Oct8

Wednesday, October 7, 2020 10:40 PM

Project 1 Due Thursday 15th.

Include some written stuff.

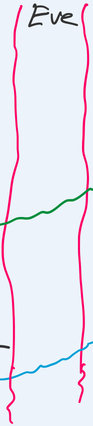
RSA:

Bob

- Bob chooses large primes p, q.
- Bob choses e w/ $\gcd(e, (p-1)(q-1)) = 1$
- Bob publishes (N, e)

$N = pq$

public key.



Alice

Alice has a message $m \in \mathbb{Z}/N\mathbb{Z}$.

Alice computes

$c = m^e \bmod N$

ciphertext

Bob knows

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

Bob computes c^d

$= m^{ed} \bmod N$

$\equiv m \bmod N$

Euler's formula: p, q prime. $N = pq$ $\Rightarrow$ $a^{(p-1)(q-1)} \equiv 1 \bmod N$

Example

Bob chooses

$p=3 \quad q=5$

$e=3$

Public Key $(15,3) \rightsquigarrow$ Alice $m=\boxed{13}$

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

$7 \leftarrow$ find $\sqrt[3]{7}$

$(p-1)(q-1)$

$=2\cdot 4=8$

$d=e^{-1}=3^{-1}=3$

$7^3 \equiv \boxed{13} \bmod 15$

Remarks

N – modulus

e – encryption exponent } Public key

d – decryption exponent ← secret key.

Notice e & d determine eachother.

Attacker wants to solve the equation $x^e \equiv c \bmod N=pq$ for x.

Seen know p,q, $\sqrt[e]{\ } \Longleftrightarrow (-)^d$ where

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

Notice

A priori I don't need to know p, q just the value $(p-1)(q-1)$. Maybe I can find this value more easily than I can factor N.

↑ Turns out these are equivalent.

Prop If $N=pq$ is a product of primes. Then

$$\begin{tikzcd}
\text{① Knowing } N \text{ \& } p,q \arrow[rr, Leftrightarrow] \arrow[dr, Leftrightarrow] & & \text{② Knowing } N \text{ \& product } (p-1)(q-1) \arrow[dl, Leftrightarrow] \\
& \text{③ Knowing } N \text{ \& } p+q &
\end{tikzcd}$$

Pf/

Show ① ⇒ ② ⇒ ③ ⇒ ①

① ⇒ ② Easy.

② ⇒ ③ $\underbrace{(p-1)(q-1)}_{\text{know}} = pq - (p+q) + 1$

know

So $\underline{p+q} = N - (p-1)(q-1) + 1$

↑ found it.

③ ⇒ ①

write $f(x) = x^2 - (p+q)x + N$ ←

Apply quadratic formula

2 roots are p & q ←

Pf/ $x^2-(p+q)x+pq = (x-p)(x-q)$

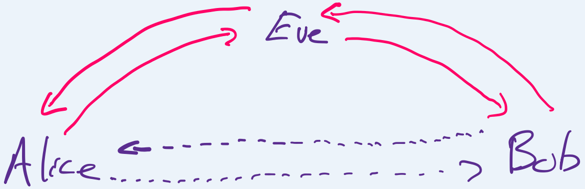
Remark

Finding product $(p-1)(q-1)$ no easier than factoring N.

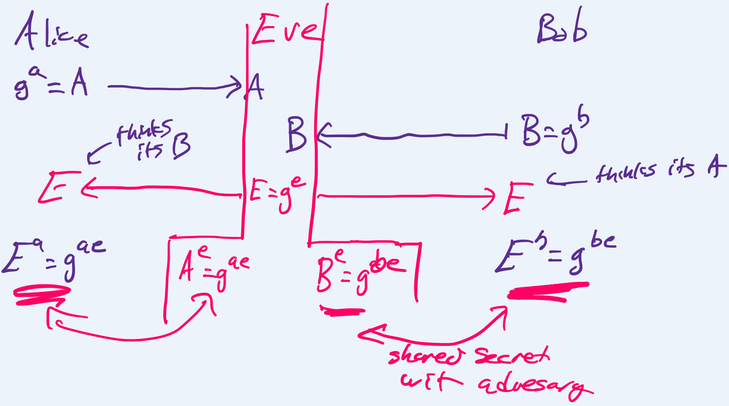
⚠ Not imply that some other mysterious way of solving $x^e \equiv c \mod N$ doesn't exist.

Attacks that don't require solving the hard problem (or warnings!)

Examples (Woman-in-the-middle Attack)



$g \in \mathbb{F}_p^*$



- *Alice & Bob share a secret w/ Eve instead of eachother, & are unaware
- * Eve didn't even solve the DHP!

Remark Public key crypto is (almost by def^n) immune to the chosen plaintext attack!

(e.g. w/ RSA m^e reduce mod N $= c$)

Example (Chosen ciphertext Attack)

Eve gets alice to decode a chosen cipher & share the plaintext.

Eve gives Alice c, Alice shares c^d mod N.

Remark This is not absurd, e.g. Alice could do this to prove ownership of a public key (N, e).

Suppose alice is so generous

Case 1

Bob sends $\overset{m^e}{\overset{\shortparallel}{c}}$ to Alice

Eve intercepts c.

Eve asks Alice to prove she can decrypt c. Alice share $c^d \equiv m$

↑ maybe alice refuses b/c she knows c is from Bob.

