Problem Set 9

Due: Monday, December 7, 2009. Slip under door of EBU3B 4244 by 11AM.

Collaboration is allowed on this problem set. See the course information sheet for collaboration rules. Attacks should always specify the advantage and resource usage of the adversary, and credit depends on their values.

Problem 1. **[45 points]** Generation of random numbers on systems is difficult and error-prone. This problem explores ways of making ElGamal signature generation deterministic. Let $p, q \geq 3$ be primes such that $p = 2q + 1$. Let g be a generator of the cyclic group $\mathbf{Z}_p^*$. Let $H\colon\ \{0,1\}^* \to \mathbf{Z}_{p-1}$ be a random oracle.

1. **[20 points]** We consider re-using randomness accross different signatures, which corresponds to the signature scheme $\mathcal{DS} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ whose algorithms are:

algorithm $\mathcal{K}$	algorithm $\mathcal{S}^H((x,k),M)$	algorithm $\mathcal{V}^H(X,M,(r,s))$
$x \xleftarrow{\$} \mathbf{Z}_{p-1}$	$m \leftarrow H(M)$	$m \leftarrow H(M)$
$X \leftarrow g^x \bmod p$	$r \leftarrow g^k \bmod p$	if $(r \notin \mathbf{Z}_p^*$ OR $s \notin \mathbf{Z}_{p-1})$
$k \xleftarrow{\$} \mathbf{Z}_{p-1}^*$	$s \leftarrow (m - rx)k^{-1} \bmod (p-1)$	then return 0
return $(X,(x,k))$	return (r,s)	if $(X^r \cdot r^s \equiv g^m \pmod p)$
		then return 1
		else return 0

Show that $\mathcal{DS}$ is not UF-CMA secure by presenting an adversary A for which $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{DS}}(A) \geq 1/3$.

2. **[25 points]** Let $F\colon\ \{0,1\}^{128} \times \{0,1\}^* \to \mathbf{Z}_{p-1}^*$ be a PRF. Let $\mathcal{DS} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ be the signature scheme whose algorithms are:

algorithm $\mathcal{K}$	algorithm $\mathcal{S}^H((x,L),M)$	algorithm $\mathcal{V}^H(X,M,(r,s))$
$x \xleftarrow{\$} \mathbf{Z}_{p-1}$	$m \leftarrow H(M)$	$m \leftarrow H(M)$
$X \leftarrow g^x \bmod p$	$k \leftarrow F(L,M)$	if $(r \notin \mathbf{Z}_p^*$ OR $s \notin \mathbf{Z}_{p-1})$
$L \xleftarrow{\$} \{0,1\}^{128}$	$r \leftarrow g^k \bmod p$	then return 0
return $(X,(x,L))$	$s \leftarrow (m - rx)k^{-1} \bmod (p-1)$	if $(X^r \cdot r^s \equiv g^m \pmod p)$
	return (r,s)	then return 1
		else return 0

Is $\mathcal{DS}$ UF-CMA secure? Answer YES or NO and then justify your answer as well as possible.

Note that YES means $\mathcal{DS}$ is UF-CMA for all PRFs F, while NO means there is some PRF F for which $\mathcal{DS}$ is not UF-CMA.

Problem 2. [**15 points**] A hospital wants to make its sensitive medical records available to doctors on a certain list, but does not want any unlisted individual to obtain access to the records. They have established the following procedure. A doctor must generate for himself/herself a public and private key pair (pk, sk) for some secure public-key encryption scheme. It must then send the hospital email containing $[\mathsf{Name}, pk]$, where Name is the name of the doctor. The hospital will check that Name belongs to its list of member doctors. If so, it will encrypt the medical records under pk and send the resulting ciphertext to the address at which the received email originated.

Does the above scheme meet the privacy goals of the hospital? Why or why not? If not, how would you fix it?
