Cryptography → Study of Encrypting

Cryptanalysis → Study of Decrypting

Cryptology → Encrypting + Decrypting.

Greek word → "Hidden, Secret"

Cryptography → Study or to write

Art of writing or Solving code

Varing aspects in Security

Authenticating

Process of recognizing User's Identity

Confidentiality

Data integrity

Is the assurance that digital info is Uncorrupted & can only be accessed or modified by

Non-Repudiating

Someone can't deny validity of

Authorization :- Security Mechanism to determine access levels or User/Client privileges related to system resource

Files Service Computer programs Data Applications Features

CHAPTER-6

Public key Cryptography And Discrete Algorithms.

Cryptography

↳ Is Associated with the process of converting

Ordinary Text → Unintelligible Text

Or vice a versa.

OR Converts data into Unreadable Form

↓

For unauthorized user.

Allowing it to be transmitted without unauthorized entities decoding it into Readable Format.

Also known as Cipher System ⟵ Cryptosystem ⟶ Is a structure consisting of set of algorithms

That converts,

P.T → C.T

Plaintext Ciphertext

To encode or decode message securely.

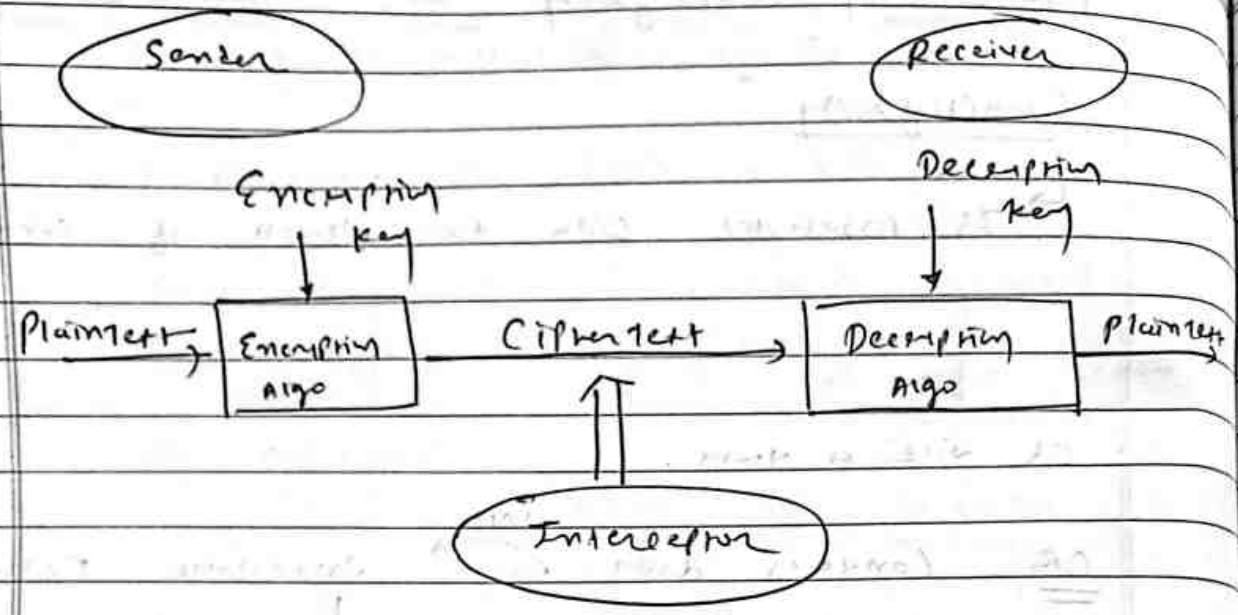
Symmetric key

Same keys are used for encryption & decryption

Asymmetric key

Different keys are used for Encryption & Decryption.

the something unauthorized user



(Model of crypto system)

↳ The model provides Confidentiality to the information being transmitter.

⟹ The model shows that

↳ sender wants to Transfer Receiver

Sensitive Info

↳ In such a way that any party intercepting or eavesdropping on the communication channel can not extract the data.

Confidentiality :- The objective is to ensure that private information remains Private & can be accessed by authorized Users only.

classmate
Date
Page

Components of a Cryptosystem

(1) **Plain Text** :- It is the data to be protected during transmission.

(2) **Encryption Algorithm** :- It is a mathematical process that produces → Cipher Text for any given Plain Text. & Encryption key

Cryptographic Algo

Plain Text + Encryption key → Cipher Text

(3) **Cipher Text** :- It is the scrambled version of Plain text → produced by → Plain Text + Encryption key

→ Not guarded.
→ Flows on public channel
→ Can be intercepted who have access to the Channel

(4) **Decryption Algorithm** :- Mathematical process that produced Plain Text. for given & Decryption key → Cipher Text.

Cryptography → Takes | Cipher Text | + | Decryption key |

Algo

As Input

↓

| Plaintext | (output)

5) Encryption Key

↳ Value which is known to the sender

→ sender inputs encryption key & plain text in order to produce → Cipher Text.

6) Decryption Key

→ Value which is known to the Receiver

Symmetric key Encryption

↓

Same keys → Encryption

↘ Decryption

→ Study of Symmetric Cryptosystems

↓

Reference to es

| Symmetric Cryptography |

Examples : → DES

↓ ↘ 3DES

→ AES.

CHALLENGES OF SYMMETRIC KEY CRYPTOSYSTEM

(1) Key establishment :- Before any communication → Sender, Receiver → Needs to agree on Common Secret key.

(2) Trust Issues :- As Sender & Receiver share same symmetric key → there is an implicit requirement of Trust

Sender — Receiver

↳ It may happen that he/she lost key to an attacker & Sender is not informed

Because of these two challenges.

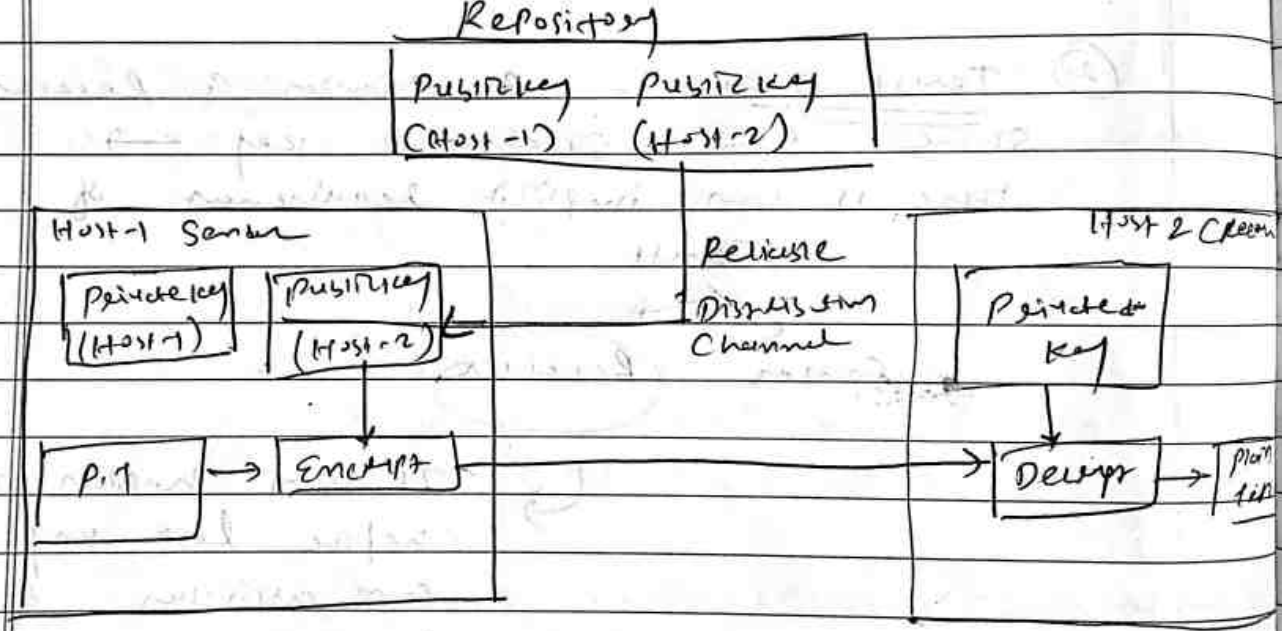
Gave rise to

Asymmetric key Encryption

A- Symmetric Key Encrypting

↳ The encrypting process where different keys are used for encrypting & decrypting the information.

