The art of cryptography: security, reductions, and group cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

2. Assignment

(Due: Thursday, 19 April 2012, 13^{00})

Exercise 2.1 (Removing bias)**.** (4 points) Suppose you are given a coin for which the probability of Heads, say p, is unknown. If $p \neq 1/2$ we call the coin *biased*. How can you use this coin to generate unbiased coin flips? Give a scheme for which the expected number of flips of the biased coin for extraction one unbiased coin-flip is no more than $1/(p(1-p))$. Hint: Consider two consecutive flips of the biased coin.

Exercise 2.2 (Linear congruential generators)**.** We consider linear congruential generators with $x_i = sx_{i-1} + t$ in $\mathbb{Z}_m$.

(i) (3 points) Compute the sequence of numbers resulting from

(a) $m = 10$, $s = 3$, $t = 2$, $x_0 = 1$ and

(b) $m = 10$, $s = 8$, $t = 7$, $x_0 = 1$.

What do you observe?

(ii) (3 points) You observe the sequence of numbers

$$13, 223, 793, 483, 213, 623, 593, \ldots$$

generated by a linear congruential generator. Find matching values of m, a and b.

How do you do this?

Exercise 2.3 (ElGamal pseudorandom generator)**.** Let p be a prime, g a generator of $\mathbb{Z}_p^\times$ and t an integer. As in the ElGamal cryptosystem, we choose a map $^*\colon \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$ that maps elements of $\mathbb{Z}_p^\times$ to elements in the exponent group of $\mathbb{Z}_p$. (For simplicity, you may assume that * maps $p-1$ to

0 and any other element of $\mathbb{Z}_p^\times$ to the same value in $\mathbb{Z}_{p-1}$.) Then a sequence x_i of values can be generated by

$$x_{i+1} = g^{x_i^*+t} \quad \text{in} \quad \mathbb{Z}_p \tag{2.4}$$

from a given seed x_0. We want to estimate the cryptographic suitability of this pseudorandom generator.

(i) (3 points) Use three consecutive values of x_i to obtain two relations that omit t. Raise those relations to appropriate powers to achieve equal exponents for g in both relations. Derive an expression in only the x_i that is a multiple of p. (Hint: Recall the "break" of the linear congruential pseudorandom generator.)

(ii) (2 points) Assume you have recovered p. Consider the two relations you derived in (i) and assume that one of the exponents of g is coprime to $p-1$. How do you recover g.

(iii) (3 points) Having determined p and g we might try to recover t from (2.4). Show that this is equivalent to the discrete logarithm problem. Assume that the discrete logarithm problem in this group is hard. Does this mean that the pseudorandom generator is secure?

(iv) (+2 points) A possible modification is to add another parameter $s \in \mathbb{Z}_{p-1}$ and use the recursion

$$x_{i+1} = g^{sx_i^*+t} \quad \text{in} \quad \mathbb{Z}_p.$$

Does this improve the cryptographic properties? (Hint: You may assume that $s \in \mathbb{Z}_{p-1}^\times$.)