Public Key Cryptography

Public Key Cryptography

Outline

- Public Key Cryptography
- RSA Algorithm

Public Key Cryptography

- The development of Public Key (or Asymmetric) Cryptography is probably the most significant advancement in the 3000-year history of cryptography.
- It is based on ***mathematical functions*** rather than on simple operations such substitution and permutation on bit patterns.
- First publicly proposed by Whitfield Diffie and Martin Hellman in 1976 at Stanford University.
- It is asymmetric, involving the use of two separate keys, one for encryption and another for decryption operations.
- It complements the private key cryptography rather than replacing.

Misconceptions

- Public-key encryption is more secure from cryptanalysis than conventional encryption.
- Public-key encryption is a general-purpose technique that has made conventional encryption obsolete.

Recap on Symmetric Encryption

- Also called **Traditional/Conventional/Symmetric/Private/Secret/Single Key Cryptography**.
- It uses only one key for both encryption and decryption.
- The single key is shared by both the sender and the receiver.
- If this key is disclosed, the communications are compromised.
- This approach does not protect a sender from a receiver forging a message and claiming it is sent by the sender.

Difficulties related to Symmetric Encryption

Problem 1: How the secret key can be distributed between the sender and the receiver in the first place (Key Distribution)?

Solutions:

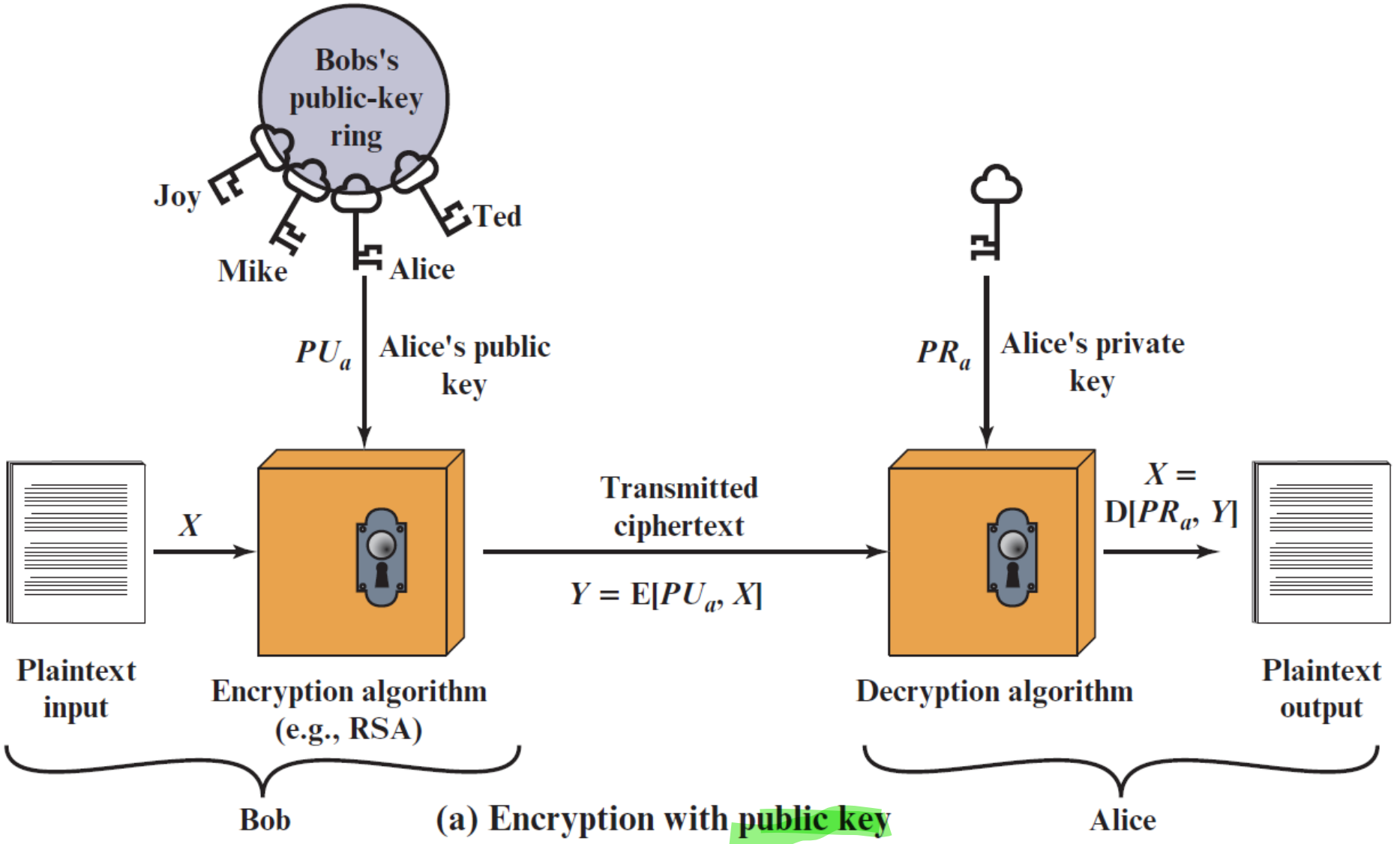
1. Two communicants already share a key, which somehow has been distributed to them(!)
2. The use of a trusted third-party called **Key Distribution Center** (KDC).

