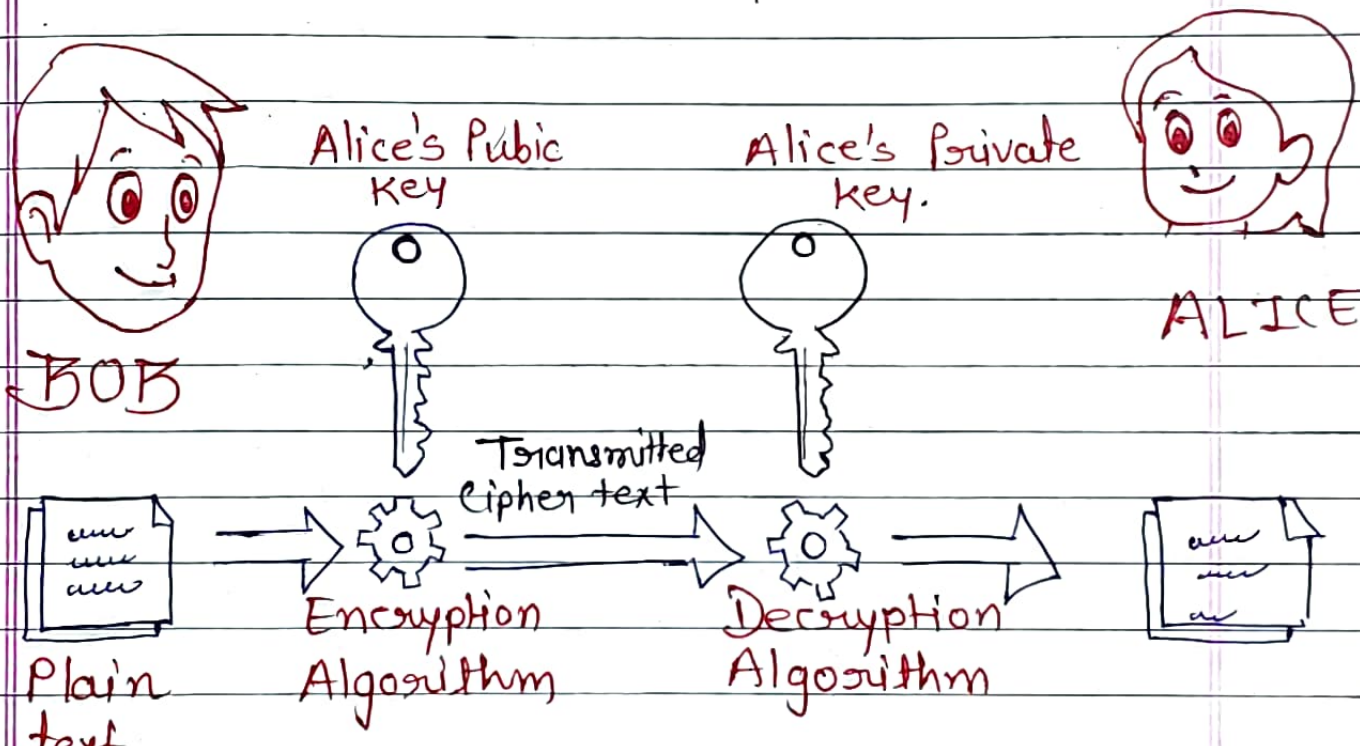
⇒ Public key Cryptography.

Symmetric Cryptography:
Same key used by Sender & Receiver

Asymmetric Cryptography:
Different key used by Sender & Receiver, public key → encryption
(secret) private key → Decryption.



Conventional Encryption	Public key Encryption.
Same Algorithm	Different Algorithm
Same key	Different key.
key is kept Secret	One of the key is secret
Faster	Slower.
classical Cryptosystem	RSA, Diffie-Hellman, ECC Rabin cryptosystem.

✡ Applications of Public-key Cryptosystems

Algorithm.	Encryption / Decryption	Digital signature	Key Exchange
RSA	✓	✓	✓
ECC	✓	✓	✓
Diffie-Hellman	×	×	✓
DSS.	×	✓	×

Modular Exponentiation

⇒ it is a type of exponentiation performed over a modulus.

