Computer Science and Engineering, UCSD
CSE 107: Introduction to Modern Cryptography
Problem Set 6

Winter 09
Instructor: Mihir Bellare
March 4, 2009

Problem Set 6

Due: Wednesday March 11, 2009, in class.

See course information section (on course web page) for instructions and rules on working on problem sets and turning them in.

Problem 1. [**40 points**] Let $p \geq 3$ be a prime and $g \in \mathbf{Z}_p^*$ a generator of $\mathbf{Z}_p^*$. (These are public quantities, known to all parties including the adversary.) Consider the key-generation and encryption algorithms below:

$$
\begin{array}{l|l}
\text{Algorithm } \mathcal{K} & \text{Algorithm } \mathcal{E}(X, M) \\
\quad x \xleftarrow{\$} \mathbf{Z}_{p-1}^* & \quad \textbf{if } M \notin \mathbf{Z}_p^* \textbf{ then return } \bot \\
\quad X \leftarrow g^x \bmod p & \quad y \xleftarrow{\$} \mathbf{Z}_{p-1} \,;\, Y \leftarrow g^y \bmod p \\
\quad \textbf{return } (X, x) & \quad Z \leftarrow X^y \bmod p \,;\, W \leftarrow Y \cdot M \bmod p \\
& \quad \textbf{return } (Z, W)
\end{array}
$$

The message space associated to public key X is $\mathsf{Messages}(X) = \mathbf{Z}_p^*$. We let k be the bit-length of p.

1. [**10 points**] Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is an asymmetric encryption scheme satisfying the correct decryption property. State the running time of your algorithm as a function of k (the lower this is, the more credit you get) and prove that the correct decryption property holds.

2. [**30 points**] Show that this scheme is insecure with regard to the ind-cpa property by presenting an adversary A such that $\mathbf{Adv}_{\mathcal{AE}}^{\text{ind-cpa}}(A)$ is high. You should specify the adversary, state its running time in as a function of k (the smaller this is, the more credit you get), state the value of its advantage (the larger this is, the more credit you get) and justify the correctness of the adversary.