→ Though keys are different → They are mathematically related & hence, retrieving the plaintext by decrypting ciphertext is possible



⇒ Every user in the system needs to have a pair of dissimilar keys.

Private Key Public Key

These keys are mathematically related - when

one key is used for encrypting

other can decrypt the cipher text back to the original text.

→ Public key → put in Public Repository

Private key → well guarded secret

Hence this scheme of encryption is called public key encryption

→ Though → Public, private key } are related

↳ computationally not feasible to find one from other.

↓

Strength of scheme

Host-1 sends data Host-2

Takes Public key of Host 2 | Encrypts it

↳ Uses its Private key

↓

Extract plaintext

Length of Keys (Number of bits) is

large → so process of encryption decryption is → slower than symmetric key encryption.

→ Processing power → ↑ higher

↳ To run Asymmetric Algo.

How can the → Encryption key & Decryption key } are related

& yet it is impossible to determine decryption key from encryption.

↳ Answer is Mathematical concept

⇓

It is possible to design cryptosystem whose keys have this property.

Challenges of Public Key Cryptosystem

(1) User needs to trust that the public key that he is using in communication ↳ with a person really is the public key of the person & has not been spoofed by a malicious third party.

Key distribution → Accomplished by
Trusted Third Party

↓

It is the responsibility of trusted Third Party → to provide Public key
Unique correct.

(Digitally signed by trusted third party).

(4) Rabin Cryptosystem

⇒ Public key Cryptosystem → Invented by Michael Rabin.

⇒ It uses Asymmetric key encryption.

↓

For communication between → Sender
Receiver

⇒ Use of two keys → Public key
Private key

(Prime Numbers → That have exactly two factors → themselves & 1. (e.g 2, 3, 5, 7, 11, 13, 17...)

(Rivest, Shamir, & Adleman).

① RSA Cryptosystem

- Public key algorithm
  - Key-1 → Encrypting (Public key)
  - Key-2 → Decrypting (Private key)

→ Encryption & decryption use modular exponentiation.

↳ exponentiation performed over a modulus.

↳ Modular exponentiation is the remainder when integer b is raised to the power e (the exponent) & divided by a positive integer m (the modulus).

that is → $c = b^e \bmod m$.

$(0 \leq c \leq m)$

Algorithm

i) Choose two large Prime no. P & Q. such that $P \neq Q$

ii) calculate $N \leftarrow P \times Q$.

iii) Choose E (Public key) such that E is not factor of $(P-1)(Q-1)$

(RSA → is a block cipher in which the plaintext & ciphertext are the integers b/w 0 & n-1 for some n.

iv) Choose D (Private key) such that (D x E) mod (p-1)(q-1) = 1 (Multiplicative inverse)

v)

vi) Cipher Text (C.T) = (P.T)^E mod N

vii) Plain Text (P.T) = (C.T)^D mod N.

eg Two users

A B.

A ⟶ B

(S)

↳ wants to send this by encrypting.

→ A & B ~~use~~ decides to use → RSA.

Assume P & Q (Two prime numbers)

↳ selected large if implemented in system

Relatively small (for manual calculation)

① P = 7, Q = 11

② N = 7 x 11 → 77

③ Sender (A) needs to choose Public key (E)

→ such that E is not factor of

$(p-1)(q-1) \rightarrow (7-1)(11-1) = 6 \times 10 = 60.$

Assume $e = 13$ (Public key)

iv) Choose D (Private key) such that

$(D \times e) \bmod (p-1)(q-1) = 1$

$(D \times 13) \bmod 60 = 1$

↳ can be found with multiplicative Inverse Property.

$D = 37$

v) $C = (T)^{13} \bmod 77$

$C = 26$

↳ A will send it to B

vi) $P = (26)^{37} \bmod 77$

$= 5.$

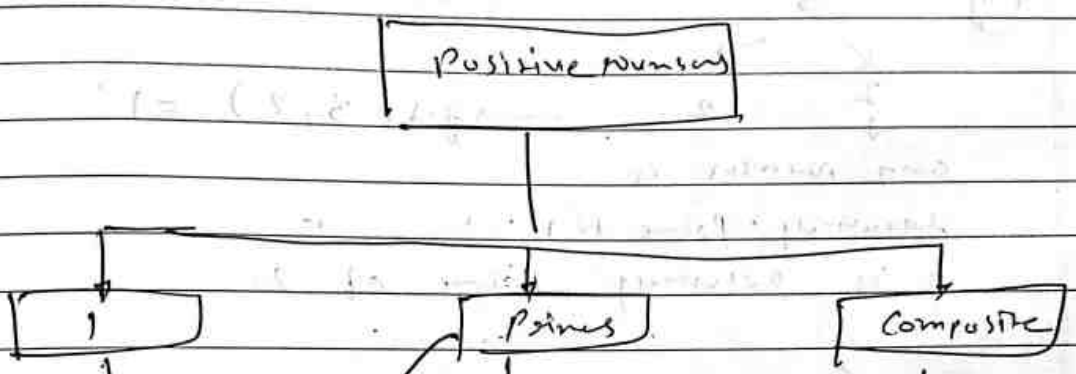
Lec-2

classmate
Date
Page

Mathematics of Symmetric key Cryptography (Video-1)

Multiplicative Inverse

⇒ Primes → are used extensively in → Public key cryptography.



Exactly one divisor

Exactly two divisors

more than two divisors.

A positive integer is a Prime if & only if it has exactly two divisors. i.e 1 & itself

A composite is a positive integer with more than two divisors.

⇒ Smallest prime is 2.

⇒ Coprime :- two positive integers, a & b are relatively prime or coprime, if

gcd (a,b) = 1

1 is Relatively Prime to any integer.

∴ If p is prime number, then all integers "1 to p-1" are relatively prime to "p"

eg 3

1 → any Number is Relatively Prime to 1.

2 → gcd(3,2) = 1

3 is Relatively Prime of 2.

6

1 2 3 5 → Relatively Prime

R.P.: Not relatively Prime → gcd (6,2) ≠ 1

gcd (6,3) ≠ 1

gcd (6,5) = 1

7 → Prime number

1 2 3 4 5 6.

↳ Relatively prime with all Numbers from 1 to 6

i.e if p is prime → 7

p is Relatively Prime to R.P

eg.

Checking for primeness (How to check number is prime or not).

Is 97 is prime?

↳ Check the square root of 97.

$\lfloor \sqrt{97} \rfloor \longrightarrow 9.84... \downarrow$

↳ Ceiling.

9.

Now check 9 is divisible by any prime number < 9 or not.

2, 3, 5, 7 → so 97 is not divisible by any of the prime number lesser than 9.

so 97 is prime.

301 is prime or not.

$\lfloor \sqrt{301} \rfloor = 17.3. = 17.$

Prime Number less than → 3, 5, 7, 11, 13

7 → so it is.

301 is divisible by prime number.

So 301 is prime number

Euler's Phi. function ($\phi(n)$)

or

Euler's totient function

↳ → The function finds the numbers of integers that are both smaller than "n" & relatively prime to "n".

→ The $\phi(n)$ calculates the number of elements in Z_n^*.

↳ (set of relatively prime numbers)

e.g. $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

↳ Z_n^*

$Z_6^* = \{1, 5\}$.

Steps - to find Euler's totient function

(1) $\phi(1) = 0$

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

$\phi(n) = (n-1)$ e.g.

