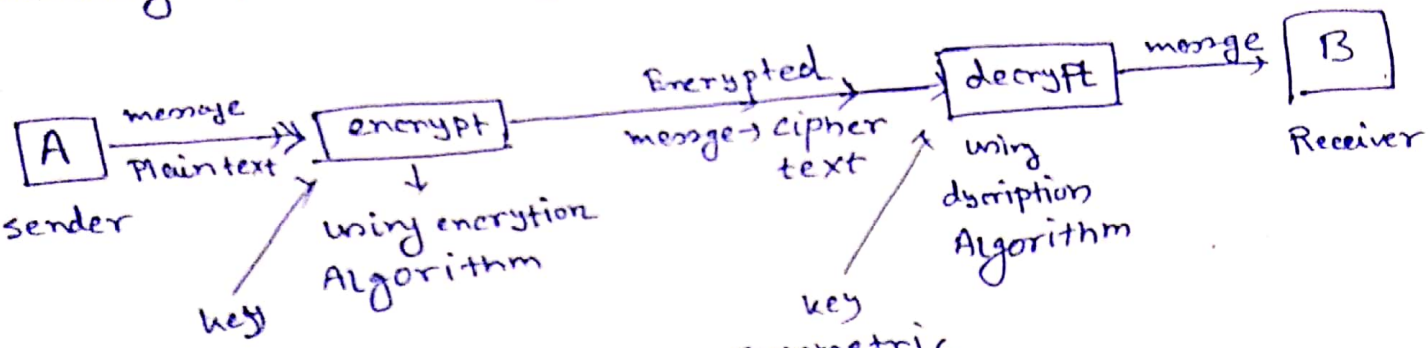
Cryptography

The art of protecting information by ~~is~~ transforming it into an unreadable format, that is called cryptography.

or

Method of protecting information and communication through the use of codes, so that only those for whom the information is intended can read and ~~decode~~ process it.

More general, cryptography is about constracting and analyzing protocols that prevent 3rd parties or the public from reading private message.



case :- (i) if keys are same → ~~Symetric~~ key cryptography

(ii) if keys are different → Asymmetric key .

Encryption :- process of trasforming information from readable to unreadable format

- Encryption Algorithms are used to encrypt the information / data.

~~De~~ Decrytion :- process of transforming data/information from unreadable - readable format.

- Decryption Algorithm are used to decrypt the data.

key :- String ~~the~~ of bits used by crytography Algorithm to transform, plain text → ciphar text or vice versa.

It is used for ~~security~~ secure communication.

