Information security

Plain text → P Cipher text → C

Encryption (E) $C = E(P, K) = E_K(P)$

Decryption (D) $P = D(C, K) = D_K(C)$

⇒ Cryptography

1) Symmetric / Private key cryptography

RC4, DES (Data encryption standard), AES (advanced encryption standard)

2) Assymmetric / Public key cryptography

RSA, EL-Gamal, Elliptic Curve Cryptography (ECC)

RSA (Rivest, Shamir, Adleman)

Both sender & receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus this is public key encryption algorithm with public key of $PU = \{e, n\}$ and private key of $PU = \{d, n\}$.

* receiver generate both key and send public key to sender.

Key Generation

Input : Security parameter l

Output : RSA public key (n, e) & private key d

1. Randomly select 2 primes p & q of same bitlength $l/2$
2. Compute $n = pq$ and $\phi = (p-1)(q-1)$
3. Select an arbitrary integer e with $1 < e < \phi$ and $\gcd(e, \phi) = 1$
4. Compute integer d satisfying $1 < d < \phi$ and $ed \equiv 1 \bmod \phi(n)$
5. Return (n, e, d)

RSA encryption

Input : public key (n, e), plaintext $m \in [0, n-1]$

Output : ciphertext c.

1. Compute $c \equiv m^e \bmod n$
2. return c

RSA decryption

Input : Public key (n, e), private key d, ciphertext c

output : plaintext m

1. Compute $m = c^d \bmod n$
2. return (m)

eg Key generation

1) $p = 61 \quad q = 53$

2) $n = pq = 3233$

$\phi(n) = \phi(p)\,\phi(q)$

$= (61-1)(53-1)$

$= 3120$

choose e : $1 \le e \le \phi(n)$

Coprime to $\phi(n)$

17

Key $(e, n) = (17, 3233)$

) d s.t. $e = 1 \bmod 3120$

2753

pubb $(d, n) = (2753, 3120)$

Way to find d

$d = 17 \bmod 3120$

$3120 = 17(183) + 9$

$17 = 9(1) + 8$

$9 = 8(1) + 1$

$1 = 9 - 8(1)$

$= 9 - (17 - 9.1)1$

$= 2 \times 9 - 17$

$= 2(3120 - 17 \times 183) - 17$

$= 2 \times 3120 - 367 \times 17$

so -367 or $3120 - 367$

$= 2753.$

ElGamal Algorithm

this public key cryptosystem is based on the difficulty of finding discrete logarithm in a cyclic group that is even if we know g^a & g^k, it is extremely difficult to calculate g^{ak}.

easy version

Key Generation :

1) Select large prime no (p) $p=11$
2) Select decryption key / Private key (D) $D=3$
3) Select second part of encryption key or public key (E_1) $e_1=2$.
4) Calculate third part of encryption key or public key (E_2)
   $E_2 = E_1^d \bmod P$ $\quad E_2 = 8$
5) public key $=(E_1, E_2, P)$, Private key $=D$
   $\Rightarrow (2, 8, 11)$ $\quad \hookrightarrow 3$

in next algo e_2 = public key
D = private key

Encryption:

$PT = 7$
PT → Plain text)

1) Select random integer (R) $\Rightarrow 4$
2) $C_1 = E_1^R \bmod P$ $\quad C_1 = 2^4 \bmod 11 = 5$
3) $C_2 = (PT \times e_2^R) \bmod P$ $\quad = (7 \times 8^4) \bmod$
   $= 6$
4) $C_T = (C_1, C_2)$

Decryption:

$PT = [C_2 \times (C_1^D)^{-1}] \bmod P$

$P=11$ $\quad C_2=6$ $\quad C_1=5$ $\quad D=3$

$PT = (6 \times (5^3)^{-1}) \bmod 11$

$= [(6 \bmod 11) \times (125^{-1} \bmod 11)]_{mod}$

$= (6 \times 3) \bmod 11$

$PT = 7$

Algorithm

1) DL Domain parameter generation

Input : Security parameters l, t

Output : DL domain parameter (p, q, g)

1) Select t-bit prime q & l bit prime p such that q devides $p-1$
2) select an element g of order q
   2.1 Select arbitrary $h \in [1, p-1]$ and compute $g = h^{(p-1)/q} \bmod p$
   2.2 if $g = 1$ go to step 2.1
3) Return (p, q, g)

