

Assignment #2

Due: Tuesday, September 28, 2004.

Problem 1 (15 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) , where $s_1, s_2 \in \mathbb{Z}_p$. 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 $(cx_1 + x_2) \bmod p$ as the current random block.
2. Set the new state to be the pair $(ax_1 + x_2, bx_2 + x_1) \bmod p$ 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. Note that a, b, c are public parameters; therefore, they are already known.

Problem 2 (15 pts) Recall that in 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.

Problem 3 (15 pts) Exercise 3.3 on Page 113 of the Textbook.

Problem 4 (40 pts) Exercise 3.4 on Page 113 of the Textbook. 20 pts for (a) and 10 pts each for (b) and (c).

There are some typos in the textbook.

1. Exercise 3.4(b). "comtains" should be "contains".
2. Exercise 3.4(b). The number of bits of memory required should be $2^{n+1}(m * \ell + n)$.
3. Exercise 3.4(c). "simultaneouly" should be "simultaneously".

Problem 5 (15 pts) Let $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a secure PRP. Consider the family of permutations $E' : \{0, 1\}^k \times \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$ defined as follows:

$$\text{for all } x, x' \in \{0, 1\}^n \quad E'_K(x \| x') = E_K(x) \| E_K(x \oplus x')$$

Show that E' is not a secure PRP.