

## Assignment #1

Due: Tuesday, January 27, 2004.

**Problem 1 (50 pts)** Let  $p$  be a 128-bit prime and let  $\mathbb{Z}_p$  be the set of integers  $\{0, \dots, p - 1\}$ . Consider the following encryption scheme. The secret key is a pair of integers  $a, b \in \mathbb{Z}_p$  where  $a \neq 0$ . An encryption of a message  $M \in \mathbb{Z}_p$  is defined as:

$$E_{a,b}[M] = aM + b \pmod{p}$$

- a. (20 pts) Show that when  $E$  is used to encrypt a message  $M \in \mathbb{Z}_p$  the system has perfect secrecy in the sense of Shannon. (It is okay to assume that  $M$  is drawn from a uniform distribution.)
- b. (20 pts) Show that if the system is used to encrypt messages  $M_1, M_2$  then the system does not have perfect secrecy.  
Hint: consider the case  $M_1 = M_2$ .
- c. (10 pts) Show that given two random plaintext/ciphertext pairs  $C_i = E_{a,b}[M_i]$  for  $i = 1, 2$  it is possible to recover the key  $a, b$  with high probability.

**Problem 2 (25 pts)** Consider the following Pseudo Random Number Generators (PRNG), which is insecure for cryptographic purposes. The fixed public parameters of the generator are a 128-bit prime  $p$  and three integers  $a, b, c$ . Let  $\mathbb{Z}_p = \{0, 1, \dots, p - 1\}$ . The seed for the generator is a pair  $(s_1, s_2) \in \mathbb{Z}_p^2$ . The generator works as follows:

1. Let  $(x_1, x_2)$  be the current state of the generator (initially the state is equal to the seed). Output  $cx_1 + x_2 \pmod{p}$  as the current random block.
2. Set the new state to be the pair  $(ax_1 + x_2, bx_2 + x_1) \pmod{p}$  and goto Step 1.

Show that no matter what parameters  $a, b, c$  are used, after observing a few consecutive outputs of the generator it is easy to predict all future outputs.

**Problem 3 (25 pts)** Recall that a block cipher built as a Feistel network the round function  $F(X, K_i)$  takes an input  $X$  and a round key  $K_i$ . Suppose that  $X$  is 32-bits and the Feistel network has 8 rounds. Furthermore, suppose that all round keys are 32 bits and the round function is defined as  $F(X, K_i) = X \oplus K_i$ . We assume that the key for the entire cipher is a concatenation of the 8 round keys, i.e., the cipher key is  $8 \cdot 32 = 256$  bits long. Show that the resulting cipher is insecure against known-plaintext attack by describing an efficient algorithm that can decrypt any encrypted message given a modest number of plaintext/ciphertext pairs. Also explain why the algorithm is correct.