Problem 2: How a receiver can be assured that a message came from a particular sender (Digital Signature)?

Six Ingredients of Public Key Cryptography

- **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. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- **Ciphertext:** This is the encrypted message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption Algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Achieving Confidentiality (Secrecy)

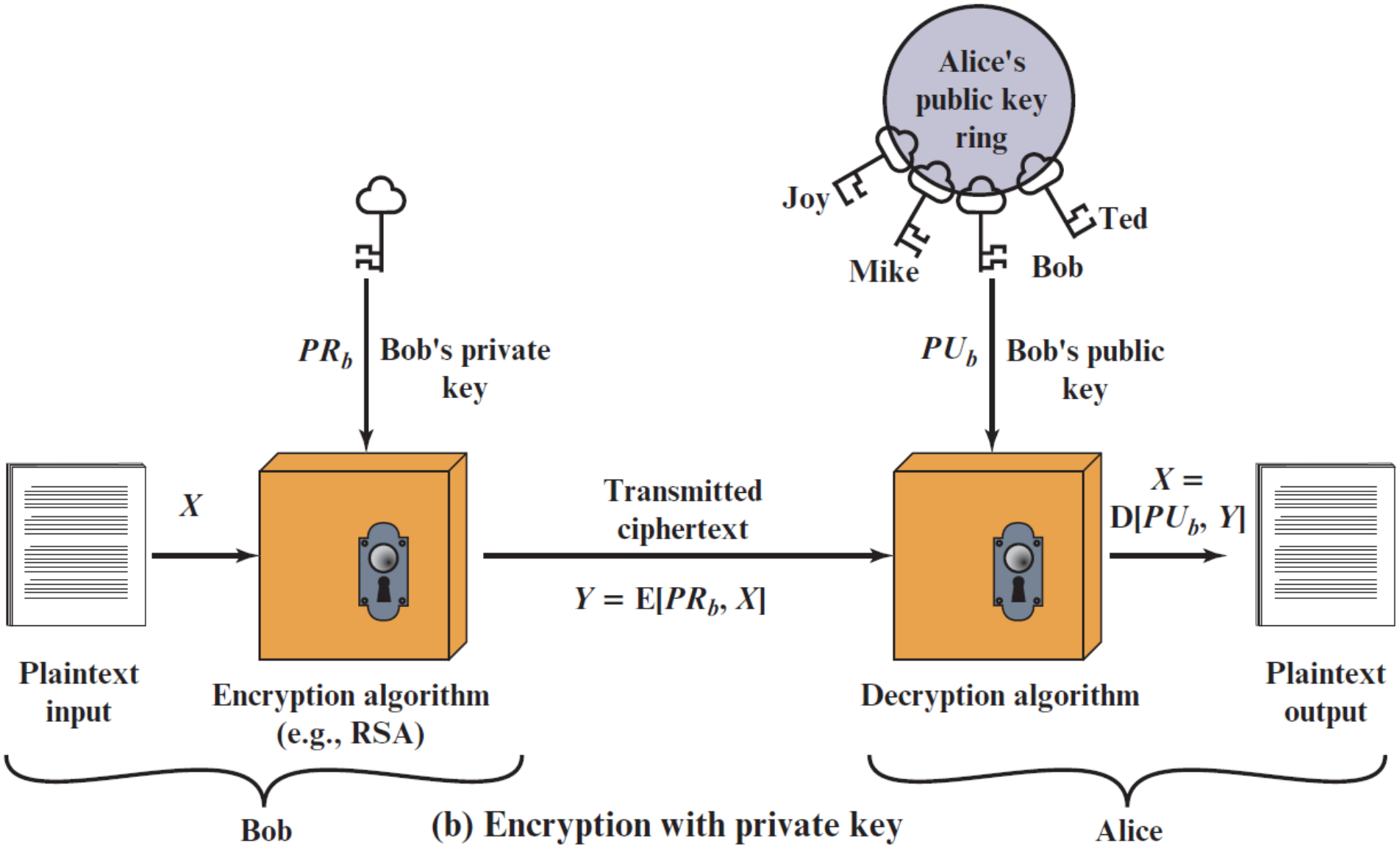


(a) Encryption with public key

Achieving Confidentiality (Secrecy)

- Alice generates a key pair (private and public keys).
- Alice distributes her public key to Bob.
- Bob encrypts a message with Alice's public key and sends the ciphertext to Alice.
- Upon receipt, Alice decrypts the ciphertext with her private key successfully.
- If adversary manages to get the ciphertext, he/she will not be able to decipher it as he/she does not know Alice's private key.