2) DL key pair generation

Input : DL domain parameters (p, q, g)

Output : Public key y and private key x

1. Select $x \in_R [1, q-1]$
2. Compute $y = g^x \bmod p$
3. Return (y, x)

3) El Gamal Encryption

Input: DL domain parameters (p, q, g)
public key y, plaintext $m \in [0, p-1]$

Output: Ciphertext (c_1, c_2)

1. Select $k \in_R [1, q-1]$
2. Compute $c_1 = g^k \bmod p$
3. Compute $c_2 = m \cdot y^k \bmod p$
4. Return (c_1, c_2)

El Gamal Decryption

Input: DL domain parameter (p, q, g), private key x, Ciphertext (c_1, c_2)

Output: Plaintext m

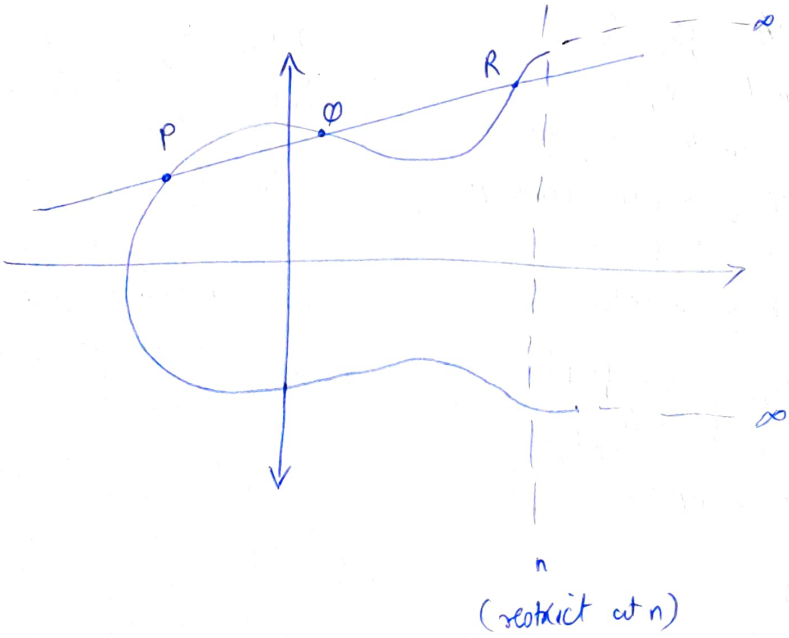
1) Compute $m = c_2 \cdot c_1^{-x} \bmod p$
2) Return m

ECC (Elliptical Curve Cryptography)

→ It is asymetric / public key cryptography
→ It provides equal security with smaller key size (as compared to RSA)
→ Uses elliptical curves
→ Elliptical curves are defined by some mathematical cubic fn's

eg $[y^2 = x^3 + ax + b]$ a, b constant, eqⁿ of degree 3

→ Symmetric to x-axis
→ If we draw a line, it will touch a max of 3 points



(restrict at n)

Let $E_p(a,b)$ be a elliptical curve $\quad E_p(ab) \rightarrow y^2 \equiv x^3 + ax + b \pmod p$

Consider eqn $\boxed{Q = kP}$

where $Q, P \rightarrow$ points on curve & $k < n$

- If k & $P \rightarrow$ given, it should be easy to find Q

but if we know P and Q, it is extremely difficult to find k.

ECC Key Exchange

Global Public Elements

$E_q(a,b)$ elliptical curve with parameters a, b & q. where q is a prime or an integer of fooorm 2^m

G point of elliptical curve whose order is larger than n.

User A key Generation

Select private key n_A $\quad n_A < n$

Calculate public key P_A $\quad P_A = n_A \times G$

User B key Generation

Select private key n_B $\quad n_B < n$

Calculate public key P_B $\quad P_B = n_B \times G$

Calculation of secret key by A

$K = n_A \times P_B$

Calculation of secret key by B

$K = n_B \times P_A$

Let $E_p(a,b)$ be a elliptical curve $\quad E_p(a,b) \Rightarrow y^2 \equiv x^3 + ax + b \pmod p$

Consider eqn $\boxed{Q = kP}$

where $Q, P \rightarrow$ points on curve & $k < n$

- If k & $P \rightarrow$ given, it should be easy to find Q

but if we know P and Q, it is extremely difficult to find k.

