Oct5

Monday, October 4, 2021 10:40 AM

RSA: Rivest-Shamir-Adleman (1977)
Clifford Cocks (1973)
$\hookrightarrow$ declassified in 1997

What is the hard problem?

Recall: Diffie-Hellman & Elgamal relied on Discrete Log:

If $a^x \equiv b \mod p$, find x.

RSA Problem

If $x^e \equiv c \mod N$

find x.

Difficult problem is computing e'th root.

Rmk
HW5
Sun Tzu $\longleftrightarrow$ Square roots mod N to Square roots mod factors of N.

Prop (Solution to RSA w/ prime modulus)
p - prime. $e \geq 1$ w/ $\gcd(e, p-1) = 1$

Let $d = e^{-1} \mod p-1$

Then $\boxed{x^e \equiv c \mod p}$ has a unique solution $x \equiv c^d \mod p$.

Proof

→ If $c \equiv 0 \mod p$ then $x \equiv 0 = c^d \mod p$ a unique solution.

→ Else $de = 1 + k(p-1)$

$$(c^d)^e = c^{de} = c^{1+k(p-1)}$$

$$= c \cdot \cancel{(c^{p-1})^k} \leftarrow 1 \text{ by Fermat}$$

$$\equiv c \mod p.$$

Uniqueness of e'th root

x_1 & x_2 are e'th roots of c mod p

$$x_1 \equiv x_1^{de} \equiv (x_1^e)^d \equiv c^d \equiv (x_2^e)^d \equiv x_2^{de} \equiv x_2 \mod p$$

Rmk.

* RSA problem is easy with prime modulus.
* Recall square roots not unique mod p...
(HW 2,4,5) p odd   didn't always exist

$\gcd(2, p-1) = 2 \neq 1$.

* If $\gcd(e, p-1) \neq 1$ may have multiple (if two?) roots or no roots....

Last Time

Theorem (Euler's Theorem)

Let $N = pq$ w/ p, q prime.

Let g a divisor of $(p-1)$ & $(q-1)$

Then $\forall$ $a \in (\mathbb{Z}/N\mathbb{Z})^*$

$$a^{\frac{(p-1)(q-1)}{g}} \equiv 1 \mod N \leftarrow$$

In particular

$$a^{(p-1)(q-1)} \equiv 1 \mod N \leftarrow$$

Prop (solution to RSA w/ $N = pq$ factored)

Let p, q distinct primes. $e \geq 1$ w/ $\gcd(e, (p-1)(q-1)) = 1$.

Let $d = e^{-1} \mod (p-1)(q-1)$.

Then

$$\boxed{x^e \equiv c \mod pq}$$

has a unique solution $x = \underline{\underline{c}}^d \mod pq$.

Pf/ $de = 1 + k(p-1)(q-1) \leftarrow 1 = de - k(p-1)(q-1)$

so $(c^d)^e = c^{de}$

$$= c^{1+k(p-1)(q-1)}$$

$$= c \cdot \cancel{\left(c^{(p-1)(q-1)}\right)}^k \leftarrow 1 \text{ by Euler.}$$

$$= c \mod pq$$

Rmk Used $\gcd(c, pq) = 1$

If $\gcd(c, pq) \neq 1$, HW.

Uniqueness

If u is another solution, $\underline{u^e = c}$

$$u = u^1 = u^{de - k(p-1)(q-1)}$$

$$= u^{de}$$

$$= (u^e)^d$$

$$= c^d \mod pq.$$ ✓

Rmk

Goal find $\sqrt[e]{c} \mod pq$.

Our algorithm is

1) compute e^{-1} mod $(p-1)(q-1)$
2) comput $c^{e^{-1}}$ mod pq.

RSA

Hard problem

Compute $\sqrt[e]{c}$ mod N

Extra Info

Know $N = pq$ w/ p, q prime.