(3) $\phi(m*n) = \phi(m) \times \phi(n)$, if m & n are relatively prime.

$\phi(15) = \phi(5 \times 3)$

$= \phi(5) \times \phi(3)$

$= 2 \times 4$

$= 8$

(4) $\phi(p^e) = p^e - p^{e-1}$

$\phi(16) = \phi(2^4)$

$= 2^4 - 2^{4-1}$

$= 16 - 8$

$= 8$

Exercise

(1) $\phi(15) = \phi(3-1) = 12.$

(2) $\phi(10) = \phi(2 \times 5)$

$= \phi(2) \times \phi(5)$

$= (2-1) \times (5-1)$

$= 1 \times 4$

$= 4$

(3) $\phi(240) =$

2	240

$\phi(2^4 \times 3^1 \times 5^1)$

$\phi(240) = (2^4 - 2^{4-1})(3^1 - 3^0)(5^1 - 5^0)$

$= (16 - 8)(3-1)(5-1)$

$= (8)(2)(4) = 64$

What is meaning of $a = b \bmod n$

↳ If we devide b by n so remainder is a

(4) $\phi(49) = \phi(7^2)$

$= 7^2 - 7^1$

$= 49 - 7$

$= 42$

Fermat's littel Theorem

1st version

↳ It such that if p is a prime & a is an integer, such that

p doesn't divide a.

then $a^{p-1} \equiv 1 \bmod p$.

↳ congruence

2nd version

If $a \equiv b \bmod n$

↳ meaning is if we devide a by n ($a|n$) then remainder is b

Date
Page

2nd Version

It removes the condition on a.

It says that if p is prime & a is any integer then,

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

Application of Fermat theorem.

↳ It is helpful for quickly finding the solution to some exponentiations.

(i) eg $6^{10} \bmod 11$

2. Modular Exponentiation

↳ It is a type of exponentiation performed over a modulus.

→ $a^b \pmod m$

eg = $23^3 \bmod 30$.

=

Date
Page

Modulo Operations

x mod y = r

↳ when x is divided by y → remainder is r

give eg. of clock

↳ 11 pm right now → want to sleep for 8 hours
At what time you will wake up

(11 + 8) = 19 pm
↳ There Nothing like 19 AM

(19 − 12) = 7 AM !!

To find the correct answer → we need to perform a modulo operation (mod 12)
- You add the two numbers (11+8) & keep subtracting 12 from it until you get <12 number →

What is modulo Congruence ?

Two numbers a & b are said to be congruent modulo n when their difference a−b is integrally divisible by n,

so (a−b) is multiple of n

Mathematically, modulo congruence formula is written as,

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

& n is called the modulus of congruence.

In simple words

↳ a & b are said to be congruent modulo n when they both have same remainder when divided by n,

$$a \bmod n = r$$
$$b \bmod n = r.$$

r is simply common remainder

So put it simply:

↳ Modulus congruence occurs when two numbers have the same remainder after the same division.

$24 \bmod 10 = 4$

$34 \bmod 10 = 4$

So 24 & 34 are congruent modulo 10.

$9 \equiv 21 \pmod 6$

$(21 - 9) = 12$

↳ (divisible by 6)

OR

(a mod n)

9 mod 6 or = 3

21 mod 6 = 3

(b mod n)

How to calculate modulo

Step-1 → 250 mod 24

Step-2 → $24 \overline{)250} = 10$ .... (Operation of integer division)

Use ~~quotient~~ quotient.

Step-3 → Take division (24) & quotient (10)

Multiply both (24 * 10) = 240

Step-3 → Subtract 250 - 240 = 10

250 mod 24 = 10.

Modular Arithmetic

(1) Modular addition & Subtraction

$(A+B) \bmod c = (A \bmod c + B \bmod c) \bmod c$

$(A-B) \bmod c = (A \bmod c - B \bmod c) \bmod c$

$A = 11, B = 7$ & $c = 4$

L.H.S $(11+7) \bmod 4 = 18 \bmod 4 = 2$

R.H.S $(11 \bmod 4 + 7 \bmod 4) \bmod 4 =$

$(3 + 3) \bmod 4 = 6 \bmod 4 = 2$

(2) Modular Multiplication

$(A*B) \bmod c = (A \bmod c * B \bmod c) \bmod c$

L.H.S $(11*7) \bmod 4 = 77 \bmod 4 = 1$

R.H.S $((11 \bmod 4) * (7 \bmod 4)) \bmod 4$

$(3 * 3) \bmod 4 = 9 \bmod 4 = 1$

(3) Modular exponentiation

eg: $A \hat{} B \bmod c = ((A \bmod c) \hat{} B) \bmod c$

$(11 \hat{} 7) \bmod 4 = ((11 \bmod 4) \hat{} 7) \bmod 4$

$(19487171) \bmod 4 = (3 \hat{} 7) \bmod 4$

$= 3$ $= 2187 \bmod 4 = 3$

Calculate 2^{60}

$A=2, y=10, C=3$

eg (2) $2^{100} = 2^{50} * 2^{50}$

$2^{100} \bmod 3 = ((2^{50} \bmod 3) * (2^{50} \bmod 3)) \bmod 3$

$= (1 * 1) \bmod 3$

$= 1 \bmod 3$

$= 1$

eg-3

$2^3 \bmod 3 = 8 \bmod 3 = 2$

How to calculate $A \wedge B \bmod C$ quickly if B is a power of 2.

$A \wedge 2 \bmod C = (A * A) \bmod C$

$= ((A \bmod C) * (A \bmod C)) \bmod C$

$7 \wedge 256 \bmod 13$

$7 \wedge 1 \bmod 13 = 7 \bmod 13 = 7$

$7 \wedge 2 \bmod 13 = (7 \wedge 1 \bmod 13 \times 7 \wedge 1 \bmod 13) \bmod 13$

$(11-4) = 7 \quad 7 \bmod 13 = 7$

$= (7 \times 7) \bmod 13$

$= 49 \bmod 13$

$= 10$

17 mod 10 3 → 17 - 3 = 14
14 - 3 = 11
11 - 3 = 8
8 - 3 = 5
5 - 3 = 2 → (2)

$7^{24} \bmod 13 = (7^2 * 7^2) \bmod 13$

$= (7^2 \bmod 13 * 7^2 \bmod 13) \bmod 13$

$= (10 * 10) \bmod 13 = 100 \bmod 13 = 9$

$7^4 \bmod 13 = 9$.

$(7^4 \times 7^4) \bmod 13 \rightarrow$
$(7^4 \bmod 13 \times 7^4 \bmod 13) \bmod 13$

Cont this for 6 iteration

$7^{256} \bmod 13 = (7^{128} * 7^{128}) \bmod 13$

$= (17^{128} \bmod 13 * 7^{128} \bmod 13) \bmod 13$

$= (3 * 3) \bmod 13$

$= 9 \bmod 13$

$= 9$.

Q.4 $23^3 \bmod 30$.

= (find diff 23 - 30 = -7.)

$23^3 \bmod 30 = (-7)^3 \bmod 30$

$= (-7)^2 \times (-7)^1 \bmod 30$.

$= 49 \times -7 \bmod 30$.

$= -343 \bmod 30$.

$= -13 \bmod 30$.

$= 17 \bmod 30$.

$23^3 \bmod 30 = 17$.

(5) $31^{500} \bmod 30$

$= (31 - 30) = 1$

$= 1^{500} \bmod 30$

$= \boxed{1}$

(6) $242^{329} \bmod 243$

$(242 - 243) = -1$

$242^{329} \bmod 243 = -1^{329} \bmod 243$

$= -1 \bmod 243$

$= 242 \bmod 243$

$\boxed{242^{329} \bmod 243 = 242}$

(7) $11^7 \bmod 13$

$= (-2)^7 \bmod 13$

$= -128 \bmod 13$

$= -11 \bmod 13$

$= 2 \pmod{13 - 11}$

$\boxed{11^7 \bmod 13 < 2}$

(8) 8^7 mod 187.

