Modulo Arithmetic $(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

$(a \times b) \bmod n = (a \bmod n \times b \bmod n) \bmod n.$

$a^x \bmod n = (a \bmod n)^x \bmod n.$

Euler's totient function $\phi(n)$: # of positive integers up to n that are relatively prime to n.

$\phi(p) = (p-1)$ if p is prime

* if p, q are coprime (relatively prime) $\phi(pq) = \phi(p)\phi(q)$
* if p, q are prime; $\boxed{\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)}$

Euler's theorem: a, n are relatively prime

$$\boxed{a^{\phi(n)} \equiv 1 \pmod n} \ *$$

Find $4^{100003} \bmod 33 = ?$

$33 = 3 \times 11$ 3, 11 are prime $\Rightarrow$ coprime.

$\Rightarrow \phi(33) = \phi(3)\phi(11) = 2 \times 10 = 20.$

$$\boxed{4^{20} = 1 \pmod{33}}$$

$100003 = 100000 + 3 = 20 * 5000 + 3$

$4^{100003} = 4^{20 \times 5000 + 3} = \left(4^{20}\right)^{5000} \cdot 4^3$

$\left(4^{20 \cdot 5000} \cdot 4^3\right) \bmod 33 = \left(\underbrace{\left(4^{20}\right)^{5000} \bmod 33}_{= 1}\right)\left(4^3 \bmod 33\right) \bmod 33$

$= 1 \times 4^3 \bmod 33$

$= 2^8 \bmod 33 = 64 \bmod 33 = 31$ □

① How to find gcd(a, b) Euclid's algorithm

② Extended Euclidean Algorithm: find x, y such that

$$ax + by = \gcd(a,b) \qquad x, y \text{ integers.}$$

Special case a, b are coprime $\Rightarrow$ $ax + by = 1$

$$ax + by = 1$$

take (mod b)

$$(ax + by) \bmod b = 1 \bmod b$$

$$((ax \bmod b) + (by \bmod b)) \bmod b = 1$$

($by \bmod b = 0$)

$$ax \bmod b = 1$$

$$ax = 1 \pmod b$$

x is the inverse of a mod b

So a : public key

x : private key

RSA algorithm:

Ⅰ Key generation

① Choose p, q large prime numbers

Compute $n = p \cdot q$ ✓

n → public

Assumption: Given n, finding p and q is hard.

- $\phi(pq) = \phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$ ✓

- $\phi(pq) = \phi(n) = \phi(p)\,\phi(q) = (p-1)(q-1)$

② Generate exponent e such that $e, \phi(n)$ are co-prime

typical value for $\boxed{e = 65537}$

Use extended Euclide's algorithm to find d

s.t. $\boxed{e.d \equiv 1 \mod \phi(n)} \Rightarrow \boxed{e.d = k\phi(n) + 1}$

So (e, n) public key

d private key

encryption M s.t. $M < n$ $\quad \boxed{M^e \mod n = C}$ → cypher text C

Decryption : Given C, $\boxed{C^d \mod n \equiv M}$

why? $C^d \mod n = (M^e \mod n)^d \mod n$

$= M^{ed} \mod n$

$= M^{k\phi(n)+1} \mod n$

$= \left(\left(M^{\phi(n)}\right)^k . M\right) \mod n$

$= \left(\underbrace{M^{\phi(n)} \mod n}_{\equiv 1}\right)^k . (M \mod n) \mod n$

$= 1 \times M \mod n = M$ □

Implications of exponentiation are that RSA is much slower than other symmetric-key cryptography algorithms

---

Application of PKC:

① Digital Signatures:

① Digital Signatures:

m sign the message w/ private key

publish m, s(m), public key to the other end

Only public key can regenerate m from s(m).

In RSA: Generate private key & sign using d

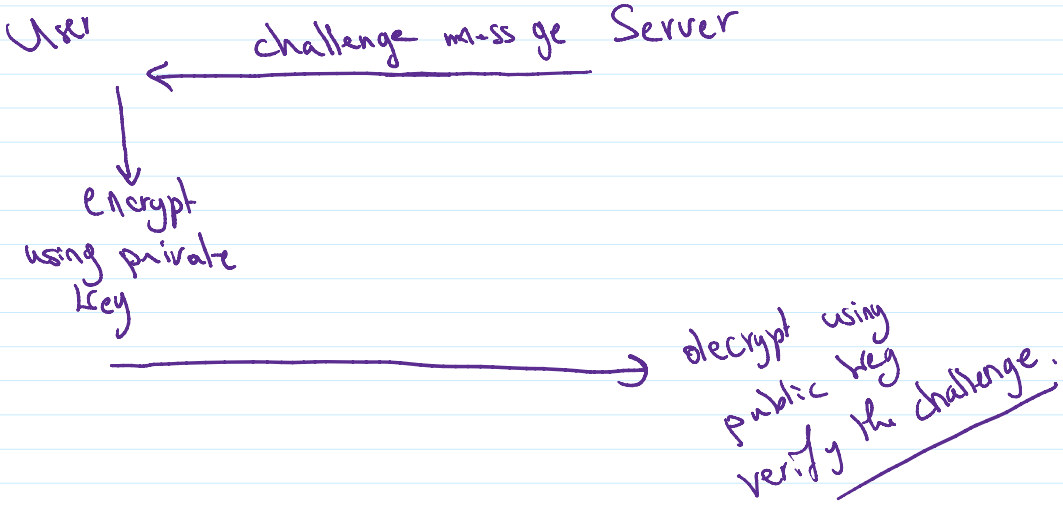
& verify signature using e, n public key.

In practice, we sign a hash of m

m $\xrightarrow{\text{SHA-256}}$ (256-bit hash) $\xrightarrow[\text{using d}]{\text{Sign}}$ signature.

② HTTPS, SSL/TLS

③ Authentication



④ Credit Card Authentication.