⇒ $a^b \bmod m$ or $a^b \pmod m$.

⇒ $a \bmod m$ ⇒ if $m > a$ ans is a itself

Examples:

(1) $23^3 \bmod 30$

$23 \bmod 30 = -7$

or

23

So replace 23 with -7

$-7^3 \bmod 30$

$= -7^2 \times -7 \bmod 30$

$= 49 \times -7 \bmod 30$

$= -133 \bmod 30$

$= -13 \Rightarrow -13 + 30 = \boxed{17}$ ✓

using calculator

$\Rightarrow 23^{\wedge 3} = 12167$

$23^{\wedge 3} \bmod 30 = \frac{12167}{30}$

Remainder is 17 Ans

(2) Solve $31^{500} \bmod 30$

$30 \overline{)31}$ (1)

30

1 = Remainder

$\Rightarrow 1^{500} \bmod 30$

$\Rightarrow 1 \bmod 30$

$\Rightarrow \boxed{1}$ ✓

(3) $242^{329} \bmod 243$

$243 \overline{)242}$ (1)

243

-1 = Remainder

$\Rightarrow -1^{329} \bmod 243$

$\Rightarrow -1 \bmod 243$

$\Rightarrow -1 + 243 = \boxed{242}$ ✓

④ Solve $11^7 \bmod 13$.

$11 \bmod 13 = -2$

So, $-2^7 \bmod 13$

$-128 \bmod 13$

$-11 \Rightarrow -11 + 13 = 2$

when its negative add it to mod way value.
(13)

Imp ⑤ Solve $88^7 \bmod 187$

$88^1 \bmod 187 = 88$

(here -99 or 88 we are taking positive value for easy calculation otherwise both will give proper Answer)

$88^2 \bmod 187 = 88^1 \times 88^1 \bmod 187$

$= 88 \times 88 \bmod 187$

$= 7744 \bmod 187$

$= 77$

$88^4 \bmod 187 = 88^2 \times 88^2 \bmod 187$

$= 77 \times 77$

$= 5929 \bmod 187$

$= 132$

$88^7 \bmod 187 = (88^4 \times 88^2 \times 88^1) \bmod 187$

$= (132 \times 77 \times 88) \bmod 187$

$= 894432 \bmod 187$

$= 11$

⑥ What is the last two digits of 29^5?
When you divide a number with 100 Remainder will give you last two digits

So, $29^1 \bmod 100 = 29$ or -71
Taking smaller value bcoz multiplicat" is easier

$29^2 \bmod 100 = 29^1 \times 29^1 \bmod 100$
$= 29 \times 29 = 841 \bmod 100$
$= 41$ or -59

$29^4 \bmod 100 = 29^2 \times 29^2 \bmod 100$
$= 41 \times 41 \bmod 100$
$= 1681 \bmod 100$
$= 81$ or -19
↳ Taking smaller value for easy multiplicat"

$29^5 \bmod 100 = (29^4 \times 2^1) \bmod 100$
$= -19 \times 29 \bmod 100$
$= -551 \bmod 100$
$= -51 \bmod 100 = -51$
$= \boxed{49}$ ✓

The RSA Algorithm

⇒ Public key encryption

⇒ Ron Rivest, Adi Shamir, and Leonard Adleman

⇒ Block cipher with variable block size.

⇒ Plaintext and ciphertext are integers between 0 and n-1 for some 'n'

⇒ A Typical size for 'n' is 1024 bits or 309 decimal digits. but it may not be the same in all cases

⇒ only public keys are shared and private keys are kept secret

⇒ The RSA Algo :-

⇒ Select prime numbers P, q such that $P \neq q$ larger the number higher the Security.

⇒ Calculate $n = P \times q$, n is an Integer

⇒ calculate $\phi(n) = (P-1)(q-1)$.

⇒ Select Integer 'e' such that

$GCD(\phi(n), e) = 1$ & $1 < e < \phi(n)$

e should be relatively prime to $\phi(n)$ so, they will be rel. prime if they have only one common factor 1.