Hard problem becomes easy

$$\sqrt[e]{c} = c^{e^{-1} \bmod (p-1)(q-1)}$$

RSA

Bob Eve **Alice.**

① Bob chooses secret primes p, q

② Bob chooses encryption exponent $e \geq 1$ w/ $\gcd(e, (p-1)(q-1)) = 1$

③ Bob computes $N = pq$ & publishes (N, e)

Encryption

1) Chooses plaintexts $m \in \mathbb{Z}/N\mathbb{Z}$
2) Alice encrypts

$$c = m^e \bmod N$$

3) Alice sends c

Decryption

① Bob computes

$$d = e^{-1} \bmod (p-1)(q-1)$$

(decryption exponent)

② Bob computes

$$c^d \bmod N$$

That's m

Proof of correctness

m is an e'th root of c

c^d is too.

The root is unique mod N

so $c^d \equiv m$

Example

Bob

* Secret primes are

$p = 3, \; q = 5$

so $pq = 15$

* $e = 3$

Alice

* $m = 7$

* $c = m^e$

$= 7^3 = 343 \equiv 13 \bmod 15$

---

* $(p-1)(q-1) = 2 \cdot 4 = 8$

$3^{-1} = 3 \bmod 8$

* Bob computes

$$c^d = 13^3 = 2197 \equiv 7 \bmod 15$$

Project 9: Implement this & send messages on Discord.

Security of RSA

Setup $N = pq$, $e, c \in \mathbb{Z}$

Problem solve $x^e \equiv c \mod N$ for x

Easy If I know p & q, compute
$d = e^{-1} \mod \underbrace{(p-1)(q-1)}$
Solution is c^d

Hard Eve doesn't know p & q.

First observation

- Don't technically p & q, just the product $(p-1)(q-1)$

Q. Can we deduce this from pq w/o factoring?

$N = pq$	$(p-1) \cdot (q-1)$	
$14 = 7 \cdot 2$	$6 \cdot 1 = 6$	
		+
$15 = 3 \cdot 5$	$2 \cdot 4 = 8$	
		+
$21 = 7 \cdot 3$	$6 \cdot 2 = 12$	

Figuring out this pattern isn't obviously any easier than factoring

$22 = 11 \cdot 2$

$26 = 13 \cdot 2$

$33 = 11 \cdot 3$

$34 = 17 \cdot 2$

$10 \cdot 1 = 10$

$12 \cdot 1 = 12$ +

$10 \cdot 2 = 20$ +

$16 \cdot 1 = 16$ −

$O(N)$

$N = pq$

$p, q \approx \sqrt{N}$

$\Rightarrow (p-1)(q-1) \approx N$

Observation $N = pq$

To solve $x^e = c \mod N$, I just $\underline{\underline{(p-1)(q-1)}}$ not necessarily pq.

↑ compute e^{-1} here.

In fact, finding $(p-1)(q-1)$ is no easier than factoring N.

Prop Suppose p, q distinct primes & $N = pq$.

Then the following peices of information are equivalent.

i) Knowing N, p, q.

ii) knowing N, $(p-1)(q-1)$

iii) knowing N, $p+q$.

Proof

(i) $\Rightarrow$ (ii) clear.

(ii) $\Rightarrow$ (iii) Find $p+q$.

well $A = (p-1)(q-1) = pq - p - q + 1$

So $$p+q = \underbrace{pq}_{N} - A + 1$$

know all this

$(iii) \Longrightarrow (i)$

Can write the equation

$$f(x) = x^2 - (p+q)x + N$$

$$= (x-p)(x-q)$$

Two roots of f are $x=p$ & $x=q$.
Use quadratic formula to find p & q.

Rmk

Upshot: knowing $(p-1)(q-1)$ is not any easier than factoring N.

⚠ Warning

Does not imply that there isn't some other clever way to solve $x^e \equiv c \bmod N$ w/o factoring N.

Attacks

① Chosen Plaintext attack

⇝ Eve choose m & see the pair (m, c). ($c = m^e \bmod N$ Eve knows (e, N)

⇝ Public Key Crypto is by definition secure to Chosen Plaintext.

very false w/ symmetric encryption.

Ex. $e_k(m) = km$

So eve computes $e_k(1) = k$ ← gets secret key.

