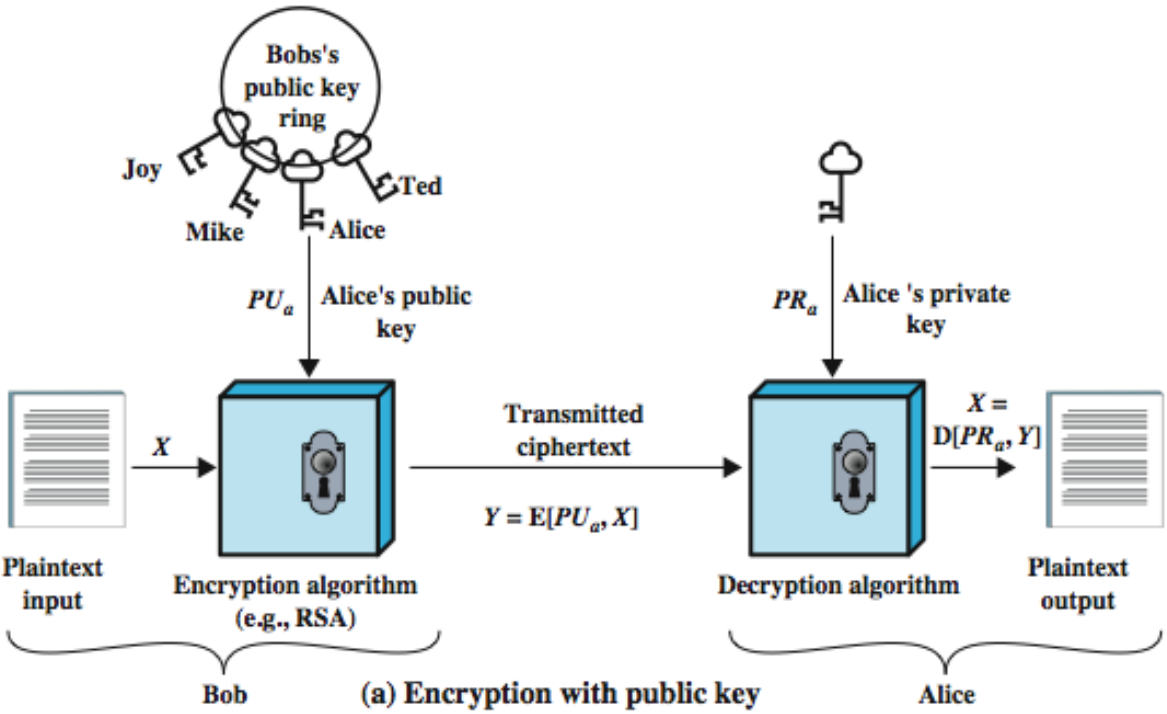
Private-Key Cryptography

- **Traditional private/secret/single-key cryptography uses one key**
- **Shared by both sender and receiver**
- **If this key is disclosed communications are compromised also symmetric, and parties are equal**
- **Hence does not protect the sender from the receiver forging a message & claiming it is sent by the sender**
- **Probably the most significant advance in the 3000-year history of cryptography**
- **Uses two keys – a public & a private key**
- **Asymmetric since parties are not equal**
- **Uses clever application of number theoretic concepts to function**
- **Complements rather than replaces private key crypto**



(a) Encryption with public key

Public-key algorithms rely on two keys where:

it is computationally infeasible to find the decryption key knowing only the algorithm & encryption key it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)