Problem Set 6

Due: Monday November 29, 2010, 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:

Algorithm $\mathcal{K}$	Algorithm $\mathcal{E}(X, M)$
$x \xleftarrow{\$} \mathbf{Z}_{p-1}^*$	if $M \notin \mathbf{Z}_p^*$ then return $\perp$
$X \leftarrow g^x \bmod p$	$y \xleftarrow{\$} \mathbf{Z}_{p-1}$; $Y \leftarrow g^y \bmod p$
return (X, x)	$Z \leftarrow X^y \bmod p$; $W \leftarrow Y \cdot M \bmod p$
	return (Z, W)

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 $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A)$ is high. You should specify the adversary, state its running time 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.

Hints: You have seen an example that is very similar, namely the El Gamal encryption scheme presented in class. Refer to the slides on that scheme to get ideas about how to solve **1.** above. The attack for part **2.** is similar to the attack on El Gamal that exploits the $J_p(\cdot)$ functions. Try to use the Facts stated in the slides and model your attack on the one given there.
