Extended Euclidean Algorithm

Find the multiplicative inverse of 3 mod 5.

Q	A	B	R	T_1	T_2	$T = T_1 - T_2 \times Q$
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
[X]	1	0	[X]	(2)	-5	[X]

Q. Find the multiplicative inverse of :

1. 11 and 13.

Q	A	B	R	T_1	T_2	$T = T_1 - T_2 \times Q$
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6
2	2	1	0	-1	6	-13
[X]	1	0	[X]	(6)	-13	[X]

2. 11 mod 26.

Q	A	B	R	T_1	T_2	$T = T_1 - (T_2 \times Q)$
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
[X]	1	0	[X]	(-7)	26	[X]

$26 - 7 = 19$ [11 mod 26 = 19]

PAGE NO.:
DATE: / /

3. 99 mod 78. gcd ≠ 1. not exist.

Q	A	B	R	T_1	T_2	$T = T_1 - (T_2 \times Q)$
1	99	78	21	0	1	-1
3	78	21	15	1	-1	4
1	21	15	6	-1	4	-5
2	15	6	3	4	-5	14
2	6	3	0	-5	14	-33
☒	3	0	☒	14	-33	☒

Generation of Digital Certificate:

1. Choose a certificate authority :

2. Generate a key pair : Public / Private key pair.

3. Generate a certificate signing request (CSR):

4. Validate your identity :

e.g. SSL certificate, TLS certificate.

ans. in bullet points.

PAGE NO.:
DATE: / /

BENEFITS :

- Enhanced Security
- Enhanced Efficiency
- Reduced costs.
- Increased convenience
- Scalability

(They are valid throughout) (RAS Algorithm)

What are digital certificates?

Document that verifies the identity of an entity, including its name, public key and certificate insurance authority (CA).

STEPS :

1. Generate a Public / Private key pair.
2. Create a certificate signing request (CSR):
3. Submitting CSR to a certificate Authority (CA).
4. Receive and Install the certificate :
5. Testing.

PAGE NO.:
DATE: / /

1. Define Information security

→ practices, tools, policies → designed → protect info. system from threats ensuring CIA of data.

Importance in today's digital world safeguarding personal, organisational & governmental information.

Goals of ISS :

Confidentiality.	Integrity	Availability
Information is accessible to authorized users. to view it.	Information remains accurate and complete	Ensures information & resources are accessible to authorized users when needed.
Methods: encryption	Hash Fun^n	Redundancy
Access control	Digital sign.	Failover systems
Data Masking	Checksums	DDoS Protection.

PAGE NO.:
DATE: / /

9.	ECC	RSA
•	Smaller key size results in faster computations and reduced storage and transmission requirement	• Larger key size to achive same level of security results in slower performance and increased computational overhead.
•	Provides a higher security level per bit compared to RSA.	• security scales linearly with key size, longer bits are required.
•	More resistant to quantum attacks.	• Vulnerable to quantum attacks.

8. Common Methods for securely distributing symmetric keys.

- Key Exchange Algo. - Allows 2 parties to securely generate a shared key over an insecure network without transmitting the key.
- Public key Cryptography (e.g DES): the symm. key is encrypted with recepient public key ensuring only recepient can access it.
- Key Distribution centres (eg kerbros): A trusted party securely distributes session keys to users reducing the risk of key exposure.
- Secure Network Protocals: Protocols → exchange sym. keys

PAGE NO. :
DATE : / /

EULER'S ~~QUOTIENT~~ TOTIENT FUNCTION :

$\phi(7) = 6.$

$\phi(13) = 12 \quad (n-1 = 12)$

$\phi(n) = n-1$

$\phi(n) = p \times q$ (prime no.)

$= (p-1) \times (q-1)$

$= p \times q$

$= n \times \left(1 - \frac{1}{p}\right) \times \left(1 - \frac{1}{q}\right)$

(composite no.)

RSA Algorithm :

The RSA Algorithm is one of the most widely used algorithms for secure data transmission. It is an assymetric encryption algorithm i.e uses public key and private key.

STEPS :

1) Key Generation
2) Encryption
3) Decryption.

