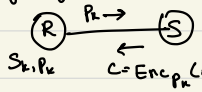
Review

- Public Key Cryptography

$m = Dec_{Sk}(c)$



- Diffie-Hellman Key Exchange Protocol
- El Gamal Public Key Cryptosystem
- El Gamal is CPA secure

El Gamal is not CCA secure

El Gamal is partially Homomorphic Encryption scheme

Given $E(m_0)$ & $E(m_1)$ we can get $E(m_0 m_1)$ for some choices of group operations

If $c_0 = g^{r_0}, m_0 \cdot g^{r_0 a}$

Choose an r, get $c_1 = g^{r_1}, r \cdot g^{r_1 a}$

Then get decryption of $c' = g^{r_0+r_1}, m_0 \cdot r \cdot g^{(r_0+r_1)a}$

Not CCA secure

$Enc_{P_k}(m) = m^e \bmod N$

$Dec_{S_k}(c) = c^d \bmod N$

Euler's theorem:

$a^{\phi(N)} \bmod N = 1$, if $gcd(a,N) \equiv 1$

Lagrange's Theorem: If H is a subgroup of G, a finite group, then $o(H) \mid o(G)$ (order $(|H|)$)

Correctness of RSA:

$$\begin{aligned} Dec_{S_k}(c) &= c^d \bmod N \\ &= (m^e \bmod N)^d \bmod N \\ &= m^{ed} \bmod N \\ &= m^{ed \bmod \phi(N)} \bmod N \\ &= m \end{aligned}$$

This RSA scheme was deterministic & thus is not CPA secure.

RSA:

Gen (1^n): $P_k = \langle N = pq, e \rangle$

$gcd(e, (p-1)(q-1)) = 1$

$S_k = p, q, d$ $\quad e \cdot d \equiv 1 \bmod (p-1)(q-1)$

$|Z_N^*| = \phi(N)$ numbers less than N coprime to N

$$\begin{aligned} \phi(N) &= N - \frac{N}{p} - \frac{N}{q} + \frac{N}{pq} \\ &= pq - q - p + 1 = (p-1)(q-1) \end{aligned}$$

Internet-RSA:

$c = (00\ 0\ 0..0 \underset{\text{2 bytes of 0s}}{\longleftrightarrow} \underset{\text{All as byte}}{\underset{\searrow}{r}} \geq 8 \text{ bytes}\ 0000\ m)^e \bmod N$

For RSA, MSB is easy to get & LSB is hard.

r is not truly random, cannot have a byte of all 0s