Rabin Cryptosystem

This is a passage that mainly describes how rabin cryptosystem works, including encryption and decryption.

1. History

The process was published in January 1979 by Michael O. Rabin. The Rabin cryptosystem was the first asymmetric cryptosystem[1] where recovering the entire plaintext from the ciphertext could be proven to be as hard as factoring.

2. Encryption

First we need to choose a semiprime number, which means its only factor are a pair of prime numbers, for example $n = 77 = p * q = 7 * 11$. This number N, the public key will be used to encrypt data. While p and q, the private keys, should only be known by recipient and used to decrypt.

Suppose we have a $P = \{0, 1, 2, \ldots, n-1\}$ which is the plaintext space and element m belongs to P. We can simply get the encrypted data by $c = m^2 \bmod n$.

Take $n = 77$ and $m = 20$ as an example, we can get $c = 400 \bmod 77 = 15$.

3. Decryption

1. $m_p = c^{(p+1)/4} \bmod p$

   $m_q = c^{(q+1)/4} \bmod q$.

   For our example, $m_p = 1$, $m_q = 9$.

2. Find y_p and y_q such that $y_p*p + y_q*q = 1$.

   For our example, $y_p = -3$, $y_q = 2$.

3. $r = (y_p * p * m_q + y_q * q * m_p) \bmod n$

   $-r = n – r;$

   $s = (y_p * p * m_q – y_q * q * m_p) \bmod n$

   $-s = n – s$

   For our example, we can solve these all four data are 64, 20, 13, 57.[2]

4. References:

1. https://en.wikipedia.org/wiki/Rabin_cryptosystem#References
2. https://www.math.auckland.ac.nz/~sgal018/crypto-book/ch24.pdf

Notes:

[1]. asymmetric cryptosystem: cryptosystem that use different keys to encrypt and decrypt.

[2]. For most cases, the encryption is a 4 to 1 system, therefore we need some redundant to choose the correct decrypted data. For example, we can send a message to choose the data with some lower bits are 1, as for large numbers, it is uncommon to get two square numbers with such same patterns. Also other math algorithm are acceptable.