8^1 mod 187 = 8

8^2 mod 187 = $8^1 \times 8^1$ mod 187
= 64
= 64 mod 187
= 64.

8^4 mod 187 = $8^2 \times 8^2$ mod 187
= 64^2 mod 187
= 64 × 64 mod 187
= 4096 mod 187 = 152

8^7 mod 187 = $8^4 \times 8^2 \times 8^1$ mod 187.
= (152 * 64 * 8) mod 187
= 77963264 mod 187
8^7 mod 187 = 11

(9) 3^{100} mod 29

3^1 mod 29 = 3 mod 29 = 3 or −26
3^2 mod 29 = 3×3 mod 29 = 9 mod 29 = 9 or −20
3^4 mod 29 = 9×9 mod 29 = 81 mod 29 = 23 or −6
3^8 mod 29 = −6×−6 mod 29 = 36 mod 29 = 7 or −22
3^{16} mod 29 = $3^8 \times 3^8$ mod 29 = 7×7 mod 29 = 49 mod 29
= 20 or −9
3^{32} mod 29 = $3^{16} \times 3^{16}$ mod 29 = −9×−9 mod 29 = 81 mod 29
= 23 or −6.
3^{64} mod 29 = $3^{32} \times 3^{32}$ mod 29 = $3^{32} \times 3^{32}$ mod 29
= −6 × −6 mod 29
= 36 mod 29 = 7 or −22

$3^{100} \bmod 29 = 3^{64} \times 3^{32} \times 3^{4} \bmod 29$

$= 7 \times (-6) \times (-8) \bmod 29$

$= 7 \times 36 \bmod 29$

$= 252 \bmod 29$

$= 20$

(9) $23^{16} \bmod 30$.

$23^{16} \bmod 30 = (((23^2)^2)^2)^2 \bmod 30$

$= (((-7)^2)^2)^2 \bmod 30$

$= (((49)^2)^2)^2 \bmod 30$.

$= (((19)^2)^2)^2 \bmod 30$.

$= (((-11)^2)^2)^2 \bmod 30$

$= ((121)^2)^2 \bmod 30$.

$= 1 \bmod 30$

$= 1$

In many ways you can solve example

* Fermat's theorem.

↳ States that

If p is a prime number and a is a positive integer not divisible by p then

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

Ch1 Does fermat's theorem hold for $p=5$ & $a=2$?

Given $p=5$ & $a=2$

p is prime number ? → Yes

a is multiple integer ? → Yes & not divided by p.

Initial conditions are met

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

$2^{5-1} \equiv 1 \pmod{5}$

$2^4 \equiv 1 \pmod{5}$

$16 \equiv 1 \pmod{5}$

↳ write verify $16 \mid 5$ = remainder = 1

So Fermat's theorem holds true for $p=5$ & $a=2$

(2) $p=13$ & $a=11$

$(11)^{13-1} \equiv 1 \pmod{13}$

$(11)^{12} \equiv 1 \pmod{13}$

↳ use modular exponentiation

$(-2)^{12} \equiv 1 \pmod{13}$

$(-2)^{4\times3} \equiv 1 \pmod{13}$

$(16)^3 \equiv 1 \pmod{13}$

$(3)^3 \equiv 1 \pmod{13}$

$27 \equiv 1 \pmod{13}$

$27 \mid 13 \rightarrow$ remainder = 1

↳ Fermat's theorem holds true for $p=13$ & $a=11$

classmate
Date
Page

(5) $p = 6$ & $q = 2$

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

$(2)^5 \equiv 1 \pmod{6}$

$32 \equiv 1 \pmod{6}$

Rem $32 \mid 6 \rightarrow$ remainder $= 2$

Multiplicative inverse

eg $5 \times 5^{-1} = 1$

$5 \times \left(\frac{1}{5}\right) = 1$

$\frac{1}{5}$ is multiplicative inverse of 5

for any number $A \times \left(\frac{1}{A}\right) \rightarrow 1$

$\frac{1}{A}$ is multiplicative inverse of A

↳ Real challenge comes when we deal with modulo arithmetic

Under mod n

$A \times A^{-1} \equiv 1 \pmod{n}$

(1) $3 * ? \equiv 1 \bmod 5$

↳ what is multiplicative Inverse of $3 \bmod 5$

$3 * 1 \equiv 1 \bmod 5$

$\frac{3}{5}$ → remainder will not be 1

$\frac{3 \times 2}{5}$ → we get 1 as remainder.

2 is multiplicative of for $3 \bmod 5$

or

3 is multiplicative of for $2 \bmod 5$:

(2) $2 \times ? \equiv 1 \bmod 11$

$(2 * 1) \mid 11$ → remainder ≠ 1

$(2 * 2) \mid 11$ → No

$(2 * 3) \mid 11$ → No

$(2 * 4) \mid 11$ → No

$(2 * 5) \mid 11 \rightarrow 10 \mid 11 \rightarrow 10$ or -1 remainder

$(2 * 6) \mid 11 \rightarrow 12 \mid 11 \rightarrow$ remainder = (1).

6 is multiplicative inverse of $2 \bmod 11$

If gcd (A, B) two numbers is not classmate
that is → they are not relatively
prime → & hence no multiplicative inverse
be there.

Date
Page

(3) $4x ? \equiv 1 \mod 5$

$4 \times 4 \equiv 1 \mod 5$

$16 \mid 5 = 1$ remainder.

(4) $5x ? \equiv 1 \mod 10$

$(5 \times 1) \mid 10$ = 5 as remainder

$(5 \times 2) \mid 10 = 0$ as remainder

$(5 \times 3) \mid 10 = 15 \mid 10$ = 5 as remainder

↳ U will never get m.i.

bcz 5 & 10 are not relatively prime

So m.i is possible only if

$4x ? \equiv 1 \mod 5$

Numbers are relatively prime

NOTE, 2 mod 5 → ans is 3

2 mod 7 → ans is 4.

(2 × 4) mod 7 = 1.

So it depends on the number.

RSA Examples

(1) Two prime numbers p & q

(2) Calculate $n = p \times q$

(3) Calculate $\phi(n) = (p-1)(q-1)$

(4) Choose e → such that gcd $(e, \phi(n)) = 1$
$1 < e < \phi(n)$

(5) Calculate d so that,
$d \equiv e^{-1} \bmod \phi(n)$
such that $ed \equiv 1 \bmod \phi(n)$
→ d is multiplicative inverse of e
in mod $\phi(n)$

(6) get public key $\{e, n\}$

(7) get private key $\{d, n\}$

Encryption → Ciphertext $C = P^e \bmod n$

decryption → plain text $P = C^d \bmod n$

① $p = 3, \quad q = 11$

② $n = p * q = 33$

③ $\phi(n) = (3-1)(11-1) = (2)(10) = 20$

④ Choose → e, e may be given
↳ such that $1 < e < \phi(n)$

$= e = 7 \rightarrow 1 < 7 < 20$ & $\gcd(e, \phi(n)) = 1$
$\gcd(7, 20) = 1$

⑤ $d \equiv e^{-1} \bmod \phi(n)$

$de \equiv 1 \bmod \phi(n)$

$7 * d \equiv 1 \bmod \phi(n)$

$(7 * d) \bmod \phi(n) = 1$

$(7 * d) \bmod 20 = 1$

find multiplicative inverse of 7.
↳ 3

$7 * 3 \bmod 20 = 1$

$d = 3$

(extended euclidean algo)
euclidean

(4) For large numbers, → How to find multiplicative inverse
Take multiples of 20,
$7 \times d \bmod 20 = 1$

20 → +1 = 21 → Try to multiply that with
40 +1 = 41 7 & remainder should be 1
60 +1 = 61
80 +1 = 81

(5) Public key = $\{e, n\} = \{7, 33\}$

(6) Private key = $\{d, n\} = \{3, 33\}$

ENCRYPTION
$C = m^e \bmod n$ $m < n$
↳ (imp).

