Outline

Rabin encryption scheme

Elgamal encryption scheme

Rabin Encryption Scheme

public keys : $N = pq$, a product of two distinct odd primes.
$p \equiv q \equiv 3 \mod 4$

private keys : p, q

encryption : $c = m^2 \mod N$

decryption : m is a square root of $c \mod N$.

Alice knows p, q, knows how to find square roots of $c \mod N$.

$c_p = c \mod p$
$c_q = c \mod q$

square roots of c_p is $\pm c_p^{\left(\frac{p+1}{4}\right)}$: $m_1, -m_1$
square roots of c_q is $\pm c_q^{\left(\frac{q+1}{4}\right)}$: $m_2, -m_2$

use CRT to compute m s.t. $m \equiv \pm m_1 \mod p$
$m \equiv \pm m_2 \mod q$

Eve doesn't know p, q. Eve needs to solve square root modulo N.

This is a hard problem.

Rabin vs RSA

Advantage: Encryption is faster in Rabin.
(Decryption speed is the same)

Disadvantage: There are four square roots of $c \mod N$.
Four potential plaintexts.
Extra information about the plaintext is required.

Similar with RSA: Rabin is also deterministic.

Theorem: N is called a Blum integer if $p \equiv q \equiv 3 \mod 4$.

Given $x \in QR_N$. There exactly one square root of x which is a QR.

Application: If $\boxed{m \in QR_N}$, then $c = m^2 \mod N$ has exactly one square root which is a QR, hence, we know which one is original plaintext.

Textbook Rabin: $m \in \mathbb{Z}_N^*$

Blum version: $m \in QR_N$ $\quad |QR_N| = \frac{1}{4} |\mathbb{Z}_N^*|$

Padded version: $m \| \underbrace{1\,1\,1\,1\,1}_{\ell}$

Probabilistic Encryption

The same plaintext can be encrupted into different ciphertexts.

Elgamal

Public parameter creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Alice	**Bob**
Key creation	
Choose private key $1 \le a \le p-1$. Compute $A = g^a \pmod{p}$. Publish the public key A.	
Encryption	
	Choose plaintext m. Choose random element k. Use Alice's public key A to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$. Send ciphertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	$(g^{ka})^{-1} m g^{ak} = m$

Table 2.3: Elgamal key creation, encryption, and decryption

This is called 2-1 msg. expansion.

Given A, P, g, find $g^a \equiv A \bmod p$.

This is Discrete Logarithm problem (DLP) which is hard problem.

If we can solve DLP, then we can break Elgamal.

Given A, B, P and g where $A = g^a \bmod p$ and $B = g^b \bmod p$.
to find $g^{ab} \bmod p$.
This is Diffie-Hellman problem (DHP).

If we can solve DHP, then we can break Elgamal.
[Homework]