1) Introduction to Modern Cryptography - Jonathan Katz and Yehuda Lindell. (3rd edition)

2) Cryptography Theory and practice - Douglas R. Stinson - (3rd edition).

3) A graduate course in applied cryptography. Dan Boneh and Victor Shoup - (draft version).

4) A computational Introduction to Number theory and Algebra - Victor Shoup - (2nd edition).

Weightage:

Mid-sem: 30%.

End-sem 60%.

Assignments 10%.

set of plaintext M

set of ciphertext C

$m_1 \rightarrow c$

$m_2 \rightarrow c$

$E \subseteq M \times C$

$E(m_1) = c$

$E = \{(m_1, c_1), (m_1, c_2), (m_3, c_2)\}$

E is a fn. $M \rightarrow C$

key - "k"

$E: K \times M \rightarrow C$

$D: K \times C \rightarrow M$

set of plaintext $\mathcal{M}$

set of ciphertext $\mathcal{C}$

$m_1 \rightarrow c$

$m_2 \rightarrow c$

$\mathcal{E} \subseteq \mathcal{M} \times \mathcal{C}$

$\mathcal{E}(m_1) = c$

$\mathcal{E} = \{(m_1, c_1), (m_1, c_2), (m_3, c_2)\}$

$\mathcal{E}$ is a fn. $\mathcal{M} \rightarrow \mathcal{C}$

$\mathcal{E} : K \times \mathcal{M} \rightarrow \mathcal{C}$

$\mathcal{D} : K \times \mathcal{C} \rightarrow \mathcal{M}$.

key - "K"

$\forall k \in K \;.\; \forall m \in M$, it holds that

$$D(k, E(k, m)) = m.$$

Symmetric

(PK_A, SK_A) Alice

(PK_B, SK_B) Bob

$C = E(pk_B, m)$

Public-key

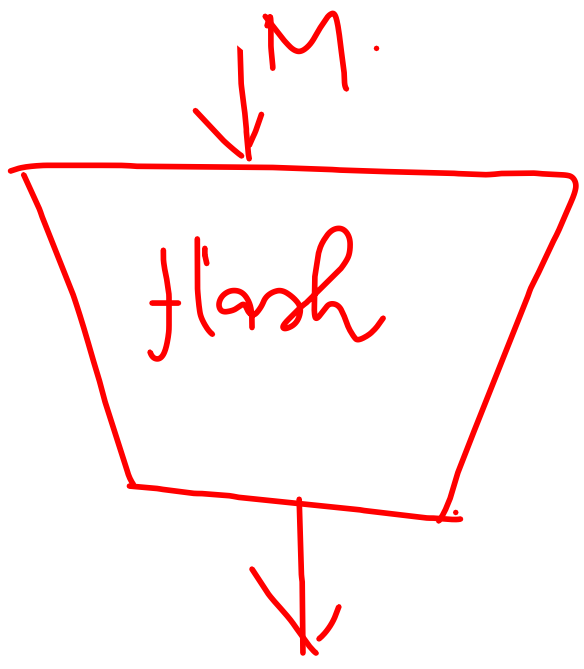
Each party will have a pair of keys.

(Public key., Private key)
||
Secret key.

$\forall (pk, sk) \in K$, $\forall m \in M$, it holds that

$$D(sk, E(pk, m)) = m$$

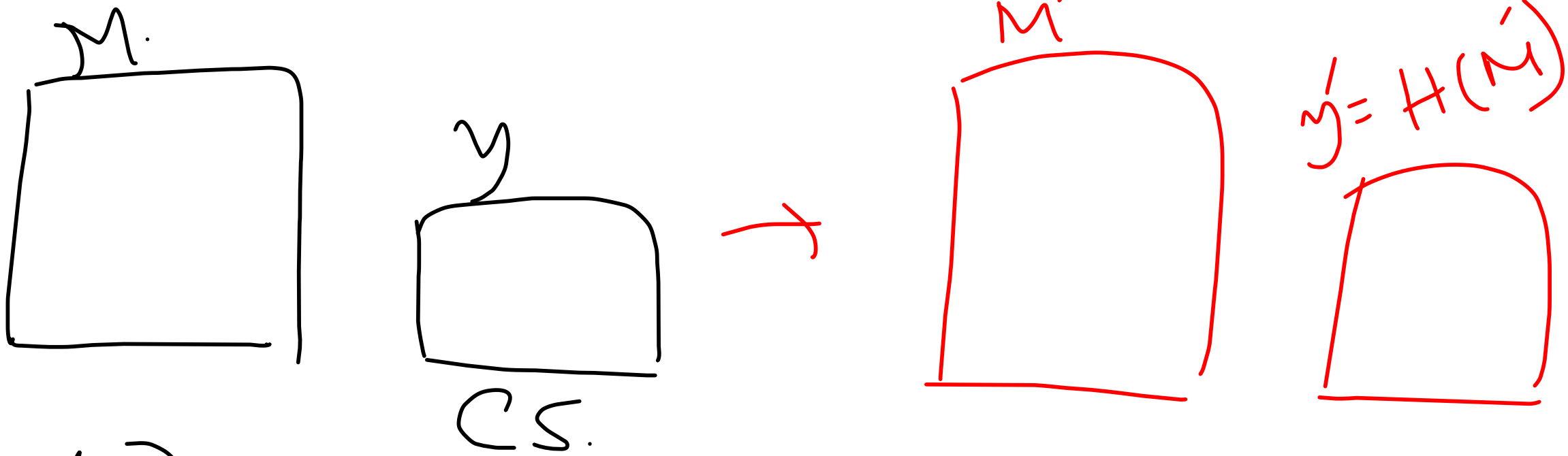
Hash Function:



@ Collision Resistance.

Infeasible to produce two messages $M_1 \neq M_2$ s.t

$$H(M_1) = H(M_2)$$



$y = H(M)$

Message Authentication Code (MAC).

① It preserves the integrity of the message.

② It ensures the authenticity.

Eve

Alice

Bob

m

$k \in K$

$Sign(m) = t$

(m, t)

$(1000, t)$

$t = Sign(k, 1000)$

$Verify(k, m, t)$

$= \begin{cases} 0 & \text{not accept} \\ 1 & \text{accept} \end{cases}$

$Sign(k, m) = Sign(k, m')$

Eve

Alice

Bob

m

$k \in K$

$Sign(m) = t$

(m, t)

(m', t')

$(10\,00, t)$

$t = Sign(k, 10,000)$

$Verify(k, m, t)$

$= \begin{cases} 0 & \text{not accept} \\ 1 & \text{accept} \end{cases}$

$Sign(k, m) = Sign(k, m')$

Authenticaled Encryption:

Integrity + Confidentiality

"Key-exchange algorithm"