Public key

⇒ Calculate d such that $e \times d \equiv 1 \bmod \phi(n)$.

if $\frac{e \times d}{\phi(n)}$ will get Remainder 1

Private key

So, d is multiplicative Inverse of e & e is multiplicative Inverse of d

⇒ Public key $PU = \{e, n\}$

⇒ Private key $PR = \{d, n\}$

⇒ Suppose this Algo is actually performed by Alice

⇒ Alice will share Pubic key with bob.

Encryption by Bob. using Alice's Public key.	Decryption by Alice. using Alice's Private key
Plaintext : $M < n$	Ciphertext : C
Cipher text : $C = M^e \bmod n$	Plaintext : $M = C^d \bmod n$

Example :→ Perform Encryption for the plaintext 20 using RSA Algorithm with the values $P=5$, $q=11$, 13 as the public key.

plaintext = $M = 20$

St - 1 prime numbers $P = 5$, $q = 11$ such that $P \neq q$.

St - 2 calculate $n = 5 \times 11 = 55$

St - 3 calculate $\phi(n) = \phi(P\,q) = (5-1)(11-1) = 40$

St - 4 Select integer $e = 13$ such that

$GCD(40, 13) = 1$ & $1 < 13 < 40$

Calculate 'd' such that $13 \times d \equiv 1 \bmod 40$

⇒ find multiplicative inverse of 13 mod 40 = d.

Q	A	B	R	T_1	T_2	T	A > B
3	40	13	1	0	1	0-1×3 = -3	40 13
							$T_1 = 0$ $T_2 = 1$
13	13	1	0	1	-3	1-(-3)13 = 40	$T = T_1 - T_2 \times Q$
1	0				-3	40	

Q = 3, 13 | 40, 39, R = 1

Q = 13, 1 | 13, R = 0

M.I of 13 mod 40 = -3, it negative

add -3 to 40 = 37 ⇒ d = 37

calculate d such that $13 \times 37 \equiv 1 \bmod 40$

$481 \equiv 1 \bmod 40$

$\frac{481}{40}$ = Remainder is 1

public key $PU = \{13, 55\}$

private key $PR = \{37, 55\}$

⇒ Encryption by bob using Alice's Publickey

plaintext : $M < n$

$20 < 55$

Cipher text : $C = 20^{13} \bmod 55 = 25$

⇒ $20^{13} \bmod 55$

$20 \bmod 55 = -35$ or 20

$20^2 \bmod 55 = 20^1 \times 20^1 \bmod 55$

$= 20 \times 20 \bmod 55$

$= 400 \bmod 55$

$= 15$

$20^4 \bmod 55 = 20^2 \times 20^2 \bmod 55$

$= 15 \times 15 \bmod 55 = 225 \bmod 55$

$= 5$

$20^8 \bmod 55 = 20^4 \times 20^4 \bmod 55$

$= 5 \times 5 \bmod 55 = 25 \bmod 55$

$= -20$ or 25

$20^{13} \bmod 55 = (20^8 \times 20^4 \times 20^1) \bmod 55$

$= (25 \times 5 \times 20) \bmod 55$

$= 2500 \bmod 55$

$= 25$

⇒ Decryption by Alice using Alice's Private key.

Ciphertext : $C = 25$

plaintext : $M = 25^{37} \bmod 55 = 20$

$C^d \bmod n$

$\Rightarrow 25^{37} \bmod 55$

$25 \bmod 55 = 25$

$25^2 \bmod 55 = 25^1 \times 25^1 \bmod 55$

$= 25 \times 25 \bmod 55$

$= 625 \bmod 55 = 20$

$25^4 \bmod 55 = 25^2 \times 25^2 \bmod 55$

$= 20 \times 20 \bmod 55$

$= 400 \bmod 55 = 15$

$25^8 \bmod 55 = 15 \times 15 \bmod 55$

$= 225 \bmod 55$

$= 5$

$25^{16} \bmod 55 = 5 \times 5 \bmod 55$

$= 25 \bmod 55 = 25$

$25^{32} \bmod 55 = 25 \times 25 \bmod 55 = 20$

$25^{37} \bmod 55 = (25^{32} \times 25^4 \times 25^1) \bmod 55$

$= (20 \times 15 \times 25) \bmod 55$

$= 7500 \bmod 55 = 20$

RSA Algo

Example 2: perform Encryption for the plaintext 88 using RSA algorithm with the values: $p = 17$, $q = 11$ and $e = 7$

