28.02.2020

NO CLASS

03.03.2020

RSA

- "Textbook" RSA
- Some Attacks
- PKCS v1.5
- RSA signatures

Outline for today's class and how the internet standards deal with it.

Textbook RSA

Gen: Choose 2 large distinct primes p, q and $N = pq$

choose (e, d) s.t. $ed \equiv 1 \bmod [(p-1)(q-1)]$

Public Key: $\langle N, e \rangle$

Private Key: $\langle d, p, q \rangle$

Given we know Primality testing (Miller Rabin, etc), , [Algorithms course (Kannan, et al Monsoon 2018)]

so we do not prove that this is efficiently computable.

Enc: $m \in \{0, 1, 2, \ldots, N-1\}$

$C = m^e \bmod N$

Dec: $c \in \{0, 1, 2, \ldots N-1\}$

$m = c^d \bmod N$

Efficient algos for both exist

doubling technique

Now for correctness, by Euler's theorem

euler's theorem

$$a^{\phi(N)} \equiv 1 \bmod N$$

Defn: $\phi(N)$ is the no. of nos. $< N$ that are co-prime to N

Euler's totient

euler's totient

Now, $(m^e)^d \bmod N = m^{ed} \bmod N$

Again, and now, $m^{\phi(N)} \bmod N = 1$

euler's totient of N=pq

and $\phi(pq) = (p-1)(q-1)$

and we know $ed \equiv 1 \bmod N$

or $N \mid k(ed) + 1$

TODO COMPLETE

Textbook RSA is not CPA-Secure

Now going back to Textbook RSA,

- it is deterministic
- so, is ciphertext-only secure, not CPA secure

> but in public key systems, notion of adversary does not have oracle access is meaningless. As it is public
>
> ⇓
>
> so, CPA is easily mountable
>
> ⇒ minimum security required for PKC is CPA-secure
>
> ⇒ there can be no PKC system that is deterministic, as
>
> - deterministic ⇒ no CPA security
> - PKC needs a min of CPA security.

Looking at other attacks

⊙ If $e=3$ (or small) and m is also small

eg: $m < \sqrt[3]{N}$

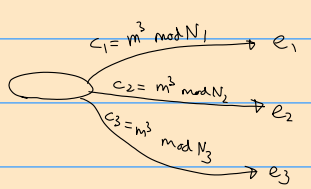
$c = m^3 \bmod N$

$\Rightarrow c = m^3$

or $m = \sqrt[3]{c}$

⊙ Same e with multiple people

eg: $e=3$, N_1, N_2, N_3



consider: $x = c_1 \bmod N_1$, $x = c_2 \bmod N_2$, $x = c_3 \bmod N_3$ } CRT says ∃ unique x such that all 3 hold.

Unique $x \in [0, N_1 N_2 N_3 - 1]$ s.t.

Chinese Remainder Theorem

Looking at the suggestions for modified RSA

"recommended by current Internet": PKCS v. 1.5

((∃ no proof that this rec is secure))

((but ∃ other algos (nonstandard) that are provably secure))

Gen:
- Same as regular RSA
- there are some restrictions on prime selection, but we can just say "any large primes should work"

we modify this to make it secure.

Enc: Ciphertext $C = [\quad]^e \bmod N$

$\log N$ bit no. / $(\log N)_8$ byte no. of "K"-byte no.

Constructing the number:

- first byte : fixed (01000000, he says from memory)
- second " : " all 0's

then, at least

- 8 more bytes are filled with random (not truly random — none can be all 0s)

then, another set of 00000000

then, message m (at most K−11 bytes)

for decryption:

- ignore first byte
- " second "
- " byte after byte after byte until we hit another all−0 byte.
- then, print the rest as message.

General Idea of Working

somehow, they decided

− first 16 MSBs are very weak

???

− at least 64 bits of random r recommended

↳ but not fixed. So message start unknown, cannot build easy algo

⇒ getting to hard-core predicate (RSA ka LSB) difficulty.

h(RSA) is LSB

~~ this is modern internet.

Q: Can RSA be made provably secure?

A: Yes. RSA-OAEP (Optimal Assymetric Encryption Padding)

Kannan Trivia

RSA based schemes are hard to prove. For provable we use discrete log based schemes, like El Gamal.

RSA-based Digital Signatures (will show deterministic → attacks → randomized)

Defining signatures → **Req:** • Adv should not be able to produce new m, σ without sk.

$A \xrightarrow{m} B$ • auth data • auth user

so

$A \xrightarrow{m, \sigma_A} B$ s.t. • σ Alg known to everyone

• ∃sign, uses private key of A

• ∃Verify, uses public of A to verify signature done by A.

RSA – signature says,

sign (d, m) : $m^d \bmod N = \sigma$ ← signature

verify $(m, e, \sigma) =$ yes if $\sigma^e \bmod N = m$

Sign yourself with sk
Verify by others " pk.

Breaking Vanilla (Textbook) RSA – sign

I. • choosing m, then σ is hard.

Algorithm

• But, do reverse:

1. Choose random signature σ
2. Compute $\sigma^e \bmod N$
3. Send $\langle \sigma^e \bmod N, \sigma \rangle \longrightarrow$

Verify $(\sigma^e \bmod N, \sigma, (N,e)) =$ yes.

II. Improved Attack

Algorithm

• suppose I have $\langle m_1, \sigma_1 \rangle$ sent by A.

• A also sent $\langle m_2, \sigma_2 \rangle$

• We produce third message that A never sent : $\langle m_1 m_2 \bmod N, \ \sigma_1 \sigma_2 \bmod N \rangle$

now, CPA from this :

we want to sign M
- ask for σ for m_1
- ask for σ for m_2

s.t. $M = m_1 m_2$ } Done

New Paradigm: → instead of signing directly

Hash and Sign Paradigm

signature $\sigma = [H(m)]^d \bmod N$ | Yes if $\sigma^e \bmod N = H(m)$

Signing | Verifying

(why do old attacks not work) Collision resistance

Proof: None for RSA

Rest of Course: a) A few more PKCs

b) Proof of CPA security for El-Gamal PKC

c) El-Gamal is not CCA – secure

d) CCA – secure PKCs

This should be done by mid-march

then sir will "talk about what we actually want to do"

"freedom to work, not freedom from work"