$m = 31$ given
eg. Abhi → 4 chars
$m = 4$

$C = 31^7 \bmod n$

$= 31^7 \bmod 33$

$C = 4$

Decryption
$m = C^d \bmod n$
$= (4)^3 \bmod 33$
$m = 31$

Can be thought of as RSA → in which value of $\frac{e}{d}$ → fixed

* Rabin Cryptosystem (based on Quadratic Congruence)

↳ Public key cryptosystem → invented by

→ Uses asymmetric key encryption

→ Rabin cryptosystem can be thought of as an RSA → where value of e d are fix.

→ The encryption is

$$C \equiv P^2 \pmod{n}$$

The decryption is

$$P \equiv C^{\frac{1}{2}} \pmod{n}$$

→ In Rabin cryptosystem → Public key → n & Private key is (n)

Quadratic Congruence

↳ is the equation of the form

$$a_2 x^2 + a_1 x + a_0 = 0 \pmod{n}$$

↳ in the eqn $a_2 = 1$ & $a_1 = 0$;

↳ $x^2 \equiv a \pmod{n}$

(1) Quadratic congruence modulo a prime

incongruent numbers → after dividing by same number → remainder is different.

- $x^2 \equiv a \pmod{n}$
, where p is prime, a is integer. Such that $p \nmid a$.

- It can be proved that, this kind of eqn's will have either no solution or exactly two incongruent solution.

Eg: $x^2 \equiv 3 \pmod{11}$

What will the value of x that we will get 3 remainder.

$x = 5$ & $x = -5$

$x^2 \equiv 3 \pmod{11}$

$x \equiv 5 \pmod{11}$

$x \equiv -5 \pmod{11}$ → $x \equiv 6 \pmod{11}$

↳ instead of writing -5, we will write 6 $(11-5)$.

$(5, 6)$ are the solution → which are the incongruent solutions.

eg.2 eqn → $x^2 \equiv 2 \bmod 11$

↳ No solution

(No integer such that its square is $2 \bmod 11$)

Rabin Algo example

Procedure :- Key generation, encryption & decryption are.

Key generation

① Choose two large prime numbers p & q in the form of $4k+3$ & $p \neq q$

↳ when we are performing modulo operation ↳ remainder should be 3.

② $n \leftarrow p \times q$

③ Public key $\leftarrow n$

④ Private key $\leftarrow (q, p)$

Encryption :- $C \leftarrow P^2 \bmod n$

Decryption :- $a_1 \leftarrow + \left(C^{(p+1)/4}\right) \bmod p.$

$a_2 \leftarrow - \left(C^{(p+1)/4}\right) \bmod p.$

$b_1 \leftarrow + \left(C^{(q+1)/4}\right) \bmod q$

$b_2 \leftarrow - \left(C^{(q+1)/4}\right) \bmod q$

Security of Rabin cryptosystem → Difficulty of factoring

Drawback → Four possible inputs generated

→ Extra complexity is required to decrypt

Note :- Rabin cryptosystem is not deterministic i.e decrypting creates 4 plain texts.

Ex (1) Let $p = 23$ & $q = 7$.

↳ Receiver

(1) Bob selects $p = 23$ & $q = 7$. Note that both are congruent to 3 mod 4 → i.e.

$23 \bmod 4 \rightarrow$ will give 3

$7 \bmod 4 \rightarrow$ will give 3

select

p & q → such that they are in the form of $4k+3$.

(2) bob calculates $n \leftarrow p \times q$

$\leftarrow 23 \times 7$

$n \leftarrow 161$ → Public key

(3) Bob announces $n \rightarrow$ public key & keep p & q secret.

(4) Alice wants to send plain text $P = 24$. Note that value of n & P are relatively prime, 24 is in Z^*_{161}

P should be less than n (i.e. $24 < 161$)

Alice calculates cipher text text by using

$C \leftarrow P^2 \bmod n \Rightarrow C \leftarrow 24^2 \bmod 161$

↳ plain text

$\leftarrow 576 \bmod 161$

$\leftarrow 73$

Alice sends $C = 73$ to bob.

5. Bob receives 93 & calculates 4 values

$a_1 = +(c^{(p+1)/4}) \bmod p$

$= 93^{(23+1)/4} \bmod 23$

$= 1 \bmod 23$

$a_2 = -(c^{(p+1)/4}) \bmod p$

$= -9 \bmod 23 = 22 \bmod 23$

$a_3 = +(c^{(q+1)/4}) \bmod q$

$b_1 = +(c^{(q+1)/4}) \bmod q$

$= +(93^{(7+1)/4}) \bmod 7$

$= 93^{8/4} \bmod 7 = 93^2 \bmod 7 = 4 \bmod 7$

$b_2 = -(c^{(q+1)/4}) \bmod q$

$= -4 \bmod 7 \Rightarrow 3 \bmod 7$

6). Possible answers are (a_1, b_1) (a_1, b_2), (a_2, b_1) (a_2, b_2)

* Chinese Remainder Theorem

↳ CRT is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below.

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_n \pmod{m_n} \end{aligned}\right\} \text{different moduli}$$

CRT states that above equations have a unique solution if the moduli are relatively prime.

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \dots + a_n M_n M_n^{-1}) \bmod m$$

Eg.1

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \end{aligned}$$

Solution:-

Given		To find		
$a_1 = 2$	$m_1 = 3$	M_1	M_1^{-1}	m
$a_2 = 3$	$m_2 = 5$	M_2	M_2^{-1}	
$a_3 = 2$	$m_3 = 7$	M_3	M_3^{-1}	

Note :- Unique soln exists if & only if m_1, m_2 & m_3 are relatively prime.

$$\boxed{\gcd(m_1, m_2, m_3) = 1}$$

$$\boxed{M = m_1 \times m_2 \times m_3}$$

$$\boxed{M = 3 * 5 * 7 = 105}$$

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

To find $m_1^{-1}, m_2^{-1}, m_3^{-1}$

$$\boxed{M_1 \times M_1^{-1} = 1 \bmod m_1}$$

$$35 \times M_1^{-1} = 1 \bmod 3$$

$35 \mid 3 \Rightarrow$ will get 2 as remainder so 1 is not multiplicative inverse

$$35 \times 2 = 1 \bmod 3$$

$70 \mid 3 = (1) \rightarrow$ will get remainder

classmate
Date
Page

$m_1^{-1} = 2$

$m_2 \times m_2^{-1} = 1 \bmod m_2$

$21 \times m_2^{-1} = 1 \bmod 5.$

$m_2^{-1} = 1$

$m_3 \times m_3^{-1} = 1 \bmod m_3$

$15 \times 1 \mid 7 \longleftrightarrow (1) \rightarrow$ we'll get 1 as remainder.

$m_3^{-1} = 1$

$x \equiv (a_1 m_1 m_1^{-1} + a_2 m_2 m_2^{-1} + a_3 m_3 m_3^{-1}) \bmod m$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= 233 \bmod 105$

$x = 23$

Now we have eqn,

$x \equiv 2 \pmod 3$

Put $x = 23$

$23 \equiv 2 \pmod 3$

$23 \mid 3 \rightarrow (2)$ remainder

$x \equiv (3 \bmod 5)$

$23 \mid 5 = (3) \rightarrow$ remainder

$x \equiv 2 (\bmod 7)$

$23 \mid 7 = (2) \rightarrow$ remainder

↳ CRT → help us to find different congruent eqn under one variable.

(only one condition → Moduli value should be relatively prime)

* Quadratic Residues & non-residue.

↳ In eqn $x^2 \equiv a (\bmod p)$, a is called quadratic residue (or) if eqn has two solution & a is called quadratic non-residue if the eqn has no solution.