ECC Key Exchange

Global Public Elements

$E_q(a,b)$ elliptical curve with parameters a, b & q. where q is a prime or an integer of fooom 2^m

G point of elliptical curve whose order is larger than n.

User A key Generation

Select private key n_A $\quad n_A < n$

Calculate public key P_A $\quad P_A = n_A \times G$

User B key Generation

Select private key n_B $\quad n_B < n$

Calculate public key P_B $\quad P_B = n_B \times G$

Calculation of secret key by A

$K = n_A \times P_B$

Calculation of secret key by B

$K = n_B \times P_A$

ECC encryption

- Let the message be M
  First encode this message M into point on elliptic curve
  Let this point be P_m
  ↓
  now this point is encrypted.

for encryption chose a random positive integer k

Cipher point will be

$$C_m = \{kG, P_m + kP_B\}$$ → for encryption public key of B used

This point will be sent to receiver

ECC decryption

for decryption, multiply 1st point in pair with receiver's secret key.

ie $kG * n_B$ // for decryption private key of B used

Then subtract it from 2nd point / coordinate in pair

ie $P_m + kP_B - (kG * n_B)$

But we know $P_B = n_B \times G$

so

$= P_m + kP_B - kP_B$

$= P_m$

~ original point

→ So receiver get the same point

Finding points on elliptical curve

$y^2 = x^3 + ax + b$.

means $E_{11}(1, 6)$

$y^2 \equiv x^3 + x + 6 \pmod{11}$

$a = 1 \quad b = 6$

11 → mod 11

x	RHS $x^3+x+6 \pmod{11}$
0	6
1	8
2	5
3	3
4	8
5	4
6	8
7	4
8	9
9	7
10	4

(for mod 11 so less than 11)

y	LHS $y^2 \pmod{11}$ (n value)
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

match RHS with LHS.

Points on curve

(2, 4) (2, 7)
(3, 5) (3, 6)
(5, 2) (5, 9)
(7, 2) (7, 9)
(8, 3) (8, 8)
(10, 2) (10, 9)

find $P+Q$ & $2P$

$P(x_1, y_1)$ $Q(x_2, y_2)$

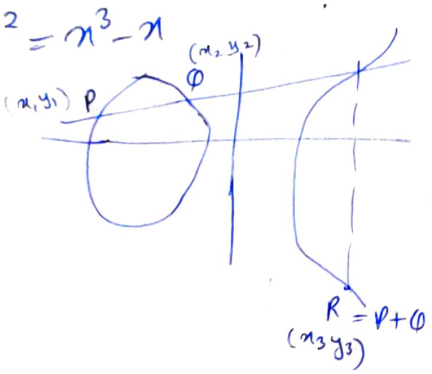
$P+Q \Rightarrow x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$ ($\frac{y_2-y_1}{x_2-x_1} = m$)

$y_3 = -y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3)$

$2P \Rightarrow Q = P$

$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1$ $\quad y_3 = -y_1 + \left(\frac{3x_1^2+a}{2y_1}\right)(x_1 - x_3)$

eg $y^2 = x^3 - x$



Q. $y^2 = x^3 - 36x$ $\quad P = (-3, 9)$ $\quad Q = (-2, 8)$

so $a = -36$

- $x_3 = \left(\frac{8-9}{-2+3}\right)^2 - (-3) - (-2) = 6$

  $y_3 = -9 + \left(\frac{8-9}{-2+3}\right)(-3-6) = 0$

  $P+Q = (6, 0)$

- for $2P$ $\quad x_3 = \left(\frac{3(-3)^2 + (-36)}{2 \times 9}\right) - 2(-3)$

  $= 25/4$

  $y_3 = -35/8$

Q. $E_{23}(1,1)$

So curve is $y^2 = x^3 + x + 1 \pmod{23}$

so points allowed 0, 1, ... 22 only integers.

1) $P = (13, 7)$ so $-P$?

