SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

UNIT-2 NUMBER THEORY AND PUBLIC KEY CRYPTOSYSTEMS

Public key Cryptosystem

Asymmetric algorithms rely on one key for encryption and a different but related key for decryption.

Plaintext: This is the readable message or data that is fed into the algorithm as input.

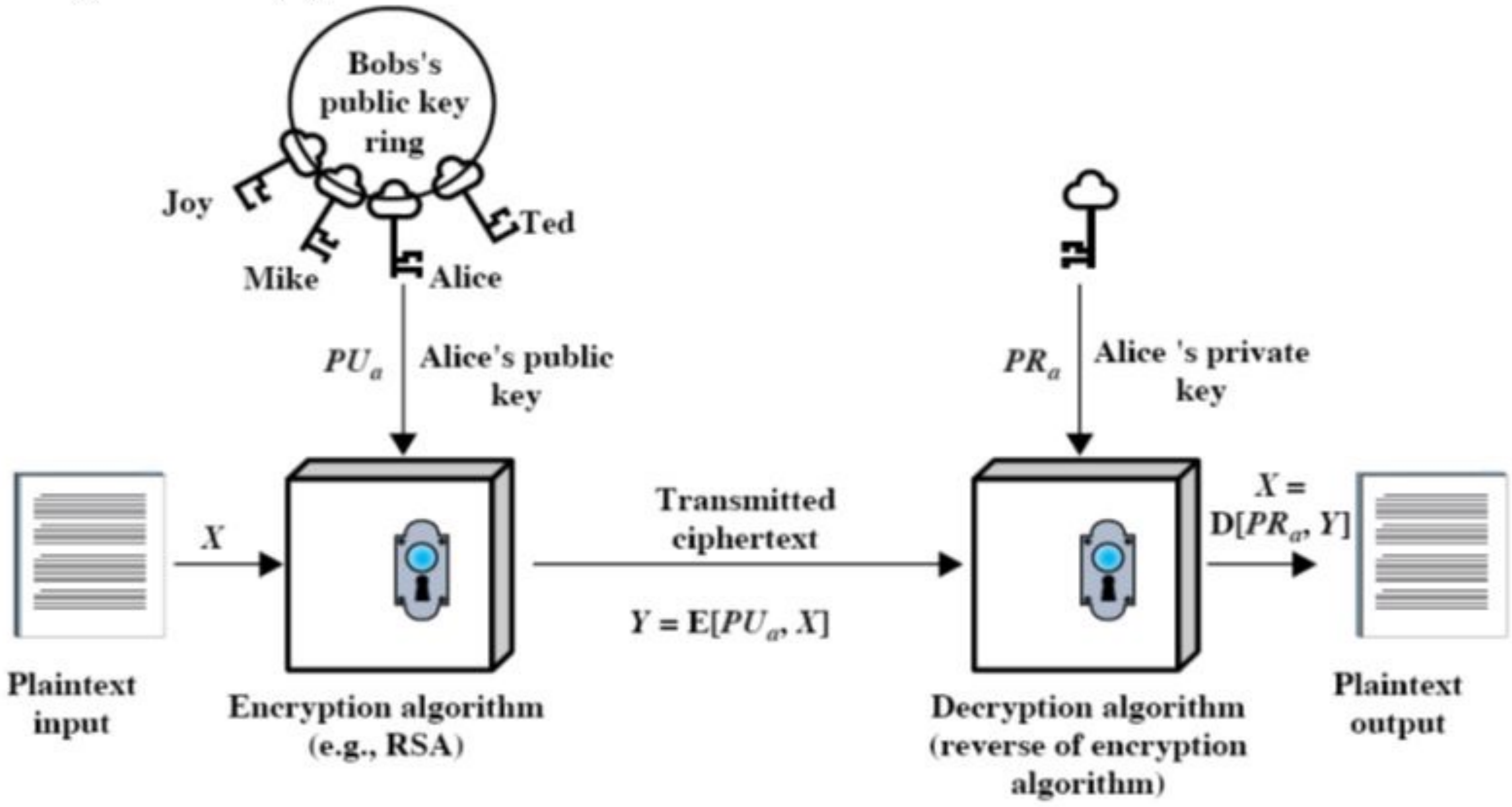
Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.

Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption

Ciphertext: This is the scrambled message produced as output.

Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. All participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed.



(a) Encryption

Sender:Bob **Receiver:Alice**

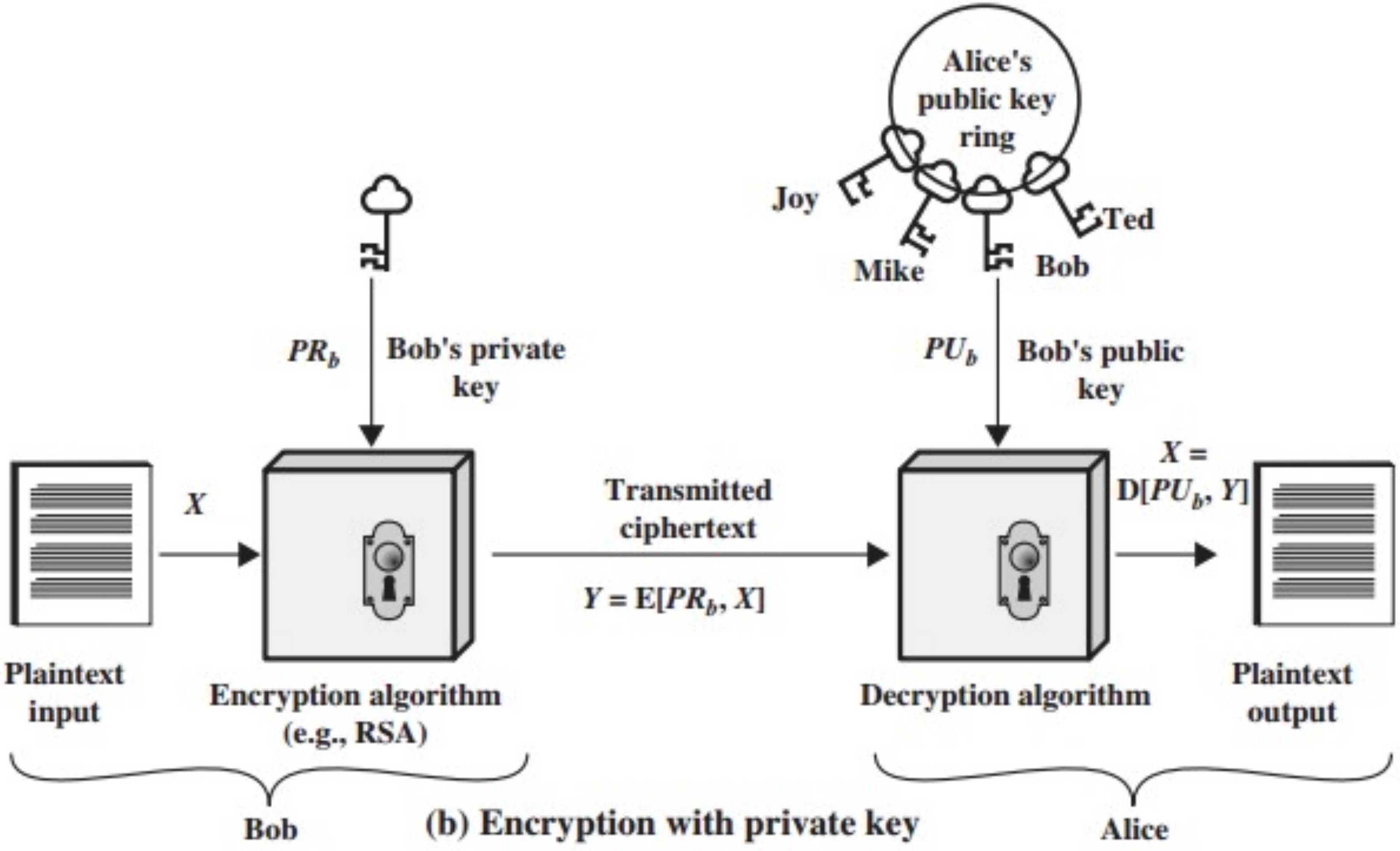


Figure 9.1 Public-Key Cryptography

Authentication

