Problem Set 7

Due on Wednesday, May 1, 2013.

Note that the due date falls on the last day of Reading Period. Late submissions can not be accepted without specific authorization from your Residential College Dean.

Instructions Work the problems below, prepare your answers in electronic form, and submit your solutions using the submit script on the Zoo. Remember to specify "7" for the problem number argument to `submit`. As always, you must *properly* cite all resources that you use to solve the problems.

Problem 1: Homomorphic Encryption

Consider the Caesar cipher extended to strings. Using the definition of homomorphic encryption given in lecture 22, show whether or not the encryption function E_k is homomorphic with respect to operations $\odot_{\mathcal{M}}$ and $\odot_{\mathcal{C}}$, where $\odot_{\mathcal{M}} = \odot_{\mathcal{C}}$ is:

(a) Componentwise addition modulo 26;

(b) Componentwise multiplication modulo 26;

(c) String concatenation.

In each case, carefully define the message and ciphertext spaces that make sense for the operation, and give a careful definition of the operation. Then argue why E_k is or is not homomorphic with respect to $\odot_{\mathcal{M}}$ and $\odot_{\mathcal{C}}$.

(over)

Problem 2: Anonymous Authentication

Consider the following proof of knowledge that allows Peggy to convince Victor that she knows either the discrete logarithm of $y_1 = g^{x_1}$ or the discrete logarithm of $y_2 = g^{x_2}$. Assume that Peggy knows x_2. Peggy and Victor execute the following protocol.

	Peggy		Victor
1.	Choose random v_1, v_2 and w		
	Compute $t_1 = y_1^w g^{v_1}$, $t_2 = y_2^w g^{v_2}$	$\xrightarrow{t_1,t_2}$	
2.		$\xleftarrow{c}$	Choose a random c
3.	Calculate $c_1 = w$, $c_2 = c - c_1$,		
	$r_1 = v_1$ and $r_2 = v_2 - x_2 c_2 + x_2 c_1$	$\xrightarrow{c_1,c_2,r_1,r_2}$	Check $t_1 \overset{?}{=} y_1^{c_1} g^{r_1}$, $t_2 \overset{?}{=} y_2^{c_2} g^{r_2}$, $c_1 + c_2 \overset{?}{=} c$
			Accept if checks succeed.

(a) Show that if Peggy and Victor are both honest, then Victor accepts.

(b) Assume Polly knows x_1. Describe how Polly can convince Victor that she also knows either x_1 or x_2.

(c) Explain why Mallory, who does not know x_1 or x_2, cannot cheat and produce a valid proof.

(d) Explain why Victor does not learn which of x_1 or x_2 that Polly knows.