Rabin Crypto System Overview

Murat Kantarcioglu

The Rabin Cryptosystem

- Computationally secure against a chosen plaintext attack
  - Provided that the modulus n = pq can not be factored.

$$p \equiv q \equiv 3 \ (mod 4)$$

- n is the public key. The primes p and q are the private key.
- Choose to simplify the computation of square roots modulo p and q

The Rabin Cryptosystem

- B encrypts a message m and sends the ciphertext c to A

- Encryption:
  - Obtain A's public key n.
  - Represent the message as an integer m in the range {0, 1, . . . ,n-1}.
  - Compute $c = m^2 \ mod \ n$
  - Send the ciphertext c to A

The Rabin Cryptosystem

- A decrypts the ciphertext c as follows:

- Decryption:
  - Compute $\sqrt{c} \ mod \ n$
  - There are four square roots m_1, m_2, m_3, m_4 of c modulo n.
  - The message m is equal to one of these four messages

The Rabin Cryptosystem

- When $p \equiv 3 \; mod \; 4$ there is a simple formula to compute the square root of c in mod p.

$$\begin{aligned}(\pm c^{(p+1)/4})^2 &\equiv c^{(p+1)/2} \; mod \; p \\ &\equiv c^{(p-1)/2} \; c \; mod \; p \\ &\equiv c \; mod \; p\end{aligned}$$

- Here we have made use of Euler's criterion to claim that $c^{(p-1)/2} \equiv 1 \; mod \; p$

The Rabin Cryptosystem

- Hence the two square roots of c mod p are

$$\pm c^{(p+1)/4} \; mod \; p$$

- In a similar fashion, the two square roots of c mod q are $\pm c^{(q+1)/4} \; mod \; q$
- Then we can obtain the four square roots of c mod n using the Chinese Remainder Theorem

The Rabin Cryptosystem

- Example: $n = 77 = 7 \times 11$
  - Suppose $c = m^2 \ mod \ 77$
  - Then for message m the ciphertext c is computed as $\sqrt{c} \ mod \ 77$
  - And for decryption we need to compute
    $c \equiv 10^2 \equiv 23 \ mod \ 77$
  - Suppose Alice wants to send message m = 10

The Rabin Cryptosystem

- To find the square roots of 23 in mod 7 and in mod 11 we can use the formula since 7 and 11 are cogruent to 3 mod 4.

$$23^{(7+1)/4} \equiv 2^2 \equiv 4 \ mod \ 7$$

$$23^{(11+1)/4} \equiv 1^3 \equiv 1 \ mod \ 11$$

The Rabin Cryptosystem

- Using the Chinese Remainder Theorem, we compute the four square roots of 23 mod 77 to be

$$\pm 10, \pm 32 \; mod \; 77$$

- Therefore the four possible plaintexts are

$$m_1 = 10, \; m_2 = 67, \; m_3 = 32, \; m_4 = 45$$