IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises X.

1. Consider the group $\mathbb{Z}_p^*$ such that $p = 2q + 1$ where p, q are primes. Let $g \in \mathbb{Z}_p^*$. Show that g is a quadratic residue modulo p if and only if $g^q \equiv 1 \pmod{p}$.

2. Consider the following 1-out-of-2 oblivious transfer scheme which uses the RSA cryptosystem.

   (1) The sender has two secrets m_0, m_1. He generates RSA keys: n, e and d, and picks two random messages x_0 and x_1.
   The sender transmits n, e, x_0, and x_1 to the receiver.

   (2) The receiver chooses a random message k, encrypts k with e, and adds x_b, $b \in \{0, 1\}$, to the encryption of k (modulo n).
   The receiver sends the result q to the sender.

   (3) The sender computes k_0 to be the decryption of $q - x_0$ and similarly k_1 to be the decryption of $q - x_1$, and sends $r_0 = m_0 + k_0$ and $r_1 = m_1 + k_1$ to the receiver.

   Show that the receiver can compute m_b, but cannot compute m_{1-b} and that the sender cannot learn b.

3. Consider the following coin flipping protocol:

   (1) Bob generates a Blum integer n (*ie.* an integer $n = pq$, where $p \equiv q \equiv 3 \pmod{4}$ are distinct primes), a random $x \in \mathbb{N}$ with $\gcd(x, n) = 1$, and computes $x_0 \equiv x^2 \pmod{n}$ and $x_1 \equiv x_0^2 \pmod{n}$. He sends n and x_1 to Alice.

   (2) Alice guesses the parity of x and sends her guess to Bob.

   (3) Bob sends x and x_0 to Alice.

   (4) Alice checks that both $x_0 \equiv x^2 \pmod{n}$ and $x_1 \equiv x_0^2 \pmod{n}$. Therefore, Alice can determine if the guess is correct.

   Show that Bob can cheat if n is not a Blum integer.

4. Alice needs to prove to Bob that she knows some secret quadratic non-residue $x \in \mathbb{Z}_n^*$. The parties decide to use for this the zero-knowledge protocol for quadratic residuosity (see lecture notes) with the modification that Bob accepts if and only if he would reject in the residuosity protocol.

   (a) Write the modified protocol explicitly.

   (b) Is it a zero-knowledge protocol? Justify your answer.

5. Given $p = 31$, $q = 23$ and $y = 220$ perform the coin flipping by telephone protocol (Protocol 2 from lecture). Show details.

6. Consider the following protocol for proving quadratic non-residuosity of x modulo n:

   (1) Victor randomly chooses a number $r \in \mathbb{Z}_n^*$ and a bit b and sends to Peggy $y \equiv r^2 x^b \pmod{n}$.

   (2) Peggy sends to Victor $c = 0$ if and only if there is z such that $z^2 \equiv y \pmod{n}$, otherwise she sends $c = 1$.

   (3) Victor accepts if and only if $c = b$.

   (a) Is this protocol an interactive proof system?

   (b) Is it a zero-knowledge protocol?

   Justify your answers.