}{\leftarrow} \mathcal{A}(y)]$$

is a negligible function in k.

Let $f : \{0,1\}^* \mapsto \{0,1\}^*$ be a one-way function and $p : \{0,1\}^* \mapsto \{0,1\}^*$ be a one-way permutation such that for any bistring x, $|p(x)| = |x|$ (i.e. a function that happens to be both a permutation and a one way function). For each of the suggested assertions below prove or disprove that they are valid. That is, if the assertion is valid give a proof by reduction. If it is not, give an example of a one-way function f such that the obtained function g is not a one-way function. [1]

a) Let $g_1 : \{0,1\}^* \mapsto \{0,1\}^*$ be the function defined by $g_1(x_1 \mid\mid x_2) = f(x_1)$ where $|x_2| \leq |x_1| \leq |x_2| + 1$, i.e. g_1 is the function that behaves like f applied to the first half of the input and that ignores the second half of the input. Then g_1 is a one-way function.

b) Let $g_2 : \{0,1\}^* \mapsto \{0,1\}^*$ be the function defined by

$$g_2(x) = \begin{cases} 0^{2\times|x|} & \text{if } \exists y \text{ such that } \; x = y \mid\mid 0^{|x|/2} \\ p(x) \mid\mid 0^{|x|} & \text{otherwise} \end{cases}$$

i.e. g_2 is the function that if the input ends with "enough" zeroes, then it returns a string containing only zeroes; if not, it applies the one-way permutation p to its input and appends $|x|$ zeroes to the result. Then g_2 is a one-way function.

c) Let $g_3 : \{0,1\}^* \mapsto \{0,1\}^*$ be the function defined by $g_3(x) = f(f(x))$, i.e. g_3 is the function that applies twice f to its input. Then g_3 is a one-way function.

Exercise 6

In this exercice, $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a public key encryption scheme, $||$ denotes concatenation and $\overline{x}$ is the bitwise complement of x.

a) Let $\mathcal{S}' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ be the public key encryption scheme defined by

$$\mathcal{E}'(pk, m) \stackrel{def}{=} y_1 \stackrel{R}{\leftarrow} \mathcal{E}(pk, m); y_2 \stackrel{R}{\leftarrow} \mathcal{E}(pk, \overline{m});\ \text{return } y_1||y_2,$$

$$\mathcal{D}'(sk, c_1||c_2) \stackrel{def}{=} x_1 \leftarrow \mathcal{D}(sk, c_1); x_2 \leftarrow \mathcal{D}(sk, c_2); \text{if } \; x_1 = \overline{x_2} \; \textit{then} \; \text{ return } x_1 \, \textit{else} \; \text{ return } \; \textit{error}.$$

1. Prove that, if $\mathcal{S}$ is IND-CPA secure, than $\mathcal{S}'$ is also IND-CPA secure.
2. Prove that $\mathcal{S}'$ cannot be IND-CCA2 secure, even if $\mathcal{S}$ is IND-CCA2 secure.

b) Let $\mathcal{S}' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ be the public key encryption scheme defined by

$$\mathcal{E}'(pk, m) \stackrel{def}{=} y \stackrel{R}{\leftarrow} \mathcal{E}(pk, m);\ \text{return } y||y,$$

$$\mathcal{D}'(sk, c_1||c_2) \stackrel{def}{=} \text{if } \; c_1 = c_2 \; \textit{then} \; \text{ return } \mathcal{D}(sk, c_1) \; \textit{else} \; \text{ return } \; \textit{error}.$$

Prove (by reduction) that, if $\mathcal{S}$ is IND-CCA2 secure, than $\mathcal{S}'$ is also IND-CCA2 secure.

[1] For this exercice you may assume the existence of such functions f and p.

Exercise 7

In this exercice, $\mathcal{S}^a = (\mathcal{K}^a, \mathcal{E}^a, \mathcal{D}^a)$ is a public key encryption scheme, $\mathcal{S}^s = (\mathcal{K}^s, \mathcal{E}^s, \mathcal{D}^s)$ is a symmetric key encryption scheme and $||$ denotes concatenation.

Let $\mathcal{S}' = (\mathcal{K}^a, \mathcal{E}', \mathcal{D}')$ be the public key encryption scheme (called hybrid encryption) defined by

$$\mathcal{E}'(pk, m) \stackrel{def}{=} k \stackrel{R}{\leftarrow} \mathcal{K}^s(); y_1 \stackrel{R}{\leftarrow} \mathcal{E}^a(pk, k); y_2 \stackrel{R}{\leftarrow} \mathcal{E}^s(k, m);\ \text{return } y_1||y_2,$$

$$\mathcal{D}'(sk, c_1||c_2) \stackrel{def}{=} k{\leftarrow}\mathcal{D}^a(sk, c_1); x{\leftarrow}\mathcal{D}^s(k, c_2);\ \text{return } x\ .$$

Prove that, if $\mathcal{S}^a$ and $\mathcal{S}^s$ are IND-CPA secure, than $\mathcal{S}'$ is also IND-CPA secure.