Shared
secret key
K
Shared
secret key
K
Plaintext
P
Encryption
E()
Ciphertext
C=E(K,P)
Decryption
D()
Plaintext
P=D(K,C)