Case 2

- Bob sends $c = \boxed{m^e}$ mod N to Alice.
- Eve intercepts c.
- Eve computes random k & $\underset{\overset{\parallel}{c'}}{k^e \cdot c}$ mod N.

notice difference btwn c, c' is k^e looks random to Alice

- Asks alice to decrypt c'.
- Alice Agrees Eve gets

$$m' = (k^e c)^d = (k^e m^e)^d = k^{ed} m^{ed}$$

$$\equiv \underline{km} \text{ mod } N$$

- Eve knows $\boxed{k}$, knows k^{-1}, computes $k^{-1} \cdot k \cdot m \equiv \boxed{m}$ mod N.

Moral: Don't use RSA to prove your identity (& decode messages).

Notice Eve did not break RSA
↳ didn't factor N
↳ didn't compute φ.
Eve had Alice do it for her.

Example (only use 1 encryption exponent per modulus?).

Fix (N, e_1, e_2). $\underline{\text{Good chance } \gcd(e_1, e_2) = \boxed{1}}$

Eve compute $ue_1 + ve_2 = g$

Bob encrypts m w/ both exponents

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

Eve: $c_1^u c_2^v = m^{ue_1} m^{ve_2} = m^{ue_1 + ve_2} = m^g$

$= m$

As above, no factoring or roots. Just Ext. Euc. Alg.

Alice ready to open up Cocalc and generate an RSA public key.

....Needs 2 large secret primes

Finding Large Primes

Remark Not good enough to find large composite numbers n, m, b/c Euler's formula isn't $a^{(n-1)(m-1)} \equiv 1 \mod nm$ in general.

(there is a general form of Euler's thm)

Non Example

n = 15485207. Is it prime? Try factoring can't find any small ones.

Factoring slow

$2^{n-1} = 4136685 \mod n$?

Conclude n not prime!

Why? Fermat!

Fast powering is fast.

Theorem (Fermat's Little Theorem).

p prime. $a \in \mathbb{Z}$.

$$a^p \equiv a \bmod p. \leftarrow$$

Pf/ $p \nmid a$ FLT $\Rightarrow a^{p-1} \equiv 1 \bmod p$. $\times a$ on both sides.

If $p \mid a$ $\quad a^p \equiv 0 \equiv a \bmod p$.

So

$$n \text{ prime} \underset{\not\Longleftarrow\ ?}{\Longrightarrow} \underline{2^n \equiv 2 \bmod n}.$$

If $2^n \equiv 2 \bmod n$ is n prime?

No!

$$\boxed{\begin{gathered} 2^{341} \equiv 2 \bmod 341 \\ 341 = 11 \cdot 31 \quad \text{not prime} \end{gathered}}$$

Remark

Philosophically if $2^n \equiv 2 \bmod n$ we can think of this as meaning it is more likely that a is prime.

If $2^n \not\equiv 2 \bmod n$, n can't be prime

100%

Defn We say a is a witness for the compositeness of n if $a^n \not\equiv a \bmod n$.

Rmk

1 witness proves n is composite!

Feeling

If I find more & more a w/ $a^n \equiv a \bmod n$ seems more likely that n is prime.

Example

$$561 = 3 \cdot 11 \cdot 17 \quad \text{composite}$$

But $\forall a \in \mathbb{Z}$.

$$a^{561} \equiv a \bmod 561$$

So 561 is composite w/ no witnesses.

Defn

A number which is composite but has no witnesses is called a **Carmichael number**.

Theorem (Alford, Granville, Pomerance, 1994)

There are infly many Carmichael numbers.

Need something better than a "Fermat" witness.

Miller-Rabin Test

Prop: Let p be an odd prime. Factor $p-1 = 2^k \cdot m$ for m odd. Then one of the following holds

i) $a^m \equiv 1 \mod p$

or

ii) one of $a^m, a^{2m}, a^{4m}, a^{8m}, \dots, a^{2^{k-1}m}$ is $\equiv -1 \mod p$.

Pf/ Notice $a^{2^k m} = a^{p-1} \equiv 1 \mod p$.

so either $a^m \equiv 1 \mod p$

or $a^{2^i m} \equiv 1 \mod p$ for minimal $i \leq k$.

Then $\left(a^{2^{i-1}m}\right)^2 = 1$

your HW $\Rightarrow a^{2^{i-1}m} = \pm 1$ (HW showed only square roots of 1 mod p)

Minimality of $i \Rightarrow a^{2^{i-1}m} = -1$

Gives me an algorithm:

Given n. Factor $n-1 = 2^k \cdot m$ m odd. pick a

Compute $a^m, a^{2m}, a^{4m}, \dots, a^{2^k m}$

If $a^m \neq 1$ & $a^{2^i m} \neq -1$ $\forall i$

$\Longrightarrow$ n not prime.

Def^n Call such an a a Miller–Rabin witness for compositness of n.

Example $n = 561 \leftarrow$ Carmichael # had no Fermat witnesses.

$\underline{n-1} = 560 = 2^4 \cdot 35$

Compute: $2^{35} \equiv 263 \mod 561$

$2^{2\cdot 35} \equiv 263^2 \equiv 166$ "

$2^{4\cdot 35} \equiv 166^2 \equiv 67$ "

$2^{8\cdot 35} \equiv \underline{67}^2 \equiv 1 \leftarrow$

So $2^m \not\equiv 1$ $2^{2^i m} \not\equiv -1$ so not prime.

If 561 were prime, square roots of 1 are only ± 1.

But we saw 67 is a square root of 1, so not prime!

See 561 had no Fermat witnesses But 2 is a Miller-Rabin witness.

Prop If n is composite, $>75\%$ of $2 \le a \le n-1$ are Miller-Rabin witnesses.