Asymmetric key cryptography

1. Euler's Totient Function
2. Fermat's and Euler's Theorem
3. Chinese Reminder Theorem
4. RSA
5. Diffie Hellman key Exchange
6. ECC
7. Entity Authentication : Digital Signature.

Questions :—

Q.1. Write RSA Algorithm ? ~~Ao~~ Perform Encryption using the RSA Algorithm, for the following.
$p = 7, \; q = 11, \; e = 3, \; M = 9$

Q.2. Explain the public key crypto system? what is difference betⁿ. Symmetric Encryption algorithm and Asymmetric algorithm.

Q.3 Explain Diffie-Hellman key Exchange algorithm with Example ? Is Diffie-Hellman key Exchange Secure ?

Q.4. Describe Euclid's Algorithm with example

PAGE NO.:
DATE

Q5. Write a short note on "centralized key Distribution Scenario".

Q6. Describe Diffie-Hellman key exchange algorithm.

Q7. Write RSA algorithm. Explain its implementation an security

—x—x—x—x—

Topic :- Euler's Totient function :-

also called as (phi function)

the Euler's Totient function $\phi(n)$

How to find $\phi(n)$

① Euler's Totient function denoted as $\phi(n)$.

② $\phi(n)$ = Number of positive integers less than 'n' that are relatively prime to n.

ex., Find $\phi(5)$.

→ Here $n=5$.

Numbers less than 5 are 1,2,3,4 and 5

GCD	Relatively prime?
GCD(1,5)	✓
GCD(2,5)	✓
GCD(3,5)	✓
GCD(4,5)	✓

$$\phi(5) = 4$$

1x1	5x1
2x1	5x1
3x1	5x1
2x2	5x1
2x2x1	

DATE

ex., Find $\phi(n)$

$\phi(11)$

Here., $n = 11$.

Numbers less than 11 are

1, 2, 3, 4, 5, 6, 7, 8, 9, & 10.

GCD	Relatively prime
GCD(1,11) = 1	✓
GCD(2,11) = 1	✓
GCD(3,11) = 1	✓
GCD(4,11) = 1	✓
GCD(5,11) = 1	✓
GCD(6,11) = 1	✓
GCD(7,11) = 1	✓
GCD(8,11) = 1	✓
GCD(9,11) = 1	✓
GCD(10,11) = 1	✓

How many no. are relatively prime to 11. $\Rightarrow$ 10.

Find $\phi(8)$

Sol^n :

Here $n = 8$

Numbers less than 8 are 1, 2, 3, 4, 5, 6 & 7

GCD

Relatively Prime

GCD (1, 8) = 1 ✓

GCD (2, 8) = 2 ✗

GCD (3, 8) = 1 ✓

GCD (4, 8) = 4 ✗

GCD (5, 8) = 1 ✓

GCD (6, 8) = 2 ✗

GCD (7, 8) = 1 ✓

$1 \times 1 \quad 8 \times 1$

$2 \times 1 \quad 2 \times 4 = 2 \times 2 \times 2$

$3 \times 1 \quad 8 = 2 \times 4 = 2 \times 2 \times 2$

$2 = 2 \times 1$

$8 = 2 \times 4 = 2 \times 2 \times 2$

$1 = 1 \times 1 \quad 8 = 4 \times 2 = 2 \times 2 \times 2 = 2 \times 2 \times 2 \times 1$

$2 = 2 \times 1$

$8 = 4 \times 2 = 2 \times 2 \times 2$

$\phi(8) \Rightarrow 4$

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

$\phi(6) = \{1, 5\}$

no. of elements in these sets is the totient funⁿ.

Note :-

Two integers a, b are said to be relatively prime, mutually prime or co-prime if the only the integer/factor that divides both of them is 1.

"n" should be +ve".

PAGE NO.:
DATE

$\phi(10) = 1, 3, 7, 9$

Note ① $\phi(n)$ for $[n \geq 1]$ is ~~desig~~ defined as the no. of all the +ve integers less than 'n' that are coprime to 'n'.

Imp

not zero ② coprime to 'n' :-

$\boxed{\text{GCD of those two no.} = 1}$

$\phi(n) \Rightarrow$

$\phi(5) \Rightarrow \underbrace{\{1, 2, 3, 4\}}$ — ④

no. of elements in these sets is the totient funⁿ.

$\phi(6) = \{1, 5\}$ — ②

PAGE NO.:
DATE

Note

(11) When 'n' is a prime number :-

$\phi(n) = n-1$;

$\phi(23) = 23-1$

$= 22$

Note

$\phi(a * b) = \phi(a) * \phi(b)$

$\phi(35) = \phi(7 * 5)$

$= \underbrace{\phi(7)}_{(n-1)(7-1)} * \underbrace{\phi(5)}_{(n-1)=(5-1)}$

$= 6 * 4$

$\boxed{\phi(35) = 24}$

[gcd (7,5) = 1]

What is the greatest common divisor of 24, 30, 36 ?

2	24	30	36
3	12	15	18
	4	5	6

a) 2
b) 6
c) 8
d) 12

$2 \times 3 = \boxed{6}$

PAGE NO.:
DATE

GCD (12, 15)

$12 = 2 \times 6$
$= 2 \times 2 \times \underline{\underline{3}}$

$15 = 3 \times 5$
$= \underline{\underline{3}} \times 5 \times 1$

GCD = 3

$12 = 2 \times 6$
$= \underline{2} \times 3 \times \underline{2}$
$\downarrow \quad \downarrow$
$2 \quad 2$

$32 = 2 \times 16$
$= 2 \times 2 \times 8$
$= 2 \times 2 \times 4 \times 2$
$= \underline{2} \times \underline{2} \times 2 \times 2 \times 2$
$\downarrow \quad \downarrow$
$2 \quad 2$

$2 \times 2 = 4$

GCF of 12 and 32 is 4

—x—

1 to 100

Prime No. 2, 3, 5, 7, 11, 13, 17, 9, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Relatively prime :- 4 15
(1, 2, 4) (1, 3, 5)

gcd(4, 15) = 1

PAGE NO.:
DATE

CO- Prime

35, 39 $\rightarrow$

35 $\rightarrow 5 \times 7 \times \boxed{1}$

39 $\rightarrow 3 \times 13 \times \boxed{1}$

$\rightarrow$ 1 as common factor.

$\therefore$ 35 & 39 is co-prime.

Prime :- 2, 3, 5, 7, 11, 13, 17,

co-prime :- (2, 3) (5, 7)

2×1 3×1 5×1 7×1

1 1 1

co- prime no :-

If two numbers have only 1 as their common factor, then they are called co-primes.