→ Select prime numbers $p = 17$, $q = 11$ such that $p \neq q$

→ Calculate $n = 17 \times 11 = 187$

→ Calculate $\phi(n) = \phi(pq) = (17-1)(11-1) = 160$

→ Select integer '$e = 7$' such that

$GCD(160, 7) = 1$ & $1 < 7 < 160$

→ Calculate 'd' such that

$$7 \times d \equiv 1 \bmod 160$$

⇒ Find 'Multiplicative inverse of $7 \bmod 160 = d$

$22 = 7\overline{)160}$, $14 = 20$, $14 = 6$, $1 = 6\overline{)7}$, $6 = 6$, $1 = 1\overline{)6}$, $6 = 6$, 0

Q	A	B	R	T_1	T_2	T	A > B
22	160	7	6	0	1	$0-1\times22$ -22 $1-22\times1$	160 ~~160~~ 7
1	7	6	1	1	-22	$+23$ $-22-23\times6$	$T_1 = 0$, $T_2 = 1$
6	6	1	0	-22	23	-160	$T = T_1 - T_2 \times \phi$
	1	0		23	-160		

$$\boxed{d = 23}$$

Public key $PU = \{7, 187\}$

Private key $= \{23, 187\}$

Encryption by bob using Alice's Public key.

$M < n$

Plaintext : $88 < 187$

$M^e \bmod n$.

Ciphertext : $C = 88^7 \bmod 187 = 11$

(Solved before in Modular exponentiation)

Decryption by Alice using Alice's Private key.

ciphertext : $C = 11$

$C^d \bmod n$

plaintext: $M = 11^{23} \bmod 187 = 88$

$\Rightarrow 11^{23} \bmod 187$

$\rightarrow 11 \bmod 187 \Rightarrow 11$

$11^2 \bmod 187 = 11 \times 11 \bmod 187$

$= 121 \bmod 187$

$= 121$

$11^4 \bmod 187 = 121 \times 121 \bmod 187$

$= 14641 \bmod 187$

$= 55$

$11^8 \bmod 187 = 55 \times 55 \bmod 187$

$= 3025 \bmod 187 = 33$

$11^{16} \bmod 187 = 33 \times 33 \bmod 187$

$= 154$

$11^{23} \bmod 187 = (11^{16} \times 11^4 \times 11^2 \times 11^1) \bmod 187$

$= (154 \times 55 \times 121 \times 11) \bmod 187$

$= 88$

RSA Algo (GATE CS 2019)

Example 3: In the RSA Public key Cryptosystem, the Private and public keys are (e,n) and (d,n) respectively, where $n = p \times q$ and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that $0 < M < n$ and $f(n) = (p-1)(q-1)$. Now consider the following equations:

I. $M' = M^e \bmod n$
$M = M'^d \bmod n$

Confidentiality is not achieved because msg is encrypted using private key & decrypted using public key anyone in the world can decrypt but it is still valid because authentication is achieved (this is opposite to original RSA)

II. $ed \equiv 1 \bmod n$.

III. $ed \equiv 1 \bmod f(n)$

IV. $M' = M^e \bmod f(n)$
$M = (M')^d \bmod f(n)$

Which of the above equations correctly represent RSA Cryptosystem?

a. I and II
b. I and III ✓ Ans
c. II and IV
d. III and IV

RSA Algo) (GATE CS-2017)

Example 4 :- In RSA Cryptosystem, a participant A uses two prime numbers $P=13$ and $q=17$ to generate her public and private keys. If the public key of A is 35, then the private key of A is _____

a. 11 ✓
b. 13
c. 16
d. 17

Given data	Select prime numbers.
$P=13$	$P=13$, $q=17$, $P \neq q$
$q=17$	calculate $n = 13 \times 17 = 221$
$e=35$	calculate $\phi(n) = \phi(pq)$
$d=?$	$= (13-1)(17-1) = 192$