DSA

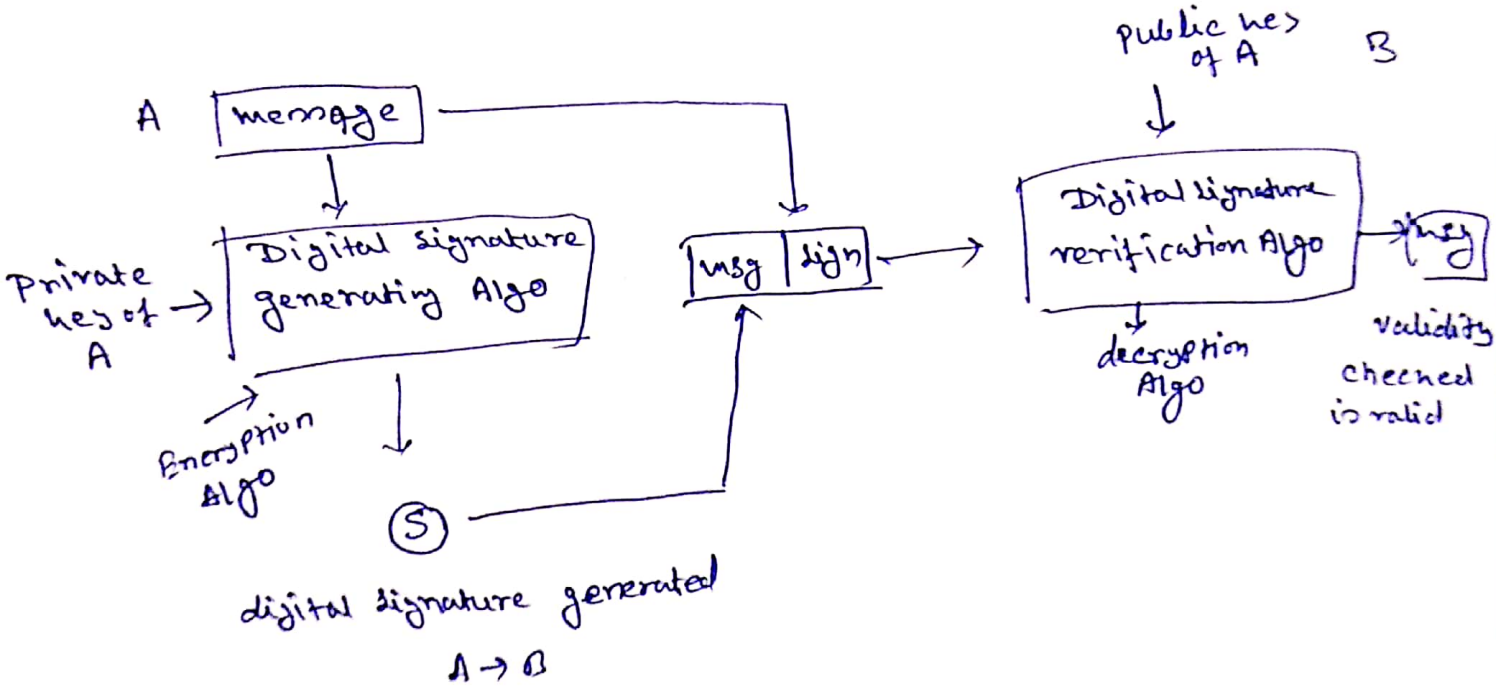
1) What is Digital signature :-

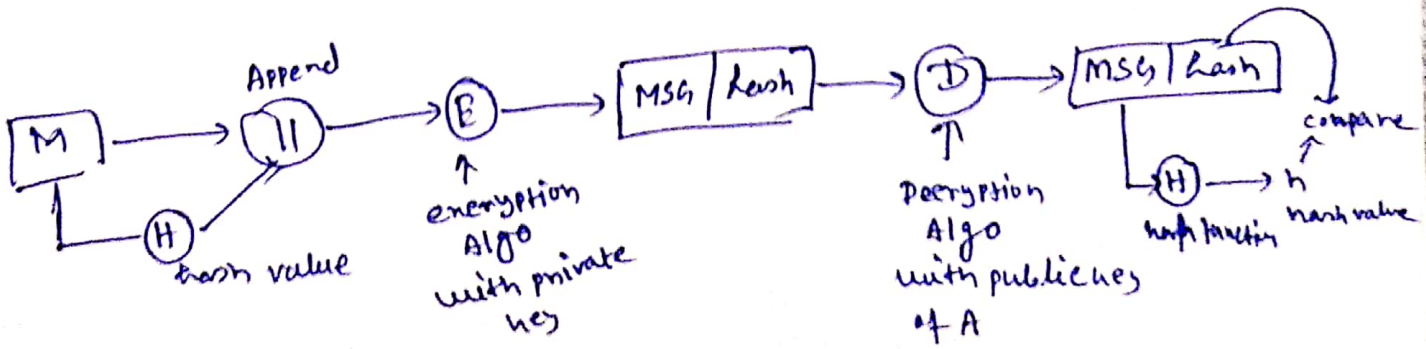
⇒ A digital signature is a mathematical technique used to validate the authenticity, non-repudiation and integrity of a message, software or digital document.

* Digital signature does not provide confidentiality.

→ Based on asymetric key cryptography.