Achieving Authentication



(b) Encryption with private key

Achieving Authentication

- Bob generates a key pair (private and public keys).
- Bob distributes his public key to Alice.
- Bob encrypts a message with his private key and sends the ciphertext to Alice.
- Upon receipt, Alice decrypts the ciphertext with Bob's public key successfully.
- Since the message was encrypted using Bob's private key, only Bob could have prepared the message.
- In this case, the entire encrypted message (ciphertext) serves as a **Digital Signature**.
- Rather than encrypting the whole message, a more efficient approach is to encrypt a small block of bits that is a function of the document (**Authenticator**).

Symmetric vs Asymmetric Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if the key is kept secret. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and a related algorithm for decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if one of the keys is kept secret. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

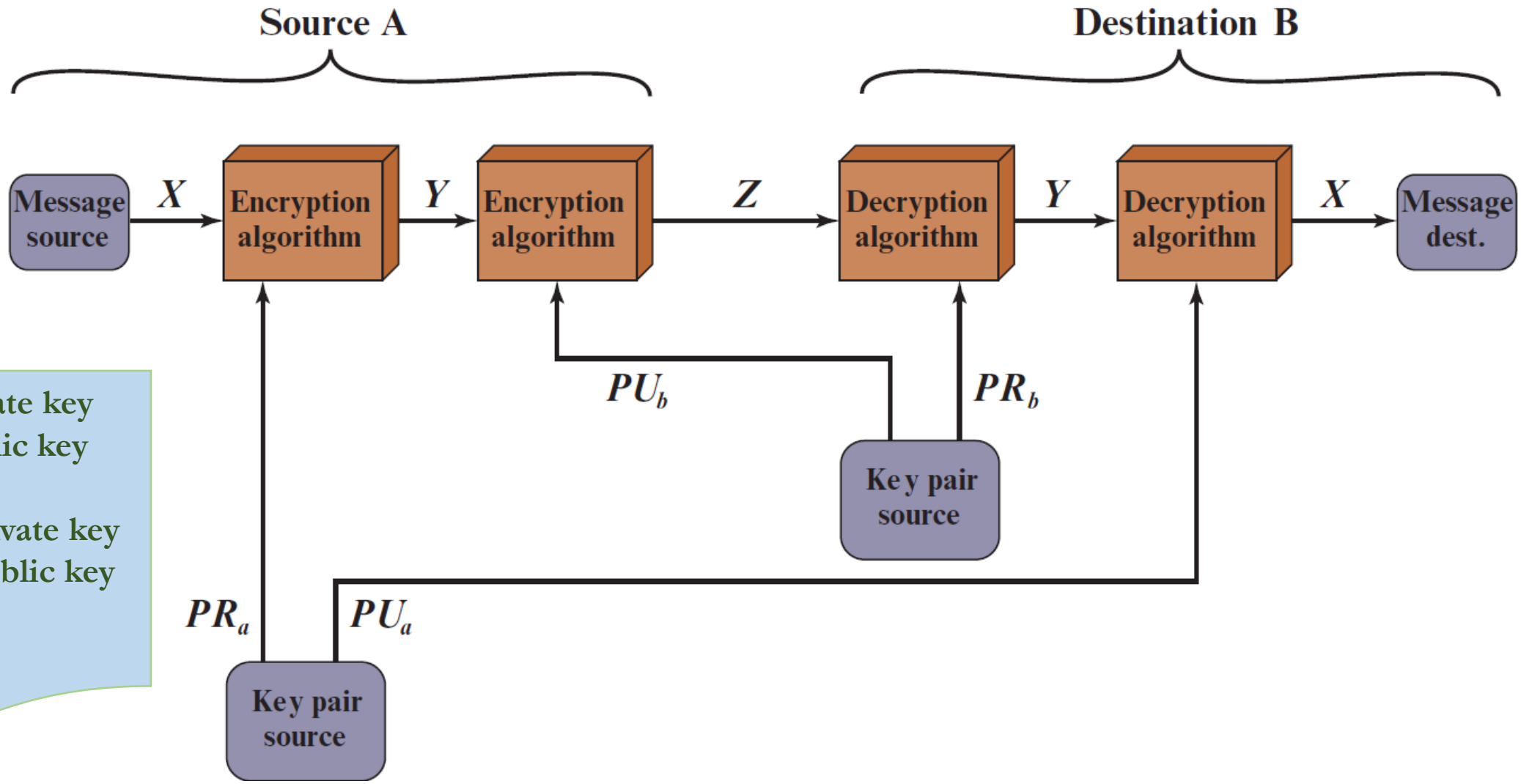
Essential Steps for Achieving Confidentiality

1. Each user (Bob and Alice) 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. Each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a confidential message to Alice, he encrypts the message using the Alice's public key.
4. When the Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

Some Facts of Public Key Cryptography

- All participants (including attackers) have access to public keys.
- Private keys are generated locally by each participant and therefore need never be distributed.
- As long as a user's private key remains protected and secret, incoming communication is secure.
- At any time, a system can change its private key and publish the companion public key to replace its old public key.