RSA Attacks

① Plain Text Attacks

- Short message Attack
  - Assume that attacker knows some block of P.T & tries to decode cipher text
  - To prevent this pad the plaintext before encrypting
- Cycling Attack
  - Attacker thinks that P.T is cipher text permutation
  - He will keep doing it & apply for cipher text
- Unconcealed message Attack
  - Sometimes it happens that P.T is same as cipher text after encryption

② Chosen cipher attack

→ If attacker is able to find out P.T from C.T using Extended Euclidean Algo.

③ Factorization attack

If attacker will able to know P & Q using N, then he could find out the value of private key. This can be failed when N contains atleast 300 longer

digits in decimal terms, but attacker will not able to find.

(4) Attacks on Encryption key

↳ If value of E is small, then attack is possible

Take value of E = $2^{16}+1$

(5) Attacks on Decryption key

↳ (1) Revealed decryption exponent Attack

If attacker somehow gets decryption key D, not only the cipher text generated by encrypting the P.T with corresponding encryption key is in danger

↳ but future messages also are in danger.

→ so take from $\nearrow p$ / $\searrow q$

(2) Low decryption exponent attack.

↳ D = $2^{16}+1$ (Carlsen)

classmate
Date
Page

Rabin Algo.

(1) p & q select

(2) $n = p \times q$ — n → Public key; (p, q) → Private key

(3) Encryption $C = m^2 \bmod n$.

(4) Decryption $m_p = \sqrt{C} \bmod p = \pm C^{\frac{p+1}{4}} \bmod p$

$m_q = \sqrt{C} \bmod q = \pm C^{\frac{q+1}{4}} \bmod q$

↓

To solve this CRT is used

$p = 7$, $q = 11$

$C = 23$ $m = ?$

$n = p \times q = 7 \times 11 = 77$.

Check $p \bmod 4 = 3$ or not → $7 \bmod 4 = 3$

$q \bmod 4 = 3$ or not → $11 \bmod 4 = 3$.

Decryption

$m_p = \pm C^{\frac{p+1}{4}} \bmod p$

$= \pm 23^{\frac{7+1}{4}} \bmod 7$

$= \pm 23^{8/4} \bmod 7$

$= \pm 23^2 \bmod 7$

$= \pm 529 \bmod 7$

$= \pm 4 \; m_2 \; 7$

$m_2 = \pm 23^{\frac{11+1}{4}} \; m_2 \; 2$

$= \pm 23^{12/4} \; m_2 \; 11$

$= \pm 23^{3} \; m_2 \; 11$

$= \pm 1 \; m_2 \; 11$

$m_1 = m_p = 4 \; m_2 \; 7$ $m_2 = 1 \; m_2 \; 11$	$m_3 = m_p = -4 \; m_2 \; 2$ $m_4 = 1 \; m_2 \; 11$
$m_2 = m_p = 4 \; m_2 \; 7$ $m_4 = -1 \; m_2 \; 11$	$m_4 = m_p = -4 \; m_2 \; 7$ $m_4 = -1 \; m_2 \; 11$

$X = (4$

classmate
Date
Page

Assign of. 1 onti ....

Calculate for P.T using Chinese Remainder theorem.

$m_1 = CRT(a_1, b_1, P, Q)$
$m_2 = CRT(a_2, b_2, P, Q)$
$m_3 = CRT(a_2, b_1, P, Q)$
$m_4 = CRT(a_2, b_2, P, Q)$

bob takes four possible answers

(a_1, b_1) , (a_2, b_2), (a_2, b_1) & (a_1, b_2)

Let $a_1 = 1$, $b_1 = 4$. Considering with modulo $\rightarrow P = 23$ & $Q = 7$.

$X = 1 \bmod 23$.
$X = 4 \bmod 7$

Use CRT

$m = m_1 \times m_2 = 23 \times 7 = 161$.

$m_1 = \frac{m}{m_1} = \frac{161}{23} = 7$

$m_2 = \frac{m}{m_2} = \frac{161}{7} = 23$.

$m_1^{-1} = 7^{-1} \bmod 23 = 10$

$m_2^{-1} = 23^{-1} \bmod 7 = 4$

As per the rule of m.I,

$m_1^{-1} = 7^{-1} \bmod 23$

$= 7^{23-2} \bmod 23$ (as 23 is prime)

$= 7^{21} \bmod 23$

$m_1^{-1} = 10$

$m_2^{-1} = 23^{-1} \bmod 7$

$= 23^{7-2} \bmod 7$

$= 23^5 \bmod 7$

$= 4.$

$X = (a_1 \times m_1 \times m_1^{-1} + a_2 \times m_2 \times m_2^{-1}) \bmod M$

$= (1 \times 7 \times 10 + 4 \times 23 \times 4) \bmod 161.$

$X = 116$ one of the value of X.

Case: 2 $(a_1 = 1, b_2 = 3)$

$X = 1 \bmod 23$

$X = 3 \bmod 7$

$m = 23 \times 7 = 161$

$m_1 = m / m_1 = 161 / 23 = 7$
$m_2 = m / m_2 = 161 / 7 = 23.$

$m_1^{-1} = 10$
$m_2^{-1} = 4$ (As per previous calculation)

$X = (a_1 \times m_1 \times m_1^{-1} + a_2 \times m_2 \times m_2^{-1}) \bmod m$

$= (1 \times 7 \times 10 + 3 \times 23 \times 4) \bmod 161$

$= 346 \bmod 161$

$X = 24$

Case: 3 $(a_2 \& b_1) = (22, 4)$

$X = 22 \bmod 23$, $m_1^{-1} = 10$
$X = 4 \bmod 7.$ $m_2^{-1} = 4$

$X = (a_1 \times m_1 \times m_1^{-1} + b_1 \times m_1 \times m_1^{-1})$

$= (22 \times 7 \times 10 + 4 \times 23 \times 4) \bmod 161$

$= (1540 + 368) \bmod 161$

$X = 137$

case - 4 $(a_2, b_2) = (28, 3)$.

$X = (a_1 + m_1 \times m_1^{-1} + b_2 + m_2 + m_2^{-1}) \bmod m$

$= (22 \times 10 + 7 + 3 + 23 + 4) \bmod 101$

$X = 45$

Final form P.T = $X = 116$ $X = 45$

$X = 24$ $X = 237$

correct one

(s) Bob needs to make a decision based on the situation

classmate
Date
Page

Elgamal Cryptography

↳ Asymmetric key

Key generation

↳ 1) select large prime number (P)

2) select decryption key (D)

3) select second part of encryption key or public key (E1)

4) Third part of encryption key or public key
$E2 = E1^D \bmod P$.

5) Public key (E1, E2, P), Private key = D.

Assume

let $P = 11$, $D = 3$

let $E1 = 2$

$E2 = E1^D \bmod P = 2^3 \bmod 11$

$= 8 \bmod 11$

$\boxed{E2 = 8}$

Public key $(2, 8, 11) \leftarrow (E1, E2, P)$

Let P1=7

Encrypting

1) select Random integer (R) = let R=4

2) $C1 = E1^{R} \bmod P$, $C1 = 2^{4} \bmod 11 = 5$

3) $C2 = (P1 \times E2^{R}) \bmod P$

$= (7 \times 8^{4}) \bmod 11$

$= 28672 \bmod 11$

$C2 = 6$

4) $C.T = (C1, C2) = (5, 6)$

Decrypting

$P1 = [C2 \times (C1^{D})^{-1}] \bmod P.$

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

Let us Calculate $(5^{3})^{-1} \bmod 11$

$(125)^{-1} \bmod 11$

$125 \times x = 1 \bmod 11$

$\frac{125 + x}{11} = 1$

$x = 3$

So $((5)^{3})^{-1} \bmod 11 = 3$

$P_T = (C+3) \bmod 11$

$= 18 \bmod 11$

$\boxed{P_T = 7}$

* The Discrete Logarithm Problem

↳ * Primitive Root

↳ To know about primitive roots of Prime numbers

— Determine whether a number is a primitive root of a given prime number or not

Diffie Hellman algo

Defn:-

α is said to be a primitive root of prime number 'p', if $\alpha^1 \bmod p$, $\alpha^2 \bmod p$ $\alpha^3 \bmod p$ ... $\alpha^{p-1} \bmod p$ are distinct

Is 2 a primitive root of prime number 5?