$-P = (x, -y) = (13, -7)$ but mod 23 so $(13, 23-7) \Rightarrow -P = (13, 16)$

2) $R = P+Q$

$P = (3, 10)$

$Q = (9, 7)$

$x_3 = \left(\frac{7-10}{9-3}\right)^2 - 3 - 9$

$= 1/4 + 11$

$= 1 \times (4^{-1}) + 11$

$= 1 \times 6 + 11$

$= 17$

$-10 = 23 - 10 = 13$

$y_3 = -10 + \left(\frac{7-10}{9-3}\right)(3-17)$

$= -13 + \left(\frac{-1}{2}\right)(-14)^7$

$= 13 + 7 = 20$

if kept -10

so $-10 + 7 = -3 \pmod{23}$

$= 20$ ✓

for Binary field F_{2^m}

$P+Q$:

$$m = \frac{y_1 \oplus y_2}{x_1 \oplus x_2}$$

$$x_3 = m^2 \oplus m \oplus x_1 \oplus x_2 \oplus a$$

$$y_3 = m(x_1 \oplus x_3) \oplus y_1 \oplus x_3$$

$P+P$:

$$m = x_1 \oplus \frac{y_1}{x_1}$$

$$x_3 = m^2 \oplus m \oplus a$$

$$y_3 = x_1^2 \oplus m x_3 \oplus x_3$$

Legendry

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$$

p → Prime

1) $\left(\frac{a^2}{p}\right) = 1$

2) $\frac{2}{p} = (-1)^{\frac{p^2-1}{8}}$

3) $\frac{p}{q} = \frac{q}{p}(-1)^{\frac{(p-1)(q-1)}{4}}$

4) $\frac{ab}{p} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

5) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

- $\left(\frac{154}{173}\right) = (-1)^{\frac{173^2-1}{8}}\left(\frac{77}{173}\right)$ niche chota rakho, formula ② $= -\left(\frac{77}{173}\right)$

formula ③ $\Rightarrow -\left(\frac{173}{77}\right)(-1)^{\frac{(77-1)(173-1)}{4}}$ (1)

$\Rightarrow \frac{-173}{77}$

formula 5 $\quad a = 173 \bmod 77 \quad a = 19$

so $= -\frac{19}{77}$

formula 3 $= -\frac{77}{19}$

formula 5 $\quad 77 \bmod 19 = 1$

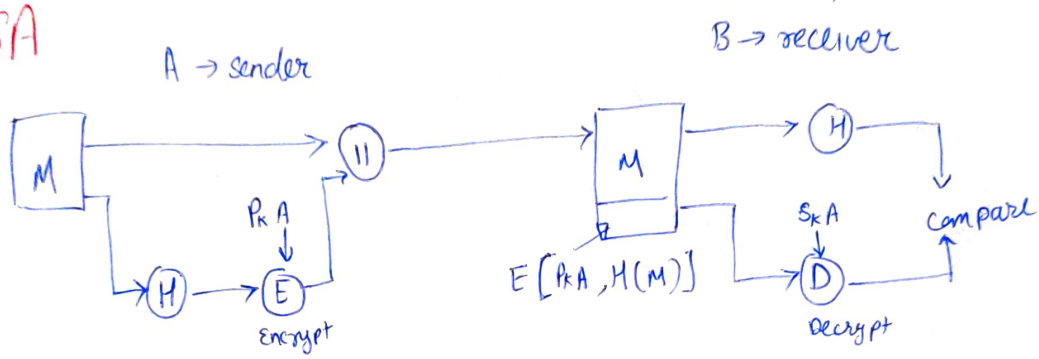
So $\frac{-1}{19} \rightarrow \frac{a^2}{p}$ form

$= -1$ ✓

Digital Signature

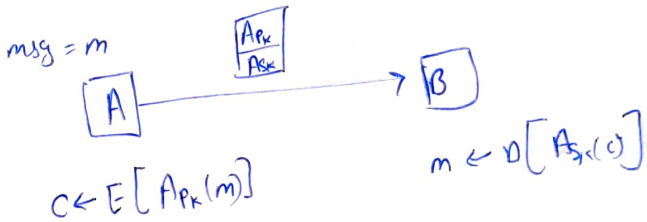
A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with creator's private key. The signature guarantees the source and integrity of message.

1) RSA



Key Pair (S_k P_k)

Secret key — Public key



Signer → Signs document using S_k & P_k

verifier → verify document using P_k

Signer

$\sigma \leftarrow h^{SK} \bmod n$

σ is signature

$h \leftarrow H(m)$ (m: message; H: hash fn)

hash message

H is one way fn

verifier (has m, σ, P_k of sender)

1) $h \leftarrow H(m)$
2) $h' \leftarrow \sigma^{P_k} \bmod n$
3) $h = h'$ valid, else invalid

has message & digital signature σ.

