Books:

(a) Foundation of Cryptography - Vol-I.
Oded Goldreich.

(b) Introduction to Modern Cryptography.
Katz & Lindell.

(3) Research papers.

Evaluation: M (30) + E (50) + A (20)

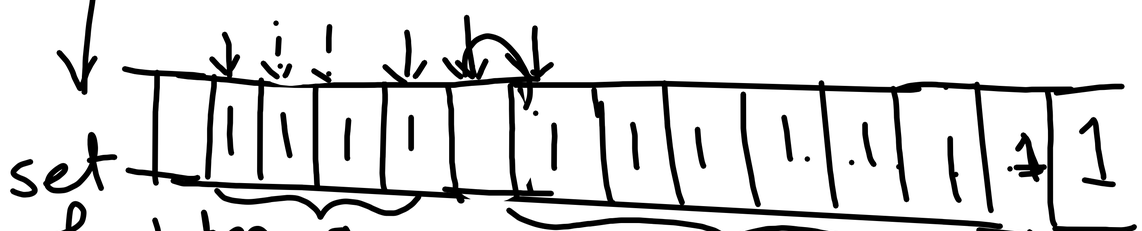
Turing Machine:

$\delta : Q \times \Sigma \times \Gamma \cup \{\square\}$

$Q \times \Gamma \times \{L, R\}$

A turing machine is a 6-tuple.

$(Q, \Sigma, \Gamma \cup \{L, R, \square\}, \delta, q_0, q_{acc}, q_{rej})$



Σ = input alphabet

↓

finite

q_{st}

q_1 q_2

$\Gamma \rightarrow$ tape alphabet

a b

4, 8

|||| |||||||

$w_1 = 101!$

$w_2 = 1100$

$w_3 = 0011\ 100$

$w_4 = 10101$

Design a TM that accepts all strings whose decimal equivalence is an even number.

$$L(M) = \{ w \in \{0,1\}^* : w \bmod 2 = 0 \}$$

Time Complexity:

P. Suppose the size of the problem instance I of P. is n.

T(n): time required to solve the problem instance I.

T(n) is a polynomial of n then the algorithm A solves P efficiently.

There exists a collection of problems $\{P_i\}$ such that for each P_i, $\exists$ an alg. A_i that solves P_i "efficiently"

Such collection is called the "P collection" / P- class.