$2^1 \bmod 5 \rightarrow 2 \bmod 5 \rightarrow 2$

$2^2 \bmod 5 \rightarrow 4 \bmod 5 \rightarrow 4$

$2^3 \bmod 5 \rightarrow 8 \bmod 5 \rightarrow 3$

$2^4 \bmod 5 \rightarrow 16 \bmod 5 \rightarrow 1$

All are distinct values

Ans :- Yes 2 is Primitive root of 5

eg: (2) 3 is Primitive root of 7?

$3^1 \bmod 7 \rightarrow 3 \bmod 7 \rightarrow 3$

$3^2 \bmod 7 \rightarrow 9 \bmod 7 \rightarrow 2$

$3^3 \bmod 7 \rightarrow 27 \bmod 7 \rightarrow 6$

$3^4 \bmod 7 \rightarrow 18 \bmod 7 \rightarrow 4$

$3^5 \bmod 7 \rightarrow 12 \bmod 7 \rightarrow 5$

$3^6 \bmod 7 \rightarrow 15 \bmod 7 \Rightarrow 1$

Distinct → Uniformly Distributed
→ Unique Values.

Yes → 3 is Primitive root of 5.

(3) eg: is 2 a Primitive ~~root~~ root of Prime number 7.

No

(4) 2 is a Primitive root of Prime number 11

* The discrete logarithm Problem

⇒ ↳ will understand the discrete logarithm problem

→ Know about the one-way function & it's Strength.

Analogy

Tea → milk + sugar + Tea powder → To prepare Tea - easy

If we have Tea → To find the exact proportion of milk, sugar with Tea Not possible ↳ difficult.

$5^1 \bmod 17 = 5$
$5^2 \bmod 17 = 8$
$5^3 \bmod 17 = 6$
$5^4 \bmod 17 = 13$
$5^5 \bmod 17 = 14$
$5^6 \bmod 17 = 2$
$5^7 \bmod 17 = 10$
$5^8 \bmod 17 = 16$
$5^9 \bmod 17 = 12$
$5^{10} \bmod 17 = 9$
$5^{11} \bmod 17 = 11$
$5^{12} \bmod 17 = 4$
$5^{13} \bmod 17 = 3$
$5^{14} \bmod 17 = 15$
$5^{15} \bmod 17 = 7$
$5^{16} \bmod 17 = 1$

(17) → Prime Number → $5^{16} \bmod 17$ → go upto 17-1

↳ Results are uniformly distributed

↓

$5^1 \bmod 17$ to $5^{16} \bmod 17$ → Once each

So we can say → 5 is primitive Root of 17

If we have,

$5^x \bmod 17 \equiv$ 1111111

x can be any number

Result will be equally distributed

↓

Only applicable if we have Prime number & primitive root for that Prime number

$5^x \bmod (17)$ → Prime number

↳ Primitive Root of 17

or

generator

$5^x \bmod 17 =$ → for any value of x computation is easy

one direction

Eg $5^{(x)} \bmod 17 \equiv 12$ Reverse direction is given

find the value of x

$5^9 \bmod 17 = 12$

$5^{25} \bmod 17 = 12$

$5^{41} \bmod 17 = 12$

$5^{57} \bmod 17 = 12$

$5^{73} \bmod 17 = 12$.

↳ so any value of x

if x is given → $5^x \bmod 17$ → easy

but reverse is not easy

↓

$5^x \bmod 17 = (12)$. → given

Theoritical Aspects

$g^x \bmod p$.

$2^x \bmod 7 = 4$

$x = 2, 5$ etc.

for smaller value of p. (ie. $2^x \bmod (7)$). (Smaller number)

↳ may be easy to find x.

If p is large → finding x is hard

If p is large → time & efforts to find x is very high

Strength of one way function → depends on how much time it takes to break it.

eg DLP Solve $\log_2 9 \bmod 11$

Soln:- Here $p = 11$

$g = 2$,

$x = 9$.

$\log_g x \equiv n \pmod p$

$x \equiv g^n \pmod p$

$9 \equiv 2^n \bmod 11$

Try $n = 1, 2, 3 \ldots$

$n = 6$

$2^6 \bmod 11 \equiv 9$

$\boxed{n = 6}$

find $2^x \pmod 7) = 4$.

Ans $\boxed{x = 2\ 45}$

Elliptic curves cryptography

↳ It is asymmetric public key cryptosystem.

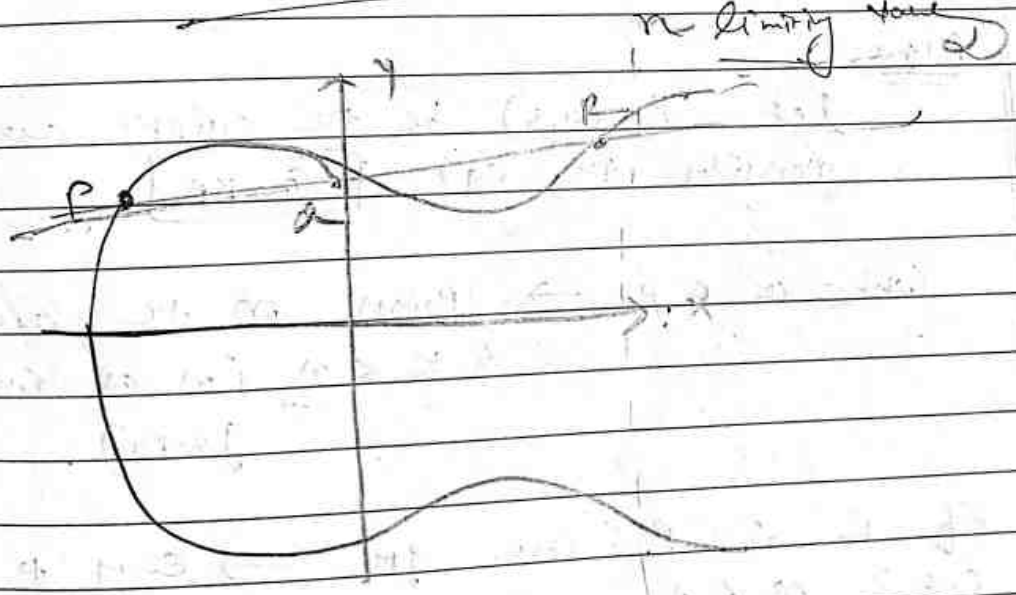
→ It provides equal security with smaller key size (as compared to RSA)

↳ 3072 bit → same security can be provided in ECC with 256 bit.

→ It makes use of elliptic curve.

→ Elliptic curves are defined by some mathematical functions - curve function.

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

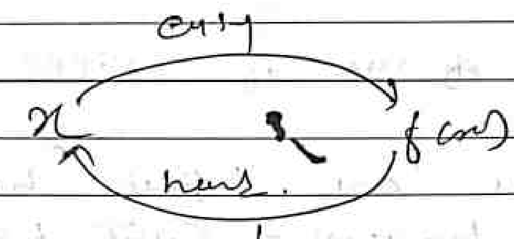


→ Symmetric to x-axis.

→ If we draw a line, it will touch max of 3 points

* Before Understanding ECC → Trapdoor Function

Trapdoor Function → Is a function that it is easy to compute in one direction yet difficult to compute in the reverse direction. (finding inverse) without special info is called Trapdoor.



↳ It is easy if given 't' → Trapdoor value.

Algo

let $E_p(a,b)$ be the elliptic curve containing the eqn, $Q = KP$.