PAGE NO.:
DATE: / /

1) KEY GENERATION :

- Choose two large prime numbers (p & q)
- Compute $n = pq$ the value will be part of both the public and private key.
- Calculate qttotient of n (denoted by $\phi(n)$) which is $(p-1) \times (q-1)$
- Choose an integer 'e' such that $1 < e < \phi(n)$ and e is co-prime with $\phi(e)$
- Compute the private exponent of which is modular inverse of e modulo $\phi(n)$

$$d \times e \equiv 1 \pmod{\phi(n)}$$

public key = (n, e)

private key = (n, d)

2) ENCRYPTION :

To encrypt the message M convert the message M into a number m such that $0 < m < n$

The encrypted message c is calculated as

$$[c = m \hat{} e \bmod n]$$

c: ciphertext.

M = C = same value

3) DECRYPTION :

$$[M = c \hat{} e \bmod n.]$$

2

$128 \bmod 33$.

128
99
29

24384
24189

1) $p = 3$, $q = 11$

2) $n = p \times q$
$= 3 \times 11$
$= 33$.

3) $\phi(n) = \phi(33) = 3 \times 11$
$= (3-1) \times (11-1)$
$= 2 \times 10$.
$\phi(n) = 20$

4) $1 < e < \phi(n)$
$\therefore e = 7$.

5) $d \times e \equiv 1 \pmod{\phi(n)}$
$7d \equiv 1 \pmod{20}$
$d = 3$

6) $M = 2$
$m = 2$
$c = 2^7 \bmod 33$.
$c = 29$
$M = c^d \bmod n$
$= 29^3 \bmod 33$.
[$c = 2$.]

$29 - 33 = -4$
$-4^3 \bmod 33$.
$-64 \bmod 33$.
$31 \bmod 33$.
2.

PAGE NO. :
DATE : / /

$p = 5$, $q = 7$.

$n = p \times q$

$= 35$

$\phi(n) = \phi(35) = 5 \times 7$

$= (5-1) \times (7-1)$

$= 4 \times 6$

$\phi(n) = 24$

$\because \quad 1 < e < \phi(n)$

$e = 5$.

$d \times e \equiv 1 \pmod{\phi(n)}$

$5d \equiv 1 \pmod{24}$

$d = 5$.

$0 < m < 35$

$c = m \hat{} e \bmod (n)$ $\quad m = 2$.

$c = 2^5 \bmod 35$

$c = 3$.

$2^5 \bmod 35$

$32 \bmod 35$

3

$M = c \hat{} d \bmod n$

$= 3^{\wedge 5} \bmod 35$

$= 243 \bmod 35$

$M. = 33$.

PAGE NO.:
DATE: 4/10/24

Chinese Remainder Theorem:

It is used to solve a set of different congruent equations with one variable but different modulo which are relatively prime.

$$X \equiv a_1 \pmod{m_1}$$
$$X \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$X \equiv a_n \pmod{m_n}$$

The CRT states that the above equations have unique solutions of the modulo are relatively prime.

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

Ex: Example: Solve the foll" eq" using CRT:
$X \equiv 2 \pmod 3$; $X \equiv 3 \pmod 5$; $X \equiv 2 \pmod 7$

Sol":
$a_1 = 2$ $m_1 = 3$ $M_1 = 35$ $M_1^{-1} = 2$
$a_2 = 3$ $m_2 = 5$ $M_2 = 21$ $M_2^{-1} = 1$ $M = 105$
$a_3 = 2$ $m_3 = 7$ $M_3 = 15$ $M_3^{-1} = 1$

Step 1. $M = m_1 \times m_2 \times m_3$
$= 3 \times 5 \times 7$
$= 105$

PAGE NO.:
DATE: / /

Step 2: Calculate the values of M_1, M_2, M_3

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

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

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

Step 3: $M_1 M_1^{-1} \equiv 1 \pmod{m}$

$35\, M_1^{-1} \equiv 1 \pmod 3$

$M_1^{-1} = 2$.

$21\, M_2^{-1} \equiv 1 \pmod 5$

$M_2^{-1} = 1$

$15\, M_3^{-1} \equiv 1 \pmod 7$

$M_3^{-1} = 1$

Step 4: Using CRT,

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod (105)$$

$$X = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$$

$$X = 140 + 63 + 30$$

$$\boxed{X = 233} \bmod (105)$$

$X = 23$.

