Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 13

Friday, July 22, 2016

Problem 1. *(Weak public-key cryptosystem)* Consider the following insecure cryptosystem: Alice secretly chooses four integers $a, b, a', b' \in \mathbb{N}$, with $a > 1, b > 1$, and computes:

$$M = ab - 1, \qquad e = a'M + a, \qquad d = b'M + b, \qquad n = \frac{ed - 1}{M}.$$

Her public key is (n, e), her private key is d. To encrypt a plaintext m, Bob uses the map $c = em \bmod n$. Alice decrypts the ciphertext received from Bob by $m = cd \bmod n$.

a) Verify that the decryption operation recovers the plaintext.

b) How can the Euclidean algorithm be applied to break the cryptosystem.

Problem 2. *(modified Rabin cryptosystem)* Consider the modification of the Rabin Cryptosystem in which $e_K(m) = c = m \cdot (m + B) \mod n$, where $B \in \mathbb{Z}_n$ is part of the public key. Supposing that $p = 199$, $q = 211$, $n = pq$, and $B = 1357$, perform the following computations.

a) Compute the encryption $y = e_K(32767)$.

b) Determine the four possible decryptions of this given ciphertext y.

Problem 3. *(forging an ElGamal signature with hash function)* An attacker has intercepted one valid signature (r, s) of the ElGamal signature scheme and a hashed message $h(m)$ which is invertible modulo $p - 1$.

Show that the attacker can generate a signature (r', s') for any hashed message $h(m')$, if $1 \leq r < p$ is not verified.