Encryption with → private key
Decryption with → public key



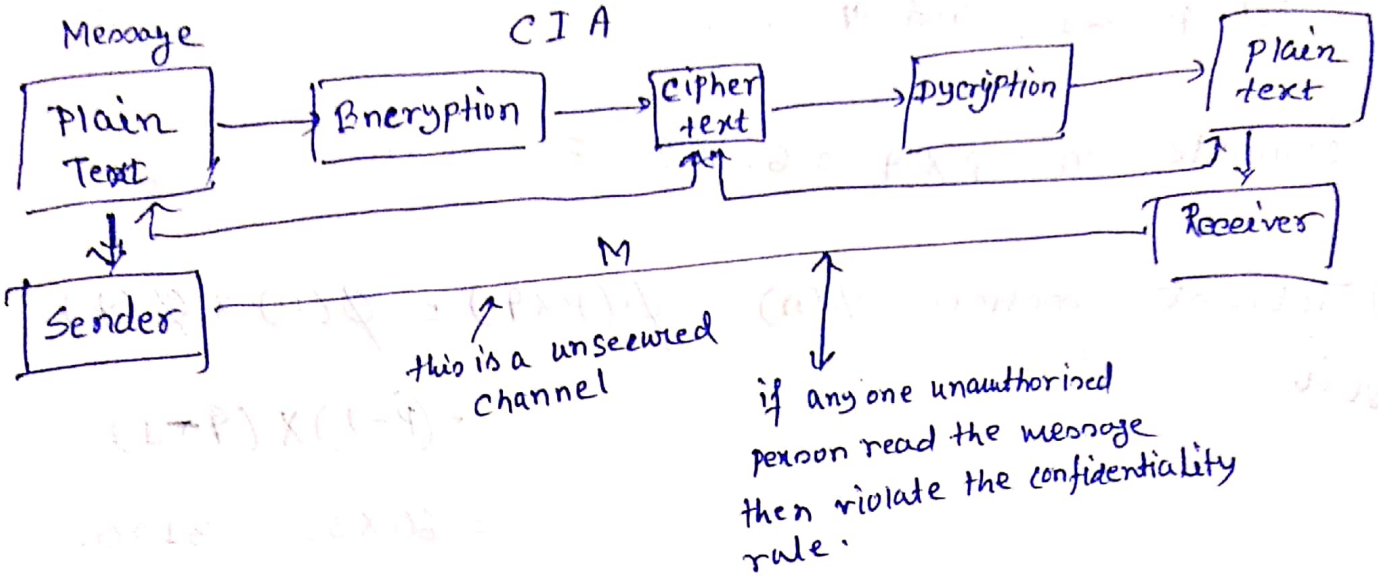


H → Hash function
h → hash code
(||) → append

Note :- The signature must use some info unique to the sender to prevent both forgery & denial.

RSA Algorithm (Rivest, Shamir, Adleman)

cryptography → confidentiality



** 'Asymmetric key' or "public key" (RSA)

public, private key.

if encryted the message using publickey then decryted the message in private key and vice versa at both end (sender or receiver)

Algorithm

1. Choose two different large random prime NO.
2. calculate $n = p * q$ [n = modulus, of p x q]
3. calculate $\phi(n) = (p-1) * (q-1)$ [$\phi(n)$ = totient function]
4. Choose 'e' such that $1 < e < \phi(n)$

   e is co-prime to $\phi(n)$, $\gcd(e, \phi(n)) \equiv 1$
5. calculate d, such that $de \equiv 1 \mod \phi(n)$
6. public key 'e' prirate key 'd'

Explanation

① Choose 2 prime nos, P & Q.

Let P = 61, and Q = 53.

② compute $n = P \times Q = 61 \times 53 = 3233$.

③ Totient function $\phi(n) = \phi(P \times Q) = \phi(P) \times \phi(Q)$

$= (P-1) \times (Q-1)$

$= 60 \times 52 = 3120$.

④ choose 'e', $1 < e < \phi(n)$, coprime to $\phi(n)$

Let $e = 17$, $\gcd(17, 3120) = 1$

(e, n) = public key = $(17, 3233)$

⑤ Determine 'd' as $ed \equiv 1 \bmod \phi(n)$

$d = e^{-1} \bmod \phi(n)$ (d is multiplicative Inverse (MI) of e), when e and $\phi(n)$ is co-prime.

$\therefore 17 \times d = 1 \bmod 3120$

$d = 2753$

$\therefore (d, n)$ = private key = $(2753, 3233)$.

Example:- How to calculate 'd'.

$\Rightarrow ed = 1 \bmod \phi(n)$ [if e and $\phi(n)$ its are co-prime, then d is a multiplicative Inverse of e.]

$$d = \frac{(\phi(n) \times i) + 1}{e}$$ [here i is a integer, $i = 1, 2, 3, \ldots$

$\therefore$ when $i = 1$, $d = \frac{(3120 \times 1) + 1}{17}$ [$\phi(n) = 3120$, $i = 1$, $e = 17$]

$= 183.58$ [we can not take the value, if the result is floating point value]