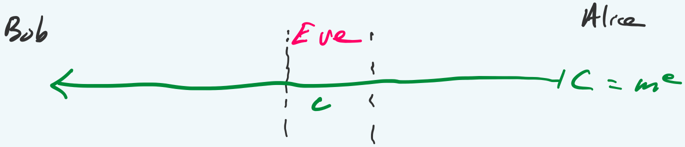
② Chosen Ciphertext Attack

Eve can choose $c \in \mathbb{C}$ & see the decryption $d(c) = m$.

e.g./ 1) Gain one time access to Bob's machine.

2) Convince Bob to decrypt a message for you (perhaps to prove Bob's identity).

↑ Never do this if you are bob.



Eve knows c. Eve can use Chosen Ciphertext in 2 ways.

Option A

Eve asks Bob to decrypt c.

Bob returns $c^d = m$ ← eve knows message.

Bob's machice machine may refuse to decrypt a ciphertext already received.

Option B

- Eve choose random $k \in (\mathbb{Z}/N\mathbb{Z})^*$ & computes $c' = c \cdot k^e$
- Eve asks Bob to decrypt c'
- Bob returns $(c')^d = (c\,k^e)^d = \underset{\overset{\uparrow}{m}}{c^d} \cdot k^{ed}$

$$= m \cdot k$$

"masking"

- Eve computes $(mk)\cdot k^{-1} = m$

Rmk

- Eve recovers m w/o ever factoring or even solving RSA problem.
- Bob can't see that c' is related to c, because k random.

Example (Never use multiple encryption exponents for one modulus).

e.g. (N, e_1, e_2) Alice sends

$$c_1 = m^{e_1} \quad \& \quad c_2 = m^{e_2}$$

Might be that $\gcd(e_1, e_2) = \underset{\uparrow \text{common}}{1}$ (at least small)

Eve $e_1 u + e_2 v = g = 1$

$$c_1^{u} \cdot c_2^{v} = (m^{e_1})^{u} (m^{e_2})^{v}$$

$$= m^{e_1 u + e_2 v} = m$$

got m

Note in implementing RSA, the security depends on the secretness of your primes.

Finding Large Primes

Observe

Not good enough to find large composites,

$m, n >> 0$ & $N = mn$

Not true that $a^{(m-1)(n-1)} \neq 1 \bmod N$.

Rmk

There is a generalization of Euler's theorem, but the exponent depends on factors of N.

(HW?)

Non-example

Is $n = 15485207$ prime?

Try to factor... no factors < 100

But $2^{n-1} \equiv 4136685 \bmod n$

$\neq 1$

So n can't be prime.

(if it were, we'd have Fermat).

Fermat

For every $a \in \mathbb{Z}$, p prime, $\underline{a^p \equiv a} \mod p$.

Pf/ If $p \mid a \Longrightarrow$ $\underline{✓}$ $0^p \equiv 0 \mod p$

If $p \nmid a \longrightarrow a^{p-1} \equiv 1 \mod p$

$\}\cdot a$

$a^p \equiv a \mod p$ ∎

Point

If n prime $\underset{\xleftarrow{?}}{\Longrightarrow}$ $2^n \equiv 2 \mod n$.

Potential strategy to find primes:

Guess a # & see if Fermat works.

Note This strategy fails.

$$2^{341} \equiv 2 \mod 341$$

↑ $= 11 \cdot 31$ not prime.

Philosophically:

$2^n \equiv 2 \mod n \rightsquigarrow$ more likely to be prime.

Def^n

An integer a is a **Fermat witness** to the compositeness of n if $a^n \not\equiv a \mod n$.

Rmk

1 witness tells me 100% that a is composite.

Potential strategy

Keep checking for Fermat witnesses. The more I get, perhaps the more likely it is I have a prime. This doesn't always work.

Example

$$561 = 3 \cdot 11 \cdot 17.$$

But $a^{561} \equiv a \mod 561$ all $a \in \mathbb{Z}$.

Exercise

check w/ a loop on cocalc.

So... no Fermat witness even though 561 is composite.

Def^n

A composite number n is called a **Carmichael number** if it has no Fermat' witnesses.

Theorem (Alford, Granville, Pomerance, 1994)

There are ∞-ly many Carmichael numbers.

Need something slightly better.

Fermat test ⇝ Fermat witnesses.

↓

Miller-Rabin test ⇝ Miller-Rabin witnesses.

↑ See on Thursday.