

# Two Cryptography Systems

## I. Symmetric Key systems:

- $K_A$  = Alice's key; secret to Alice
- $K_{AB}$  = **Key shared** only by Alice and Bob
- Same key ( $K_{AB}$ ) used to both encrypt and decrypt a message

•E.g., DES (Data Encryption Standard): 56 b key operates on 64 b blocks from the message