Cryptography

The art of secret communications

$$\text{Alice} \xrightarrow{\text{Message}} \text{Bob}$$

evedrapper

To ensure safety of their messages, A and B can agree on an encryption protocol

$$A \xrightarrow[\text{encrypt}]{M} \hat{M} \xrightarrow[\text{send}]{} \hat{M} \xrightarrow[\text{decrypt}]{} M \quad B$$

Ex: Ceasar's Cipher
M = "PIZZA"

Letters: Numbers mod 26

A	B	...	Z
0	1	...	25

Choose secret key "k"

To encrypt M, add k to "each letter" (mod 26)

ex: k = 7
P = 15 + 7 = 22 W
I = 8 + 7 = 15 P
Z = 25 + 7 = 32 = 6 G
Z = 25 + 7 = 6 G
A = 0 + 7 = 7 H

Decryption: Subtract 7 from each letter (mod 26)

$\Rightarrow$ PIZZA

Ceasar cipher is bad for 2 reasons:

1. Lock exchange problem
A and B have to agree on a secret key k, without sending it on the public channel

2. Key is crackable from the secret message
Ex: Frequency analysis
If the message is in English, the letter "e" appears more frequently than any other letter. The most frequent letter in $\hat{M}$ should be e

$$x = \underset{\substack{\uparrow \\ E}}{4} + k$$

$$k = x - 4 \pmod{26}$$

The RSA protocol

Safer protocol, which resolves these two problems

1. no need to exchange keys.
uses two keys:
- a public one (for encryption)
- a private key (for decryption)

Everyone can send messages to B, which B is the only one who can read them. (Can also be used the other way around, for certification of identity)

2. Secret key is not crackable in practice
To crack it, you need to factorize a very large number, and that's a NP-complete problem

So what is RSA?
Suppose B wants to receive secret messages from everyone

B chooses two large prime numbers p and q (checking if a number is prime is manageable and not NP-complete)

B then chooses a third number k coprime with (p-1)(q-1)

Let $n = pq$

$\Rightarrow$ Public key $= (n, k)$

Send it to everyone!

Then B finds (with Euclid's algorithm, for instance)

Private key : $S = k^{-1} \pmod{(p-1)(q-1)}$

To encrypt a message M, just calculate

$$\hat{M} = M^k \,\%\, n$$

To decrypt, B calculates

$$\hat{M}^S \,\%\, n \underset{\text{theorem}}{=} M$$

Ex: $p = 3$, $q = 11$ $n = pq = 33$

$$(p-1)(q-1) = 20$$

B chooses $k = 7$
check $\gcd(7, 20) = 1$
Send public key $(33, 7)$

Secret key: S = 3
Because 7x3 = 21 $\equiv 1 \pmod{20}$

A wants to send the message $M = 2$
calculates $\hat{M} = 2^7 \% 33$

$$2^7 = 128 = 99 + 29 \equiv 29 \pmod{33}$$

$$\hat{M} = 29$$

When B receives $\hat{M} = 29$
He calculates

$$29^3 \equiv (-4)^3 \equiv -64 = 2 \pmod{33}$$

$$M = 2$$

Why does this work?

Lemma: Let p,q be primes $p \neq q$

Then $a \equiv b \pmod{pq}$

$$\Updownarrow$$

$a \equiv b \pmod p$ and $a \equiv b \pmod q$

Proof

$\boxed{\Downarrow}$ Assume $a \equiv b \pmod{pq}$

$\Rightarrow pq \mid a - b$

Since $p \mid pq$ and $q \mid pq$, by transitivity

$p \mid a-b$ and $q \mid a-b$

$\Rightarrow a \equiv b \pmod p$ and $a \equiv b \pmod q$

$\boxed{\#}$ Assume $p \mid a-b$ and $q \mid a-b$

By fundamental theorem of arithmetic, both p and q must appear (with exponent >= 1) in the prime decomposition of (a-b)

$$(a-b) = p^{\alpha} q^{\beta} m, \quad \alpha, \beta \geq 1$$

Since $pq \mid p^{\alpha} q^{\beta}$, then

$$pq \mid a-b$$

$$a \equiv b \pmod{pq}$$

$\square$

Theorem (RSA works)

$$\hat{M} = M^{k} \pmod{pq} \implies M = \hat{M}^{s} \pmod{pq}$$

where $s = k^{-1} \pmod{(p-1)(q-1)}$

Proof: this is the same as:

$$M \equiv (M^{k})^{s} \pmod{pq}$$

Since $s = k^{-1} \bmod (p-1)(q-1)$

$$\implies sk \equiv 1 \bmod (p-1)(q-1)$$

$$\implies sk = 1 + m(p-1)(q-1)$$

Then $(M^{k})^{s} = M^{sk} \pmod{pq}$

$$= M^{1 + m(p-1)(q-1)} \pmod{pq}$$

$$= M \cdot M^{m(p-1)(q-1)} \pmod{pq}$$

By Lemma:

$$M^{ks} \equiv M \cdot M^{m(p-1)(q-1)} \pmod p$$

$$\equiv M \cdot \left(M^{p-1}\right)^{m(q-1)} \pmod p$$

$$\equiv M \cdot 1^{m(q-1)} \pmod p \quad \text{by FLT}$$

$$\equiv M \pmod p$$

Similarly $M^{ks} \equiv M \pmod q$

by lemma $M^{ks} \equiv M \pmod{pq}$

$\square$