Computer Science and Engineering, UCSD | Fall 09
CSE 207: Modern Cryptography | **Instructor:** Mihir Bellare
Problem Set 7 | November 9, 2009

Problem Set 7

Due: Monday November 16, 2009, in class.

Collaboration is not allowed on this problem set. See the course information sheet for collaboration rules.

Problem 1. [**30 points**] Let $G = \langle g \rangle$ be a cyclic group of order $m \geq 2^{2k}$.

1. [**10 points**] Show that the ElGamal scheme over G succumbs to a CCA in which an adversary given the public key and a decryption oracle succeeds in decrypting a target ciphertext (Y, W) without querying (Y, W) to its oracle.

2. [**20 points**] Here is a modified scheme that attempts to get around this. Let $\mathsf{e}\colon \{0,1\}^{2k} \to G$ be an injective map that encodes a $2k$-bit string as a group element, and let $\mathsf{e}^{-1}\colon G \to \{0,1\}^{2k}$ be its inverse, extended to return 0^{2k} if its input is not in the range of e. Let $H\colon \{0,1\}^k \to \{0,1\}^k$ be a public hash function. Let asymmetric encryption scheme $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be defined via

algorithm $\mathcal{K}$	algorithm $\mathcal{E}_X(M)$	algorithm $\mathcal{D}_x((Y, W))$
$x \xleftarrow{\$} Z_m$	if $M \notin \{0,1\}^k$ then return $\perp$	if $Y \notin G$ OR $W \notin G$ then return $\perp$
$X \leftarrow g^x$	$P \leftarrow \mathsf{e}(M \parallel H(M))$	$K \leftarrow Y^x$; $P \leftarrow WK^{-1}$
return (X, x)	$y \xleftarrow{\$} Z_m$; $Y \leftarrow g^y$	$M \parallel R \leftarrow \mathsf{e}^{-1}(P)$
	$K \leftarrow X^y$; $W \leftarrow KP$	if $R \neq H(M)$ then return $\perp$
	return (Y, W)	else return M

The notation $M \parallel R \leftarrow Z$, where Z is a $2k$-bit string, means M is the first k bits of Z and R is the rest.

An adversary is given a decryption oracle $\mathcal{D}_x((\cdot, \cdot))$, the public key X, and a target ciphertext $(Y, W) \xleftarrow{\$} \mathcal{E}_X(M)$ obtained by encrypting some target message $M \in \{0,1\}^k$. The adversary is not allowed to query (Y, W) to its oracle and is successful if it outputs M.

Determine whether the scheme is secure. If you say NO, give an adversary that is successful in the above sense. If you say YES, justify your answer assuming H is a random oracle and the DDH problem is hard in G.

In any attack, say how many oracle queries your adversary makes and what is its running time. (The lower these are, the more points you get.)

Problem 2. [**30 points**] Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an asymmetric encryption scheme whose message space includes $\{0,1\}^k$. Define the KEM $\mathcal{KEM} = (\mathcal{K}, \mathcal{EK}, \mathcal{D})$ with keylength k via

algorithm $\mathcal{EK}$
$K \xleftarrow{\$} \{0,1\}^k$
$C \xleftarrow{\$} \mathcal{E}_{pk}(K)$
return (K, C)

Show that if $\mathcal{AE}$ is IND-CCA secure, then so is $\mathcal{KEM}$. This means you must state a reduction-style theorem and then prove it. The better your bounds, the more points you get.