Select integer $e=35$ such that

$GCD(192, 35) = 1$ & $1 < 35 < 192$

Calculate d such that $35 \times d \equiv 1 \bmod 192$

35 | 192

M.I. of $35 \bmod 192$

ϕ	A	B	R	T_1	T_2	T
5	192	35	17	0	1	$0-1\times5 = -5$
2	35	17	1	1	-5	$1-(-5)2 = 11$
17	17	1	0	-5	11	$-5-11\times17 = -192$
	1	0		11	-192	

A > B
192 35

$T = T_1 - T_2 \times \phi$

$d = 11$

public key = $\{e, n\} = \{35, 192\}$

private key = $\{d, n\} = \{11, 192\}$

Short cut :-

$$35 \times d \equiv 1 \bmod 192$$

$\frac{35 \times d}{192}$ will give Remainder 1

So, try all options & you will get the value of d.

(Gate CS 2019)

⇒ Example 5 :→ In an RSA cryptosystem The value of the public modulus parameter is 3007. if it is also known that $\phi(n) = 2880$, where $\phi()$ denotes Euler's totient function, then the prime factor of n which is greater than 50 is ____

Given Data

$n = 3007$

$\phi(n) = 2880$

Please note:

$n = pq.$

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

$n = pq = 3007$ —— (1)

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

$= pq - p - q + 1$

$= pq - (p+q) + 1$

$2880 = 3007 - (p+q) + 1$

$(p+q) = 3007 - 2880 + 1$

$p + q = 128$

$p = 128 - q$ —— (2)

Substitute (2) in (1)

$q^2 - 128q + 3007 = 0 \Rightarrow$ find roots

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$\frac{128 \pm \sqrt{128^2 - 4 \times 1 \times 3007}}{2}$$

$$\frac{128 \pm 66}{2}$$

$$\frac{128+66}{2} \text{ & } \frac{128-66}{2}$$

97 & 31

Second Method :-

Prime numbers less than 50 are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 & 47.

Find a number (from above numbers) where $\frac{3007}{31}$ gives

Reminder 0

$$31 \overline{)3007} \quad 97$$

97 ← quotient is Ans.

Security of RSA Algorithm

RSA algorithm is vulnerable to below mentioned attacks.

1) Brute Force Attacks
2) Mathematical Attacks
3) Timing Attacks.
4) chosen ciphertext Attacks.

(1) Brute Force attack.
- → This involves trying all possible keys.
- → larger key space
- → larger number of bits in d, the better the : Security.

(2) Mathamatical attack.
- → $n = p \times q$ ⇒ Factoring n should be very difficult
- → 3 approaches to attacking RSA Mathematically.

1. Factor 'n' into two primes.
   This enables the calculation of ~~$\phi(n)$~~ $\phi(n) = (p-1)(q-1)$ which in turn helps to determine $ed \equiv 1 \bmod \phi(n)$ (e: public, d: private)
2. Determine $\phi(n)$ directly, without p & q
   This in turn helps to determine ~~$ed \equiv 1$~~ $ed \equiv 1 \bmod \phi(n)$
   (some attacks do this)
3. Determine d directly, without first determining $\phi(n)$

(3) Timing Attack :→

Running time of the decryption Algo gives some clue about key & also some other info.

To deal with this.
Counter measures:

1) constant exponentiation time.
   All exponentiation func^{n}s takes same time.
2) Random delay.
   adding delay to exponentat^{n} fu^{n} to confuse attacker.
3) Blinding.
   Instead of directly giving CT To the algo add a Random number to the CT

(4) Chosen Ciphertext Attacks.

⇒ CCA

⇒ Vulnerable to a chosen CT.
PT ↔ CT Pairs will be available to attacker.

⇒ sol^{n} :→
Sophesticated CCAs
Add. Random Padding to algo to provide Security.

⇒ OAEP : optimal Asymmetric Encryption Padding Technique