RSA is secure because we know 'n', but not the values of p & q.

2) El-Gamal digital Signature

Elgamal is secure because of discrete logarithm problem

$y = g^x \bmod p$ — unknown x

$x \rightarrow$ private key

$y \rightarrow$ public key

Gen $\leftarrow (x, y)$ $\quad y = g^x \bmod p$

$x \downarrow$ SK, $y \downarrow$ PK

Sign (x, m)

T → mod p

all mod q

1) $k \in_R [1, q-1]$
2) $T = g^k \bmod p$
3) $h \leftarrow H(m)$
4) $r = T \bmod q$ if $r=0$ goto step 1
5) $S = k^{-1}(h + xr) \bmod q$

if $S=0$ goto step 1

(r, s) signature

Verify

1) if not, $0 < r < s < q-1$ not valid
2) $h = H(m)$
3) $w = s^{-1} \bmod q$
4) $u_1 = hw \bmod q$ and $u_2 = rw \bmod q$
5) $T = g^{u_1} y^{u_2} \bmod p$

$y \rightarrow$ PK signer

6) $r' = T \bmod q$
7) if $r = r'$ valid

else not valid

Proof of Correctness

$s = k^{-1}(h + xr)$

$w = s^{-1} \bmod q$

$= (k^{-1}(h + xr))^{-1} \bmod q = (h + xr)^{-1} k \bmod q$

$u_1 = h(h + xr)^{-1} k \bmod q \qquad u_2 = r(h + xr)^{-1} k \bmod q$

$T = g^{h(h + xr)^{-1} k \bmod q} \cdot y^{r(h + xr)^{-1} k \bmod q} \bmod p$

remove mod q & $y = g^x \bmod p$

$T = \left(g^{h(h + xr)^{-1} k} \cdot g^{rx(h + xr)^{-1} k}\right) \bmod p$

$T = (g^k \bmod p)$

Same as we took of signer

T = timestamp

Digital Signature using ECC

(A) ——— E(a,b) ———→ (B)

$y^2 = x^3 + ax + b \in F_q$ q is prime

$E(F_q) = \{ (x,y) \in F_q \times F_q \} \cup \{O\}$

$E(F_q) = \langle P \rangle = n$ $nP = O$

brackets means generator

Signature generation

1) chose $k \in_R [1, n-1]$
2) $R = kP$
3) $r = X(R)$ # take only x coordinate of signature
4) $S = k^{-1}(H(m) + dr)$ → d is secret key of signer

Signature $= (r, S)$

$n \rightarrow$ no. of points generated by curve over field F_q

verify

1) $w = S^{-1} \bmod n$
2) $u = H(m)\, w \bmod n$
3) $v = rw \bmod n$
4) $R = uP + vQ$
5) $r = X(R)$ valid
   else not valid

$Q \rightarrow$ public key of signer
$Q = dP$

Defman Algorithm

Bilinear Defman Algo $\{\hat{e}, G_1, G_2, G_T\}$ → group under multiplication

G_1, G_2 → additive group of prime order

$P_1, P_2 \in G_1$

$Q_1, Q_2 \in G_2$

bilinear mapping $\hat{e} : G_1 \times G_2 \to G_T$

$|G_1| = |G_2| = |G_T| = q$ = prime

Note

* consider it as $e(P,Q) = e^{PQ}$

① $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q_1) \cdot \hat{e}(P_2, Q_1)$

② $\hat{e}(P, Q_1 + Q_2) = \hat{e}(P, Q_1) \cdot \hat{e}(P, Q_2)$

③ $\hat{e}(O, Q) = \hat{e}(P, O) = 1$

④ $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} = \hat{e}(bP, aQ) = \hat{e}(P, abQ)$

⑤ $\hat{e}(-P, Q) = \hat{e}(P, Q)^{-1} = \hat{e}(P, -Q)$

⑥ $\hat{e}(P, Q) \neq 1$, $P = Q \neq O$

eg $x \in G_1$ $y \in G_2$ $\hat{e}(x,y) = 3^{xy}$ on Z_{11}^*

do all this with mod 11

$\hat{e}(0,y) = 3^0 = 1$

$\hat{e}(x,0) = 3^0 = 1$

$\hat{e}(1,1) = 3$

$\hat{e}(1,3) = 27 \bmod 11 = 5$

$\hat{e}(1,2) = 9$

$\hat{e}(2,1) = \hat{e}(1,1) \cdot \hat{e}(1,1) = 9$

digital Signature

Sign

$G_1 = G_2 = \langle P \rangle$

$a \in [1, n-1]$ ← secret key of Signer

$aP = A$ ← public key

$M = H(m)$ $M \in E(F_p)$

$S = aM$

So verifier has (P, A, S, M)