PAGE NO.:
DATE: / /

1. $X \equiv 5 \pmod 3$ (Invalid congruency)
$X \equiv 2 \pmod 5$
$X \equiv 1 \pmod{11}$

$a_1 = 5 \quad m_1 = 3 \quad M_1 = 55 \quad M_1^{-1} =$
$a_2 = 2 \quad m_2 = 5 \quad M_2 = 33 \quad M_2^{-1} =$
$a_3 = 1 \quad m_3 = 11 \quad M_3 = 15 \quad M_3^{-1} =$

$M = 165$

$M_1 M_1^{-1} \equiv 1 \pmod{m_1}$
$55\, M_1^{-1} \equiv 1 \pmod 3$
$M_1^{-1} = 1$

$M_2 M_2^{-1} \equiv 1 \pmod{m_2}$
$33\, M_2^{-1} \equiv 1 \pmod 5$
$M_2^{-1} = 7$

$M_3 M_3^{-1} \equiv 1 \pmod{m_3}$
$15\, M_3^{-1} \equiv 1 \pmod{11}$
$M_3^{-1} = 14$

$X = (5 \times 55 \times 1 + 2 \times 33 \times 7 + 1 \times 15 \times 14) \bmod (165)$
$= (275 + 462 + 210) \bmod (165)$
$= 947 \bmod (165)$
$X = 122$

825
×5

PAGE NO.:
DATE: / /

2) $4X \equiv 5 \pmod 9$

$2X \equiv 6 \pmod{20}$

→ $4X \equiv 5 \pmod 9$

$4^{-1} \times 4X \equiv 5 \times 4^{-1} \pmod 9$

$X = 4^{-1} \pmod 9 \times 5 \pmod 9$

PAGE NO.:
DATE: / /

3. $x \equiv 5 \pmod 7$
$x \equiv 3 \pmod{11}$
$x \equiv 2 \pmod{13}$

$a_1 = 5 \quad m_1 = 7 \quad M_1 = 143 \quad M_1^{-1} = 12$
$a_2 = 3 \quad m_2 = 11 \quad M_2 = 91 \quad M_2^{-1} = 15 \quad M = 1001$
$a_3 = 2 \quad m_3 = 13 \quad M_3 = 77 \quad M_3^{-1} = 12$

$M M^{-1} \equiv 1 \pmod m$

$143\ M_1^{-1} \equiv 1 \pmod 7$
$M_1^{-1} = 12$

$91\ M_2^{-1} \equiv 1 \pmod{11}$
$M_2^{-1} = 15$

$77\ M_3^{-1} \equiv 1 \pmod{13}$
$M_3^{-1} = 12$

$X = (5 \times 143 \times 12 + 3 \times 91 \times 15 + 2 \times 77 \times 12) \bmod (1001)$
$= (8580 + 4095 + 1848) \bmod 1001$
$= 14523 \bmod (1001)$
$x = 509.$

FERMAT'S THEOREM:

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

3m theory, 5m eg.

8m// Show that $3^{256} \equiv 21 \pmod{100}$

$a = 3 \qquad n = 100$

$3^{\phi(100)} \equiv 1 \pmod{100}$

$\phi(100) = 2^2 \times 5^2$

$= 100 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{2}\right)$

$\phi(100) = 40$

$3^{256/40} = 3^{16} \equiv 21 \pmod{100}$

$43046721 \pmod{100} = 21 \pmod{100}$

→ Prove that for any odd integer P, $P^2 \equiv 1 \pmod{8}$

→ If $\frac{a}{b}$ and $\frac{b}{c}$ with gcd(a,b)=1, then prove that $\frac{ab}{c}$

a, b = 2, 3.

Fermat's Little Theorem:

If 'p' is a prime number and 'a' is a positive integer a ⊀ p then

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

PAGE NO :
DATE : / /

Ex: Does Fermat's Theorem holds true for ~~mod~~

1) $a = 2, p = 5$

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

$2^4 \equiv 1 \pmod 5$

2) $p = 13, a = 11$

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

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

3) $p = 6, a = 2$

$2^{6-1} \equiv 1 \pmod 6$

$2^5 \equiv 1 \pmod 6$

False

$2^5 \equiv 2 \pmod 6$

4) $p = 11, a = 5$

$5^{11-1} \equiv 1 \pmod{11}$

$5^{10} \equiv 1 \pmod{11}$

True

11 | 97655625 | 887784
88
96
88
85
77
86

PAGE NO.:
DATE: / /

★ Euler's Theorem:

For every positive integer 'a' and 'n' which are said to be relatively prime.

