1 Quadratic residues

To understand the Blum Blum Shub algorithm and its proof of security, we need some basic theory about quadratic residues.

An integer $a \in \mathbb{Z}_n$ is called a quadratic residue modulo $n$ if there exists some $x$ such that $x^2 \mod n = a$. Otherwise, $a$ is a quadratic nonresidue modulo $n$. We denote the set of quadratic residues modulo $n$ by $QR_n$, and the set of quadratic nonresidues modulo $n$ by $NQR_n$.

Example 1 For $\mathbb{Z}_{23}$, we have $QR_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ and $NQR_{23} = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$.

The following theorem is due Euler:

**Theorem 1** Let $p$ be an odd prime number and let $a$ be a nonzero number in $\mathbb{Z}_p$. Then $a^{(p-1)/2} \mod p = 1$, or $a^{(p-1)/2} \mod p = p - 1$.

The following theorem is known as Euler’s criterion:

**Theorem 2** Let $p$ be an odd prime number and let $a$ be a nonzero number in $\mathbb{Z}_p$. Then the following are equivalent:

1. $a$ is a quadratic residue modulo $p$.
2. $a^{(p-1)/2} \mod p = 1$.

Hence we can also conclude that $a$ is a non-quadratic residue modulo $p$ if, and only if, $a^{(p-1)/2} \mod p = p - 1$. The quantity $a^{(p-1)/2} \mod p$ is denoted by a special symbol, called the **Legendre symbol**, which is $(\frac{a}{p}) = a^{(p-1)/2} \mod p$.

**Theorem 3** Let $p$ be an odd prime number and let $a$ and $b$ be nonzero elements of $\mathbb{Z}_p$. Then

1. $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$.
2. $(\frac{1}{p}) = 1$.
3. $(\frac{-1}{p}) = (-1)^{(p-1)/2}$.
Corollary 4  Let \( p \) be an odd prime number. Then \( \left( \frac{-1}{p} \right) = 1 \) if \( p \mod 4 = 1 \) and \( \left( \frac{-1}{p} \right) = -1 \) if \( p \mod 4 = 3 \).

Theorem 5  For an odd prime number \( p \), there are \( (p-1)/2 \) quadratic residues modulo \( p \), and there are \( (p-1)/2 \) non-quadratic residues modulo \( p \).

The following theorem is due Gauss:

Theorem 6  If \( p \) is an odd prime number, then \( \left( \frac{2}{p} \right) \) is equal to \( (-1)^{(p^2-1)/8} \).

The following theorem is known as Quadratic Reciprocity Law:

Theorem 7  Let \( p \) and \( q \) be odd prime numbers. Then \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = (-1)^{\frac{(p-1)(q-1)}{4}} \).

A prime \( p \) is called a **Blum prime** if \( p \mod 4 = 3 \).

Theorem 8  Let \( p \) be an odd prime number. Then \( -1 \in NQR_p \) if and only if \( p \) is a Blum prime.

Theorem 9  Let \( n = p \cdot q \) be the product of two distinct Blum primes. Let \( a \in QR_n \). Then \( a \) has exactly four square roots, exactly one of which is in \( QR_n \) itself.

2  **Blum-Blum-Shub pseudo random generator**

A pseudorandom generator is a deterministic algorithm that, given a truly random binary sequence of length \( n \), outputs a binary sequence of length \( m > n \) that “looks random”. The input to the generator is called the seed and the output is called the pseudorandom bit sequence. Security of a pseudorandom generator is a characteristic that shows how hard it is to tell the difference between the pseudorandom sequences and truly random sequences. For the Blum-Blum-Shub pseudorandom generator distinguishing these two sequences is as hard as factoring a large composite integer. The Blum-Blum-Shub pseudo random number generator is the following algorithm:

- Generate \( p \) and \( q \), two big Blum prime numbers.
- \( n := p \cdot q \).
- Choose \( s \in [1, n-1] \), the random seed.
- \( x_0 := s^2 \mod n \).
- The sequence is defined as \( x_i := x_{i-1}^2 \mod n \) and \( z_i := \text{parity}(x_i) \).
- The output is \( z_1, z_2, z_3, \ldots \) where \( \text{parity}(x_i) \) is 0 when \( x_i \) is even and 1 when \( x_i \) is odd.
### 3 Blum-Blum-Shub cryptosystem

Alice, the recipient, chooses two distinct Blum primes $p$ and $q$ and computes their product, $n = pq$. The number $n$ will be her public key, while its factorization is her private key.

Suppose Bob, the sender, has converted the message to a string of bits, say $M$. Let the individual bits, in their order of occurrence, be $b_0, b_1, b_2, ..., b_n$. He then chooses a number $1 < x_0 < n$ which is a quadratic residue modulo $n$, and computes the sequence $x_0, x_1, x_2, ..., x_n, x_{n+1}$ where for each $i \in [0, n]$ we have $x_{i+1} = x_i^2 \ mod \ n$. The choice of $x_0$ could be made as follows: Randomly choose a $z$ with $1 < z < n$, and put $x_0 = z^2 \ mod \ n$. Then for each of these $i$’s Bob computes $e_i = b_i + x_i \ mod \ 2$.

The encrypted message then is the sequence $e_0, e_1, e_2, ..., e_n$. Bob sends this string of bits, as well as $x_{n+1}$ to Alice.

Since $p$ and $q$ are Blum primes, for each quadratic residue $y$ modulo $n$ there is a unique quadratic residue $x$ modulo $n$ such that $x^2 = y \ mod \ n$. If the factorization of $n$ is known, then one can compute $x$ from $y$. Now Alice knows the quadratic residue $x_{n+1}$ which Bob sent her, as well as $n + 1$, the number of bits in the message, and so knows to compute square roots $n + 1$ times. By the guaranteed uniqueness, we see that Alice is in a position to recover the $x_i$’s in the following order: $x_n, x_{n-1}, ..., x_2, x_1, x_0$. Then she recovers the bits of the original message $M$ by performing the computations $m_i = e_i + x_i \ mod \ 2$ for $i = 0, 1, 2, ..., n$.

Note that indeed for each $i$ we have $m_i = b_i$. 