$\therefore i = 2$, $d = \frac{(3120 \times 2) + 1}{17} = 367.11$

$\vdots$

$i = 15$, $d = \frac{(3120 \times 15) + 1}{17} = 2753$

RSA Algorithm for Encryption and Decryption :-

Encryption $(\overset{e}{13}, \overset{n}{143})$

$C = P^e \bmod n$; $P < n$ [P should be less then n, P = plain text]

let $P = 13$

$\therefore C = 13^{13} \bmod 143$

↓ simplify this equation

cipher text

- $13 \bmod 143 = 13$
- $13^4 \bmod 143 = 104$
- $13^8 \bmod 143 = 91$

$\therefore C = [(13^8 \bmod 143)(13^4 \bmod 143)(13 \bmod 143) \bmod 143]$

$= (91 \times 104 \times 13) \bmod 143$

$C = 52$ [this is a cipher text]

Decryption $(\overset{d}{37}, \overset{n}{143})$

$P = C^d \bmod n$

Plain text / Cipher text

$= 52^{37} \bmod 143$ [$c = 52$, $d = 37$, $n = 143$]

↓ simplified

- $52 \bmod 143 = 52$
- $52^4 \bmod 143 = 26$
- $52^{32} \bmod 143 = 130$

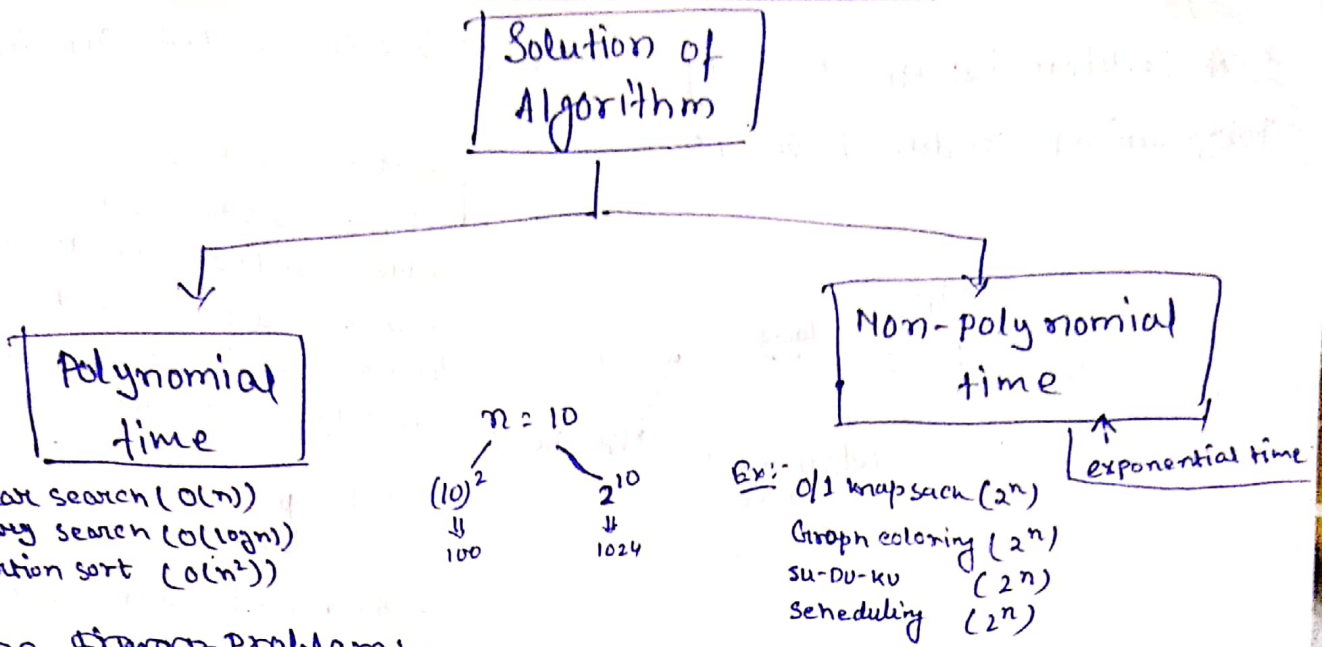
$P = [(52^{32} \bmod 143)(52^4 \bmod 143)(52 \bmod 143) \bmod 143]$

