Lecture 39, Nov. 21

39.1 Definition (RAS)**.** Key Generation: Randomly pick p,q primes $n = pq$ pick $e{\cdot}d = 1 \mod \phi(n)$ Encryption: $c = m^e \mod \phi(n)$

Some attack on RSA Collect a lot of $n_i = p_i \cdot q_i$. Compute gcd of n_i, j_i where $i \neq j$. Some gcds are not equal to 1 and thus n_i can be factored.

$$\text{number of primes} < 2^{512} \approxeq \frac{2^{512}}{512 \cdot log2}$$
$$\text{number of primes} < 2^{511} \approxeq \frac{2^{511}}{511 \cdot log2}$$
$$\text{number of primes with 512 bits} \approxeq 2^{500}$$

39.2 Example. Sometimes e = 3

Advantage: faster encryption

Disadvantage: $n \approxeq 2^{2048}$ if $m < 2^{600} m^3 \mod n = m^3$ as integer

In practice: Padding of m is about 600, where the total from 1 random m is about 2000.

Digital Signature

1. Authentic
2. Alice which is the sender cannot deny the message she sent (non-repudiation)

39.3 Example (Naive TSA Signature)**.** (Where Alice sent a message to Bob and Eve is the outsider)

(n,e) is a public key for Alice

d is a private key for Alice

$$S = m^d \mod n$$

Bob will verify by comparing $S^e \mod n$ (where S is the signature).

Attack Models

1. Key-Only Attack: Eve only knows Alice's public key
2. Known-Message attack: Eve knows some (m_i, s_i)
3. Chosen-message attack (CMA): Eve can obtain signature s_i for arbitrary message m_i.
4. Totally broken: Eve can sign any message m.
5. Selection Forgery: Eve can sign one message of her choice.

6. Existential Forgery (ET): There exist a message that Eve can sign.

   Note. We call Digital Signature a secure if Eve cannot achieve ET using CMA.

Claim. For the pervious exmaple: (1,1) is always valid, and thus we claim that it is totally broken under CMA

Proof. Given any m, Pick $a, b \neq 1$ such that $a \cdot b = m \mod n$

Eve can obtain $s_1 = a^d \mod n$ and $s_2 = b^d \mod n$. Then $s_1 \cdot s_2 = (ab)^d = m^d \mod n$. □

To make it more secure, we will apply some functions on the message on called the hash function.

39.4 Example (Hash Function)**.** $H : \{0,1\}^k \to \{0,1\}^n$ is takes an infinite set to a finite set.

Preimage Resistant: for every y, it is hard to find H(m)= y

2nd Preimage Resistant: for every value of m, it is hard to find $m' \neq m$ such that $H(m) = H(m')$

Collision Resistant: it is hard to hard m and m' with $H(m) = H(m')$

Note: Collision Resistant implies 2nd Preimage Resistant. For such function, it should occur that $H(a, b) \neq H(a) \cdot H(b)$

39.5 Example. if H is not preimage resistant, then Eve can find m such that H(m) = 1

Since 1 is a signature for m, if H is not collision resistant, Eve can compute m, m' a collision

Under a CMA, request signature for m' that's also signature for m.