Crypto and Comm Security	Homework 4
CS 6750 Fall 2009 (Pucella)	Due: Oct 22, 2009

Note on integrity: You may discuss problems with fellow students, but all written work must be entirely your own, and should not be from any other course, present or past. If you use a solution from another source you must cite it, including from other people who help you.

Questions

(1) (Stinson, 4.11) A message authentication code can be produced by using a block cipher in CFB mode instead of CBC mode. Given a sequence of plaintext blocks $x_1 \cdots x_n$, suppose we define the initialization vector IV to be x_1. Then encrypt the sequence $x_2 \cdots x_n$ using key K in CFB mode, obtaining the ciphertext sequence $y_1 \cdots y_{n-1}$ (note that there are only $n-1$ ciphertext blocks). Finally, define the MAC to be $e_K(y_{n-1})$. Prove that this MAC is identical to CBC-MAC, which was presented in Section 4.4.2.

(2) Question 7.1 in Stinson.

Suppose Alice is using the ElGamal Signature Scheme with $p = 31847$, $\alpha = 5$ and $\beta = 25703$. Compute the values of k and a (without solving an instance of the Discrete Logarithm problem), given the signature $(23972, 31396)$ for the message $x = 8990$ and the signature $(23972, 20481)$ for the message $x = 31415$.

Note: *Don't find a and k by cycling through all possibilities. That's solving an instance of the discrete log, which you are not allowed to do. See Stinson pp.291–292. You may need to figure out when an equation such as $ax \equiv b \pmod{m}$ has a solution, because you cannot use the equation at the top of p.291 directly, since the appropriate* gcd*'s are not* 1*. You'll have to think a little bit.*

(3) Question 7.14 in Stinson.

In the Lamport Signature Scheme, suppose that two k-tuples, x and x', were signed by Alice using the same key. Let ℓ denote the number of coordinates in which x and x' differ, i.e.,

$$\ell = |\{i \ : \ x_i \neq x'_i\}| \, .$$

Show that Oscar can now sign $2^\ell - 2$ new messages.