- P → base point
- A → public key Signer
- S → signature
- M → hash message

verify

$\hat{e}(P,S) = \hat{e}(A,M)$

$\hat{e}(P,S) = \hat{e}(A, aM)$

$= \hat{e}(aP, M)^a$

$= \hat{e}(aP, aM)$

$= \hat{e}(P, S)$

if $\hat{e}(P,S) = \hat{e}(A,M)$ then valid else invalid

* for Batch : if any 1 signature is wrong reject all

Security Goals : CIAEN

1) Confidentiality : it measures protection of information from unauthorized access & misuse

2) Integrity : Integrity measures protect information from unauthorized alteration

3) Availability : In order for an information system to be useful it must be available to authorized users.

4) Entity authentication : Corroborating identity of an entity - B should be convinced of identity of other communicating entity.

5) Non - repudiation : Preventing an entity from denying previous commitments or actions.

⇒ Digital signature does not provide confidentiality.

999

1) Divisibility

Let $a, b \in Z$

a devides b $\Rightarrow$ $a \mid b$

2) Division theorem

$a, b \in Z \quad a \nmid b$

$b = aq + r$

3) GCD

let $a, b \in N$

$d \Rightarrow d \mid a$ & $d \mid b$

& d is highest possible value

So d is $gcd(a, b)$

$gcd(a, b) = 1$ (coprime)

4) Fundamental theorem of arithmetic

every no. can be represented as product of primes.

$LCM(a, b) * gcd(a, b) = a * b$.

Euclidean Algorithm

$$\begin{cases} Gcd(a, b) = gcd(b, a \% b) \\ Gcd(a, 0) = a \end{cases}$$

Extended Euclidean Algorithm

It finds integer coefficients x & y such that

$ax + by = gcd(a, b)$

Congruence ($\equiv$)

$a \equiv b \bmod m \quad \Rightarrow m \mid a - b$

a is congruent to b modulus m

$a \equiv b (m)$

if $a \equiv b \bmod n$

$b = a + nq$

a & b leaves same remainder when devided by n.

$\rightarrow a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$

symetric

* Congruence is equivalence relation.

Euler totient function $\phi(n)$

$\phi(n)$ - no. of +ve integers less than n that are relatively prime to n

$\phi(5) = 1, 2, 3, 4$

$= 4$

finding ϕ (values)

1) if n is prime n0
$\phi(n) = (n-1)$

2) if $n = p \times q$
p, q → prime
$\phi(n) = (p-1) \times (q-1)$

3) $n = a \times b$ atleast one of a, b is composite

$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) - - - -$

where p_1, p_2 -- are distinct primes.

• Fermat's little theorem

p → prime $a \geq 0$ not divisible by 'p'

$a^{p-1} \equiv 1 \pmod p$

• Chinese Remainder Theorem

$X = a_1 \pmod{m_1}$ $X = a_2 \pmod{m_2}$

$X = an \pmod{m_n}$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + - - a_n M_n M_n^{-1}) \bmod M$

$M = m_1 \times m_2 \times m_3 - - - \times m_n$

$M_1 = M / m_1$

$M_1 M_1^{-1} = 1 \pmod{m_1}$

Test for primality

1) Fermat's test

Test
if p is prime
$a^p - a$ → 'p' is prime if this is multiple of 'p' for all $1 \leq a < p$.

Miller Rabin primality test

Step 1 : find $n-1 = 2^k \times m$

Step 2 = chose a such that
$1 < a < n-1$

Step 3; compute
$b_0 = a^m \pmod n$
$b_1 = b_0^2 \pmod n$
$b_2 = b_1^2 \pmod n$
$b_i = b_{i-1}^2 \pmod n$

+1 → Composite
−1 → probably prime.

Wilson Method

p is prime if & only if
$(p-1)! = -1 \bmod p$
or $(p-1)! = (p-1) \bmod p$.

---

mod using Cal.
eg 263 (mod14) so
263 ÷ 14 → 18. ~~
263 − 18 × 14 = 11
ans.