Where Q & P → points on the curve & $K < n$ (n as shown in graph).

⇒ If K & P are given → easy to find Q but if Q & P are given → difficult to find K

↳ one way function

This is called discrete logarithmic Problem

ECC Algo

(1) ECC key Exchange

Two global Public elements. Constants

Eq (a, b) :- elliptic curve with a, b q

↳ Prime number or integer of form 2^m

G: Point on the curve / elliptic curve whose order is large value of (n)

User A key generation

Select Private key n_A $n_A < n$

Calculate Public key $P_A = n_A * G$

User B key generation

Select Private key n_B $n_B < n$

Calculate Public key $P_B = n_B * G$

Calculation of secret key by User A.

$$K_A = n_A \times P_B$$

Calculation of Secret key by User B

$$K_B = n_B \times P_A$$

ECC encrypting

→ Let the message be m

→ First encode the message m into a point on elliptic curve.

Let the point be P_m

↳ Now the point is encrypted

for encrypting chose a random positive integer K.

The cipher point will be

$$C_m = \{ K_G , P_m + K P_B \}$$

↳ For encryption Public key of B used

This point will be sent to the receiver

Decrypting

For decrypting, multiply 1st point in the pair with receivers ~~secret~~ key.

i.e $K_G * n_B$ → for decrypting private key of B is used.

Then subtract it from second point in the pair

$$P_m + K P_B - (K_G * n_B)$$

$$P_B$$

$$P_m + K P_B - K P_B \neq P_m$$

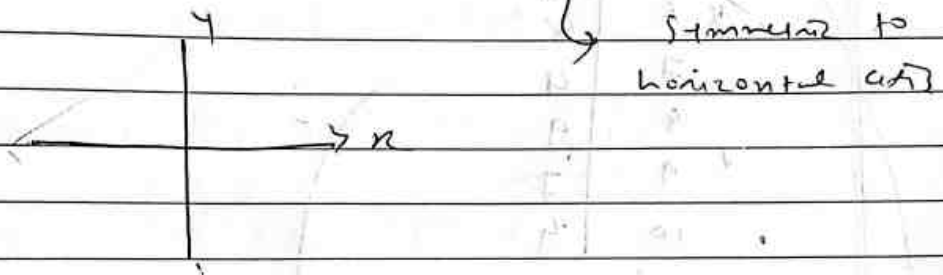
So Bruce gets the same point (P=Q) corresponds to message m.

⇒ Elliptical curve cryptography

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

$$y = \pm \sqrt{x^3 + ax + b}$$

Symmetric to $y=0$ condition



Q. To find the points on elliptic curve.

(1,6) $a=1, b=6$ $P=11$

opening in mod 11

$$y^2 = x^3 + ax + b \pmod{11}$$

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

L.H.S R.H.S

$P=11$

so value of x & y can be 0 to P-1

0 to 10

$y=1$

$x = 0 \to 10$

$y = 0 \to 10$

We need to find value of x & y such that L.H.S = R.H.S

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

R.H.S

$(6 \pmod{11})$

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

L.H.S

Check the points when L.H.S = R.H.S

$x = 2, \; y = 4$

$x = 2, \; y = 7$

for RHS = 5 → find LHS = 5 & by value

$x = 2$, $y = 4$ & $y = 7$.

(1) Here { point on elliptic curve } (2, 4) (7, 4)

(2) → (3, 5) & (3, 6)

(3) → for (5, 2), (5, 9)

(4) → (7, 2) (7, 9)

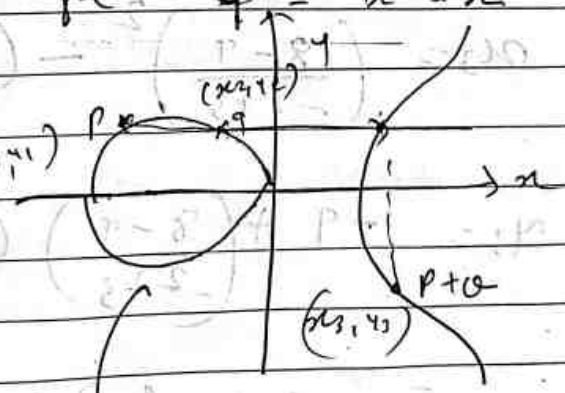
(5) → (8, 3) (8, 8)

(6) → (10, 2) (10, 9)

points on the elliptic curve

If we substitute this points on elliptic curve then → LHS Becomes RHS.

Eg Find P+Q, 2P for $y^2 = x^3 - x$



This is how elliptical curve looks like for given eqn $y^2 = x^3 - x$.

For P+Q, (case 1)

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

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

For 2P, (P = Q) Assume:

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

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

Given # $y^2 = x^3 - 36x$, $P = (-3, 9)$, $Q = (-2, 8)$

find P+Q & 2P.

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

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

$$= -9 + (1)(+9)$$

$$\boxed{y_3 = 0}$$

$(x_3, y_3) = (6, 0)$

Now find $2P$. So consider $P = (x_1, y_1) = (-3, 9)$

eq? $x^3 - 36x$ → so $a = 36$
given

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

$$= \left(\frac{27 - 36}{18}\right)^2 + 6$$

$$= (1/4) + 6 = 25/4$$

$$y_3 = -9 + \left(\frac{3 \times 9 - 36}{18}\right)(-3 - 25/4)$$
$$\hookrightarrow (x_3)$$

$$y_3 = -35/8$$

$$2P = \left(25/4, -35/8\right)$$

(This was simple as the values found were without modulo).

(x_1, y_1) $(0, 0)$

Eq.2 $E_{23}(1,1)$, $y^2 = x^3 + ax + b$

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

So the values for P+Q or 2P only lying from (0 to 22)

i) P (13,7) → ans is -P.

$-P = (x, -y) = (13, -7)$

$(-7 \bmod 23) = 16$

$-P = (13, 16)$

ii) Find Point R → P+Q

where P = (3,10), Q(9,7)

(x_1, y_1) (x_2, y_2).

$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$

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

$= \left(\frac{-3}{6}\right)^2 = 12$

$= 1/4 - 12 \pmod{23}$

$= 1/4 + 11 \quad (23 - 12)$

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

↳ find $(4^{-1}) \bmod 23$

$x_3 = 1 \times 6 + 11 = \boxed{17}$

$\boxed{x_3 = 17}$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_4 - x_3)$$

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

$$= -10 + \left(\frac{-1}{2}\right)(3-17) \quad \text{mod } 23$$

$$= \left(13 + (+1/2)(+14)\right) \quad \text{mod } 23$$

$(-10 \bmod 23 = 23 - 10 = 13)$

$$= 13 + 7$$

$$\boxed{y_3 = 20}$$

$R = (P + Q) = (x_3, y_3) = (17, 20)$

To find $2P \rightarrow x_3 = \left(\frac{3x^2 + 1}{2 \times 10}\right)^2 - (6) = \left(\frac{28}{20}\right)^2 + 17$

$\rightarrow (5/20)^2 + 17$ $\qquad (-6 \bmod 23)$

$(28 \bmod 23) = \left(\frac{1}{4}\right)^2 + 17$

$= (1 \times (4)^{-1})^2 + 17$

$(4^{-1} \bmod 23)$

$= (1 \times 6)^2 + 17$

$= 36 + 17 = 53 \bmod 23 \rightarrow (7)$

$$y_3 = -10 + \left(\frac{3 \times 9 + 1}{2 \times 10}\right)(3-7)$$

$$= 13 + \left(\frac{28}{20}\right) \times (-4)$$

$$= 13 + \left(\frac{14}{4}\right) \times (-4)$$

$$= 13 + (4)^{-1} \times (-4)$$

$$= 13 + 6(-4)$$

$$= 13 - 24 \mod 23$$

$$= 13 + 22$$

$$= 35 \mod 23$$

$$y_3 = 12$$

$$P = (x_3, y_3) = (4, 12)$$