Symmetric / private key encryption

Example: modular shifting

encryption key (k, n)

$m \longrightarrow m + k \bmod n$ encryption $\qquad$ $c \longrightarrow c - k \bmod n$ decryption

Message = "ok"

$m = 1511$ plaintext

key $= (k = 500,\ n = 2000)$

$c = 1511 + 500 \bmod 2000$

$= 11$ ciphertext

transmit over insecure channel

$m = 11 - 500 \bmod 2000$

$= -489 \bmod 2000$

$= 1511$

↑ we get back the message

Note both parties use the same key to encrypt and decrypt.

RSA: an example of asymmetric / public key encryption

RSA uses modular exponentiation.

$m \longrightarrow$ encrypt $\quad m^e \bmod n = c$

$c \longrightarrow$ decrypt $\quad c^d \bmod n = m$

encryption key = (e, n)

decryption key = (d, n) ← they're different!

Question: how do we pick e, d, n?

we want $\quad c^d \bmod n = m$

$(m^e \bmod n)^d \bmod n = m$

$m^{ed} \bmod n = m$

we use

> **Euler's theorem (special case)**
> $m^{(p-1)(q-1)} \bmod pq = 1$
> if $\gcd(m, pq) = 1$ and p, q prime

Clearly we want $\quad n = pq$

$(p-1)(q-1) = "0"$ and $ed = "1"$

formally $\quad ed \equiv 1 \bmod \underbrace{(p-1)(q-1)}_{\varphi}$

Why? ($\equiv$ means)

