User A
Key 1
Plaintext
(Message)
Encryption
Ciphertext
Key 2
User B
Decryption
Plaintext
User C
(attacker)