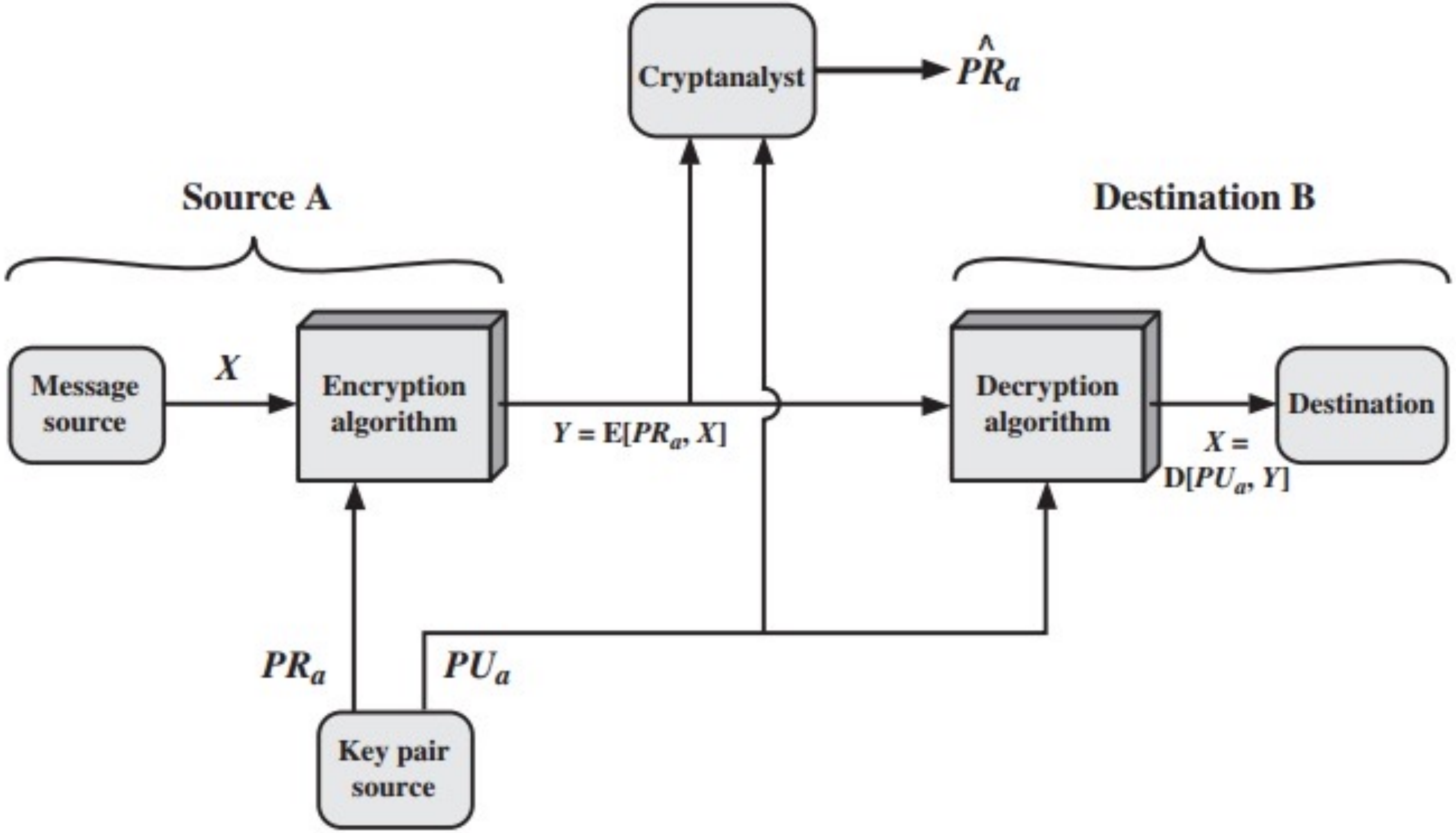


Figure 9.3 Public-Key Cryptosystem: Authentication

Confidentiality

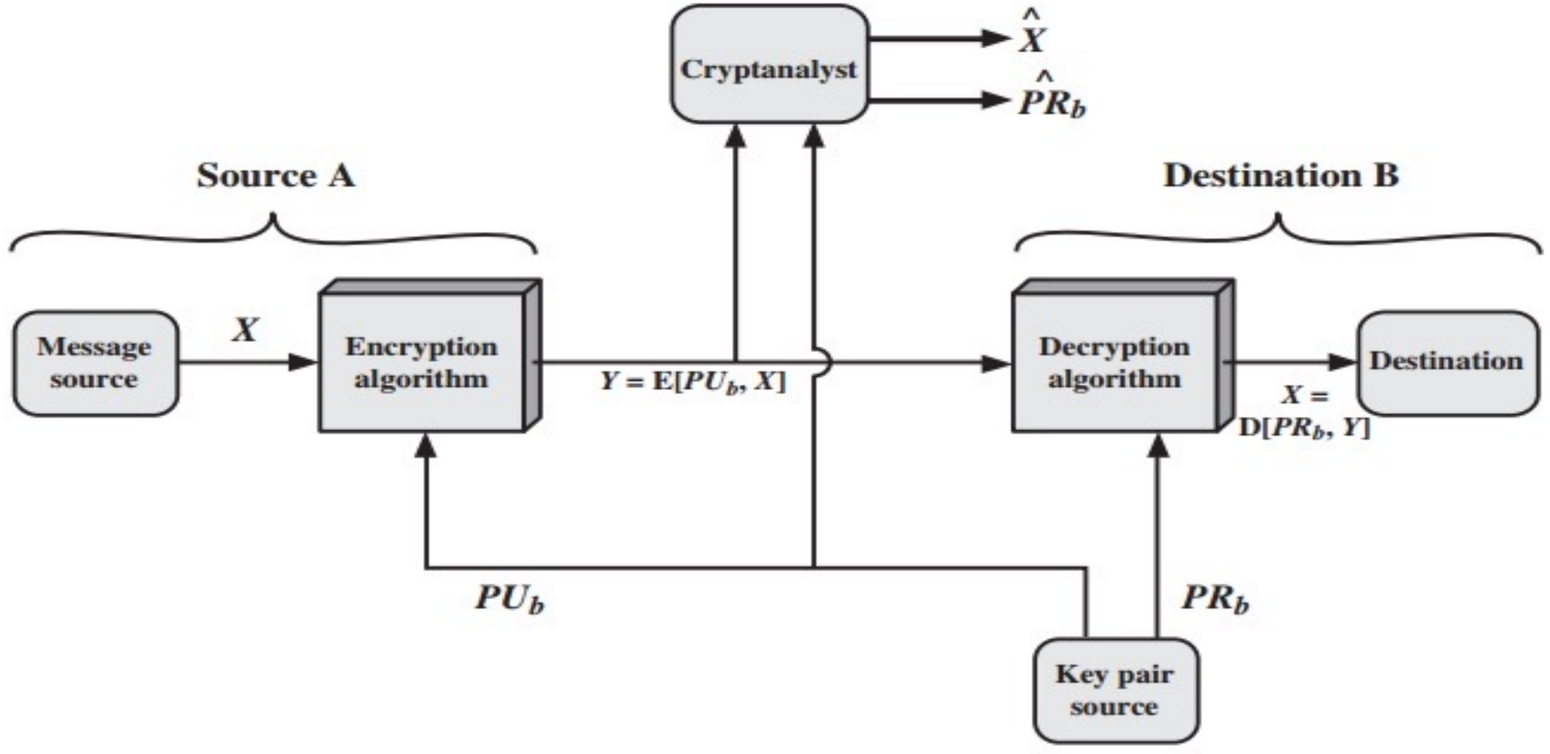


Figure 9.2 Public-Key Cryptosystem: Secrecy