Achieving Authentication & Confidentiality



PR_a: Sender's private key
PU_a: Sender's public key

PR_b: Receiver's private key
PU_b: Receiver's public key

Achieving Authentication & Confidentiality

- The process begins as before by encrypting a message $(X \rightarrow Y)$, using the sender's private key. This provides the digital signature.
- Next, Y is encrypted again, using the receiver's public key $(Y \rightarrow Z)$.
- The final ciphertext can be decrypted only by the intended receiver, who alone has the matching private key. Thus, confidentiality is provided.

Characteristics of Asymmetric algorithms

- It is ***computationally infeasible*** to find decryption key knowing only the algorithm and the encryption key.
- It is computationally easy to encrypt or decrypt messages when the relevant encryption or decryption key is known.
- In addition, for some algorithms, such as RSA, either of the two related keys can be used for encryption, with the other used for decryption.

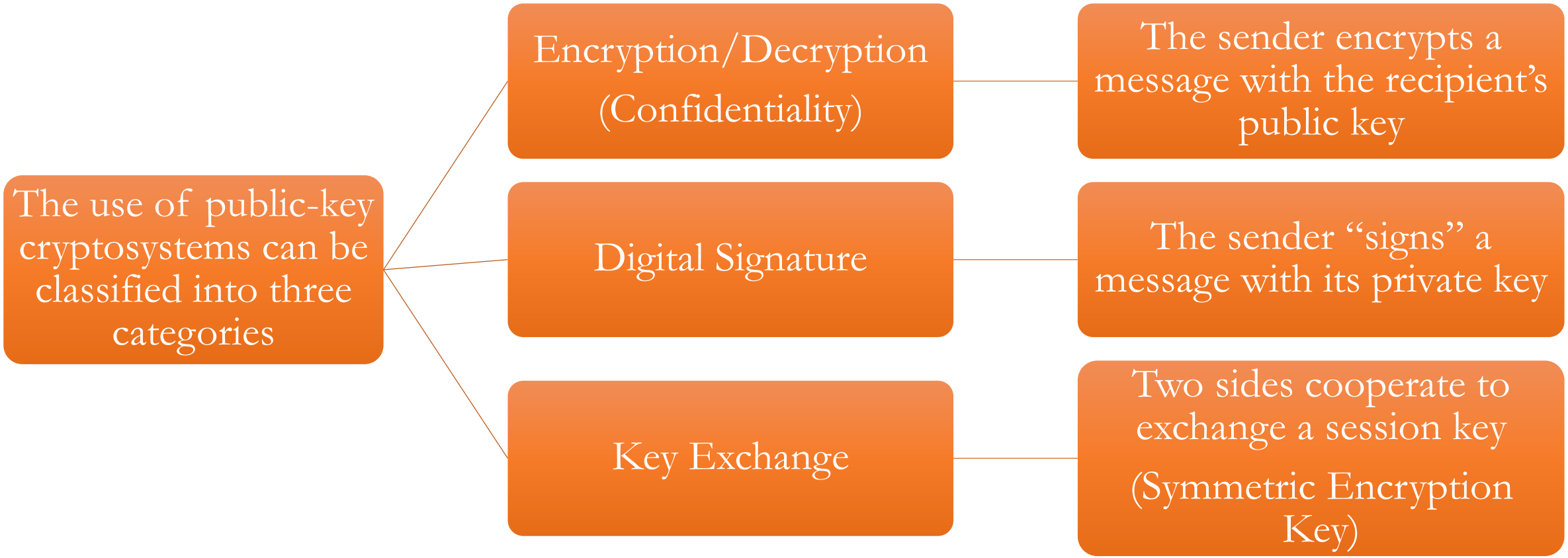
Characteristics of Asymmetric Algorithms (Short Note):

Knowing only the encryption key and algorithm, it's nearly impossible to find the decryption key.

Easy to encrypt/decrypt messages when the correct key is known.

In some cases (e.g., RSA), either key can be used to encrypt, and the other can be used to decrypt.

Applications for Public Key Cryptosystems



Applications for Public Key Cryptographic Algorithms

- Some public key cryptographic algorithms are suitable for all three applications, whereas others can be used only for one or two of these applications

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie–Hellman	No	No	Yes
DSS	No	Yes	No