$ed = 1 + k\varphi$ for some integer k

$m^{ed} = m^{1+k\varphi}$ because $ed \equiv 1 \bmod \varphi$

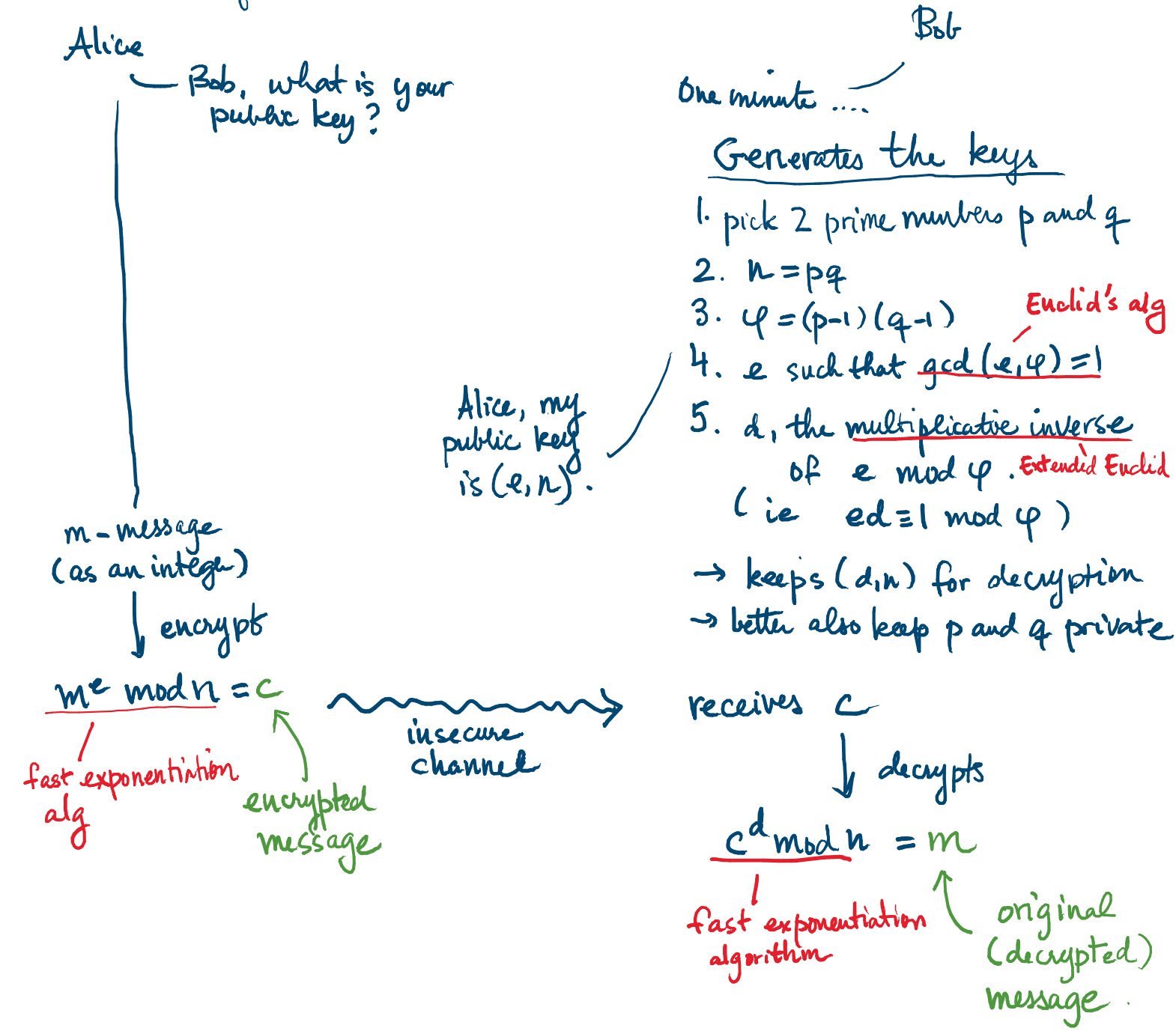
$= m \cdot m^{k\varphi}$

$\equiv m \cdot 1 \bmod n$ by Euler's theorem

$= m \bmod n$

$= m$

Description of RSA



RSA example

Alice

message = "y"

m = 25

encrypt using Bob's public key

$c = 25^{13} \bmod 77$

$25^3 = 71 \bmod 77$

$25^6 = 71^2 = 36 \bmod 77$

$25^{13} = 36^2 \cdot 25 = 60 \bmod 77$

$c = 60$

transmit

Bob

Generates the RSA key pair:

1. $p = 7$ and $q = 11$
2. $n = 77$
3. $\varphi = 6 \cdot 10 = 60$
4. $e = 13$ because $\gcd(13, 60) = 1$
5. d: inverse of $e = 13 \bmod 60$

$(e = 13, n = 77)$

Euclid:

60 13 8 5 3 2 1

$60 = 4 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$1 = 3 - 2$ ↓ write 2 in terms of 3 and 5

$= 3 - (5 - 3)$

$= -5 + 2 \cdot 3$ ↓ write 3 in terms of 5 and 8

$= -5 + 2(8 - 5)$

$= 2 \cdot 8 - 3 \cdot 5$ ↓ 5 in terms of 8 and 13

$= 2 \cdot 8 - 3(13 - 8)$

$= -3 \cdot 13 + 5 \cdot 8$ ↓ 8 in terms of 13 and 60

$= -3 \cdot 13 + 5(60 - 4 \cdot 13)$

$= 5 \cdot 60 - 23 \cdot 13$ ↓ mod 60 on both sides

$1 = 0 - 23 \cdot 13 \bmod 60$

$\Rightarrow d = -23 \bmod 60 = 60 - 23$

$d = 37$

$c = 60$

$m = 60^{37} \bmod 77$

$60^2 = 58 \bmod 77$

$60^4 = 58^2 = 53 \bmod 77$

$60^9 = 53^2 \cdot 60 = 64 \bmod 77$

$60^{18} = 64^2 = 15 \bmod 77$

$60^{37} = 15^2 \cdot 60 = 25 \bmod 77 \Rightarrow m = 25$