Authentication and Confidentiality

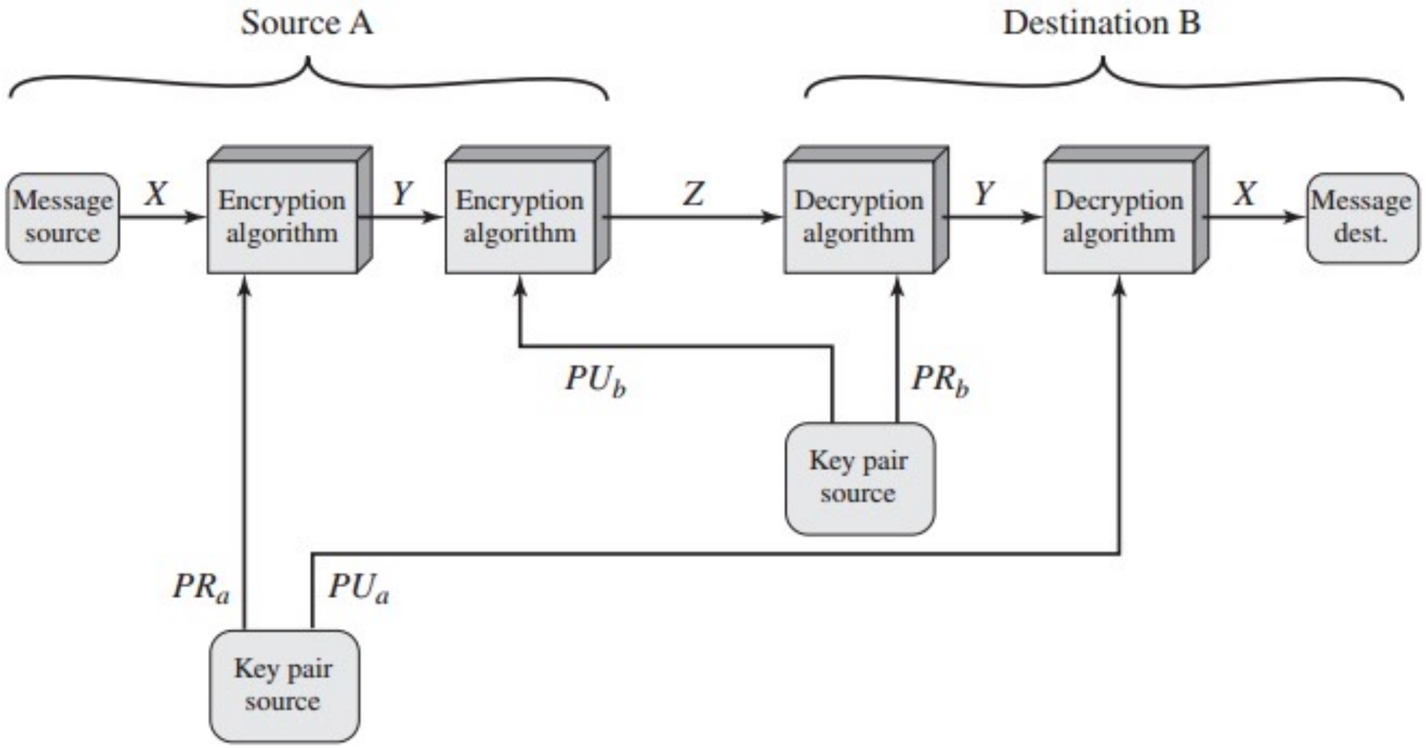


Figure 9.4 Public-Key Cryptosystem: Authentication and Secrecy

Z = E(PUb, E(PRa, X))
X = D(PUa, E(PRb, Z))