Goldwasser–Micali (GM) cryptosystem

Goldwasser–Micali (GM) cryptosystem

The Goldwasser–Micali (GM) cryptosystem is an asymmetric key encryption algorithm developed by Shafi Goldwasser and Silvio Micali in 1982. GM has the distinction of being the first probabilistic public-key encryption scheme which is provably secure under standard cryptographic assumptions. However, it is not an efficient cryptosystem, as ciphertexts may be several hundred times larger than the initial plaintext.

Quadratic Residue

Goldwasser–Micali relies on deciding whether a given value x is a square mod N, given the factorization (p, q) of N. This can be accomplished using the following procedure:

1. Compute $x_p = x \bmod p$, $x_q = x \bmod q$.
2. If $x_p^{(p-1)/2} \pmod p = 1$ and $x_q^{(q-1)/2} \pmod p = 1$

then we say that x is a quadratic residue mod N.

On the contrary, if

1. If $x_p^{(p-1)/2} \pmod p = -1$ and $x_q^{(q-1)/2} \pmod q = -1$

then we say x is a quadratic non-residue mod N.

$x_p^{(p-1)/2} = -1 \pmod p$ and $x_q^{(q-1)/2} = -1 \pmod q$ are also often referred to as **Legendre Symbols.**

Key Generation

The process of generating a public and private key involves the following steps:

1. Randomly generate two large distinct prime numbers p and q.
2. Compute N = p * q.
3. Randomly generate x from the group of units modulo N until be find a quadratic non-residue by performing the following tests:
   a. $x_p^{(p-1)/2} \pmod{p} = -1$
   b. $x_q^{(q-1)/2} \pmod{q} = -1$
4. The public key will be (x, N). The private key will be (p, q).

Encryption

To encrypt an incoming message M, we follow these steps:

1. Retrieve the public key (x, N).
2. Convert the message M into a sequence of bits:
   a. For each character in M, determine its index within a predefined alphabet.
   b. Convert each index into its binary representation to create the bit sequence.
3. For every bit m_i:
   a. Generate a random value y_i from the group of units modulo N such that $\gcd(y_i, N) = 1$.
   b. Compute the encrypted bit $c_i = y_i^2 x^{mi} \pmod N$

Decryption

To decrypt an incoming ciphered message C, we follow these steps:

1. Retrieve the public key (x, N) and private key (p, q).
2. For each ciphered bit c_i determined whether c_i is a quadratic residue by performing the following tests:
   a. $x_p^{(p-1)/2} \pmod{p} = 1$
   b. $x_q^{(q-1)/2} \pmod{q} = 1$
3. If both tests succeed c_i is a quadratic residue and we mark the current bit as 1. If either of the tests fail, then c_i is not a quadratic residue and we mark the current bit as 0.
4. With the bits deciphered, we group the deciphered bits into sequences corresponding to characters and convert each group of bits back into characters using the predefined alphabet.