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

Example:
Prove if Euler's Theorem holds true for

1) $a = 3$, $n = 10$.

$$3^{\phi(10)} \equiv 1 \pmod{10}$$

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

$$\phi(10) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

$$= 10\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$$

$$\phi(n) = 4$$

$$3^4 \equiv 1 \pmod{10}$$
$$81 \equiv 1 \pmod{10}$$

True.

PAGE NO. :
DATE : / /

2) $a = 2$, $n = 10$.

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

$= 10 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$

$= 4$

$2^4 \equiv 1 \pmod{10}$

$16 \equiv 1 \pmod{10}$

False

3) $a = 10$, $n = 11$.

$\phi(n) = 11 \times 1$

$= 11$

$10^{11} \equiv 1 \pmod{11}$

4) $a = 11$, $n = 33$.

$\phi(n) = 3 \times 11$

$= 33 \times \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right)$

$= 33 \times \left(\frac{2}{3}\right)\left(\frac{10}{11}\right)$

$= 20$.

$11^{20} \equiv 1 \pmod{33}$

Primitive Root :

A number 'a' is a primitive root modulo 'n' if every no. is co-prime to n is congruent to power of 'a' modulo 'n'

Example :

1) Is 2 a primitive root of 5?

Repeat → P. root ✗
else P. root ✓

$2^1 \bmod 5 = 2$
$2^2 \bmod 5 = 4$
$2^3 \bmod 5 = 3$
$2^4 \bmod 5 = 1.$

2) Is 3 primitive root of 7?

$3^1 \bmod 7 = 3.$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6.$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$

3. Is 2 a primitive root of 7?

$2^1 \bmod 7 = 2$
$2^2 \bmod 7 = 4$
$2^3 \bmod 7 = 1$
$2^4 \bmod 7 = 2$

Non- Primitive

PAGE NO.:
DATE: / /

4. Is 2 a primitive root of 11

$2^1 \bmod 11 = 2$
$2^2 \bmod 11 = 4$
$2^3 \bmod 11 = 8$
$2^4 \bmod 11 = 5$
$2^5 \bmod 11 = 10$
$2^6 \bmod 11 = 9$.

Primitive.

5. What are the primitive roots of 5

$1 \bmod 5 = 1$
$1^2 \bmod 5 = 1$

$2 \bmod 5 = 2$
$2^2 \bmod 5 = 4$
$2^3 \bmod 5 = 3$.
$2^4 \bmod 5 = 1$
$2^5 \bmod 5 = 2$

$3 \bmod 5 = 3$

PAGE NO.:
DATE: / /

Deffie Hellman Algorithm :

The Diffie Hellman is a cryptographic protocol to exchange cryptographic keys over public channel.
It allows two-parties to establish a shared secret key that can be used for encryption without having to send the secret key itself over the insecure channel.

1. PUBLIC PARAMETERS:

- Prime Number (P) : A large number that is publicly known
- Generator (g) : A base number (publicly known) that is primitive root of mod P.

2. PRIVATE KEYS :

- Each participant chooses a private key that is not shared with anyone. Lets call the private key of person A as a and person B as b.

PAGE NO.:
DATE: / /

3. PUBLIC KEYS :

Each participate generates their public key raising the generator g to the power of their private key and taking the result mod P

public key A : $A = g^a \bmod P$

public key B : $B = g^b \bmod P$.

4. KEY EXCHANGE :

STEP I : Both the participants agree on the public parameter p and g.

STEP II : Each participants calculates the public key based on their private keys and their parameters.

STEP III : They exchange their public keys over a public channel.

STEP IV : Both the participants compute the shared key using other participants public key and their own private key

Shared key A : $A = B^a \bmod P$

Shared key B : $B = A^b \bmod P$.

PAGE NO. :
DATE : / /

Public key

$A = g^a \bmod p$.

$= 5^6 \bmod 23$.

$A = 8$.

$B = g^b \bmod p$

$= 5^{15} \bmod 23$.

$B = 19$

7.3094
11727

Shared key

$S_A = B^a \bmod p$

$= 19^6 \bmod 23$.

$S_A = 2$

$S_B = A^b \bmod p$

$= 8^{15} \bmod 23$.

$S_B = 2$.

3 17
15
55 17
84
68

2. $p = 17$, $g = 3$.
3. $p = 29$, $g = 2$.
4. $p = 31$, $g = 5$

$$17 \overline{)371293} \quad 21$$
$$34$$
$$31$$
$$17$$