$= (130 \times 26 \times 52) \bmod 143$

$= 13$

$\therefore \boxed{P = 13}$ $\boxed{C = 52}$

P, NP, NP-Hard, NP-complete



P class problem:-

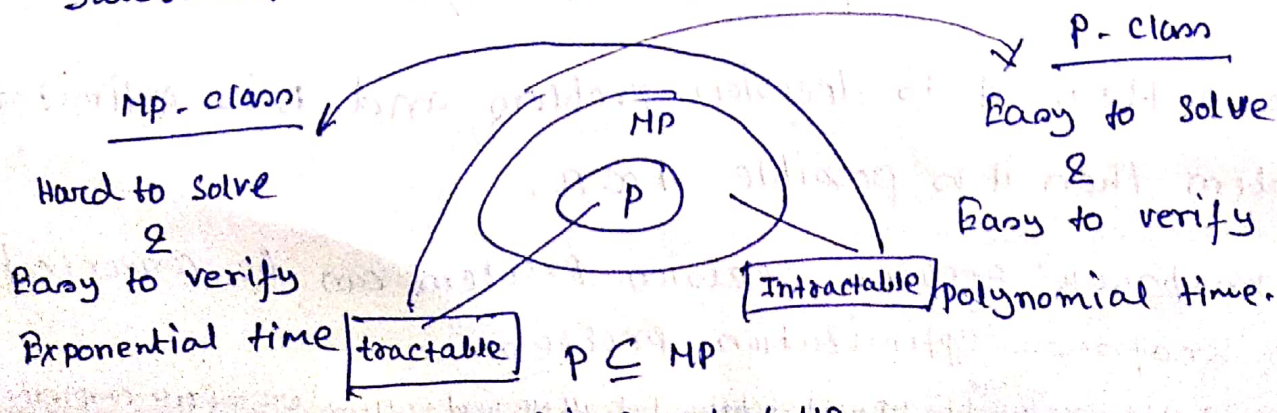
⇒ A problem which can be solved polynomial time know as P class problem.

Ex:- All Sorting and searching ~~problem~~ Algorithms.

NP class problem:

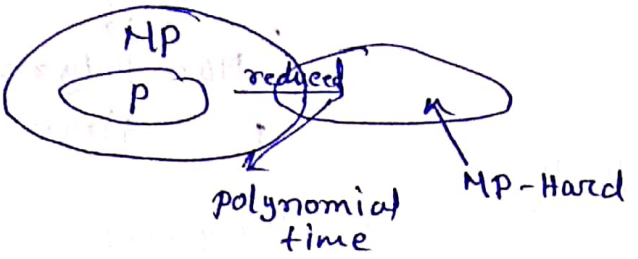
⇒ A problem which cannot be solved on polynomial time but is verified in polynomial time is known as non-deterministic polynomial or NP-class problem.

Ex:- Su-do-ku, prime factor, ~~the~~ Scheduling, Travelling Salesman.



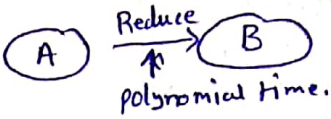
NP- Hard problem:-

⇒ A problem is NP- Hard if every problem in NP can be Polynomial reduced to it.



What is Reduction:-

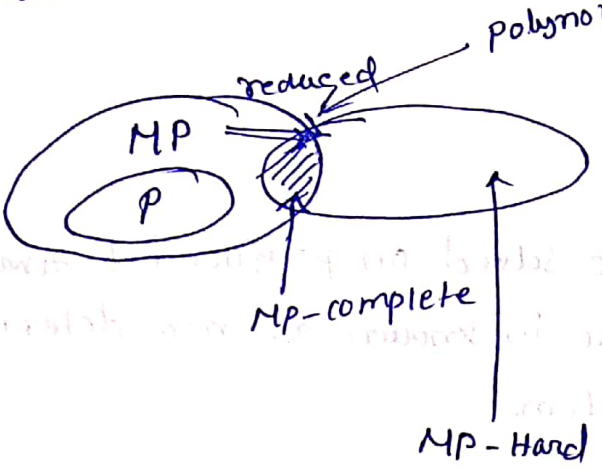
Let A & B are two problems, then Problem A reduce to problem B, ~~iff~~ if there is a ways to solve A by deterministic algorithm that solve B in polynomial time.



if A is reducible to B and B in P then A in P.

NP- complete:-

A problem is NP- complete if it is ~~is~~ in NP and it is NP- Hard.



The class of NP- complete problem is the intersection of the NP and NP- Hard class.

NP complete problem : Decision problem

NP Hard problem : optimization problem.

* if a problem A is decision problem and B is optimization problem then it is possible A ∝ B.

Ex:- knapsack ~~problem~~ Decision problem can be converted to knapsack optimization problem.

* All NP complete problem ~~reduced to~~ are NP Hard ~~problem~~ but all NP Hard problems are not NP complete.