Dr. Michael Reyer

Tutorial 2

Friday, November 2, 2018

Problem 1. *(Properties of quadratic residues)* Let p be prime, g a primitive element modulo p and $a, b \in \mathbb{Z}_p^*$. Show the following:

a) a is a quadratic residue modulo p if and only if there exists an even $i \in \mathbb{N}_0$ with $a \equiv g^i \pmod{p}$.

b) If p is odd, then exactly one half of the elements $x \in \mathbb{Z}_p^*$ are quadratic residues modulo p.

c) The product $a \cdot b$ is a quadratic residue modulo p if and only if a and b are both either quadratic residues or quadratic non-residues modulo p.

Problem 2. *(Goldwasser-Micali)* Using the Goldwasser-Micali cryptosystem, decrypt a ciphertext. Start by finding the cryptosystem's parameters.

a) Find a pseudo-square modulo $n = p \cdot q = 31 \cdot 79$ by using the algorithm from the lecture notes. Start with $a = 10$ and increase a by 1 until you find a quadratic non-residue modulo p. For b, start with $b = 17$ and proceed analogously.

b) Decrypt the ciphertext $c = (1418, 2150, 2153)$.

Problem 3.

(Knapsack cryptosystem)

A public key cryptosystem for a plaintext $m = \sum_{i=1}^{n} m_i 2^{i-1}$ with $n \in \mathbb{N}$ and $m_i \in \{0, 1\}$ is given as follows:

Key Generation:

(1) Choose a random sequence $\boldsymbol{w} = (w_1, w_2, \ldots, w_n)$, with $w_i \in \mathbb{N}$, such that $w_{k+1} > \sum_{i=1}^{k} w_i$ holds for $k = 1, \ldots, n-1$.

(2) Choose *modulus* $q \in \mathbb{N}$, such that $q > \sum_{i=1}^{n} w_i$ holds.

(3) Choose *multiplier* $r \in \mathbb{N}$ with $1 \le r < q$, such that $\gcd(r, q) = 1$ holds.

(4) Compute $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$ with $\beta_i = r w_i \mod q$.

(5) The public key is $\boldsymbol{\beta}$ and the secret key is $(\boldsymbol{w}, q, r)$.

Encryption Procedure:

The plaintext is encrypted as $c = \sum_{i=1}^{n} m_i \beta_i$.

Decryption Procedure:

$d \leftarrow c r^{-1} \mod q$
for $l = n$ **downto** 1 **do**
  if $d \ge w_l$ **then** $m_l \leftarrow 1$ **else** $m_l \leftarrow 0$ **end if**
  $d \leftarrow d - m_l w_l$
end for

a) Show that $(\boldsymbol{w}, q, r) = ((2^0, 2^1, \ldots, 2^{n-1}), 2^n, 1)$ is a weak key in the sense that $m = c$.

b) Assume that $r \neq 1$ in the following and show that $\beta_1, \ldots, \beta_n$ are pairwise different.

Alice encrypts two plaintexts $m \neq m'$ of the same length n with the same key $\boldsymbol{\beta}$ and obtains two different ciphertexts c and c'. A confidential source tells you that m and m' only differ in one bit position $1 \le j \le n$, i.e., $m_j \neq m'_j$ and $m_i = m'_i$ for all $i \neq j$.

c) How can the bit position j be determined?

Bob encrypts a plaintext m of length $n = 5$. He chooses w_1 at random and uses the rules $w_i = 2w_{i-1} + 1$ for $i = 2, \ldots, n$ and $q = 257$. His public key is $\boldsymbol{\beta} = (168, 103, 230, 227, 221)$.

d) Your confidential source provides $w_4 = 63$ and $q = 257$. Determine the secret key $(\boldsymbol{w}, q, r)$ for the given $\boldsymbol{\beta}$. **Hint**: $257 \cdot 7 - 31 \cdot 58 = 1$.

e) Now, you receive the ciphertext $c = 846$. Compute m for the given values.