Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

Public Key Cryptography

Session Objectives

Public Key Cryptography

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

- Study about the principles of public-key cryptography

Session Outcomes

Public Key Cryptography

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

At the end of this session, participants will be able to

- Discuss the principles behind public-key cryptography.

Agenda

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

1 Private-Key Cryptography

2 Public-Key Cryptography

3 Symmetric vs Public-Key

4 Public-Key Requirements

5 Summary

Presentation Outline

1 Private-Key Cryptography

2 Public-Key Cryptography

3 Symmetric vs Public-Key

4 Public-Key Requirements

5 Summary

Private-Key Cryptography

Public Key Cryptography

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

- Traditional private/secret/single key cryptography uses one key
- Shared by both sender and receiver
- If this key is disclosed communications are compromised also is symmetric, parties are equal
- Hence does not protect sender from receiver forging a message & claiming is sent by sender

Presentation Outline

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

1 Private-Key Cryptography

2 Public-Key Cryptography

3 Symmetric vs Public-Key

4 Public-Key Requirements

5 Summary

Public-Key Cryptography

Public Key Cryptography

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

- Probably 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

Why Public-Key Cryptography?

- Developed to address two key issues:
  - **key distribution** – how to have secure communications in general without having to trust a KDC with your key
  - **digital signatures** – how to verify a message comes intact from the claimed sender
- Public invention due to Whitfield Diffie & Martin Hellman at Stanford Uni in 1976 known earlier in classified community

Public-Key Cryptography

Public Key Cryptography

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

- Public-key/two-key/asymmetric cryptography involves the use of two keys:
  - A public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
  - A related private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures
- Infeasible to determine private key from public
- It is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures

Public-Key Cryptography

Public Key Cryptography

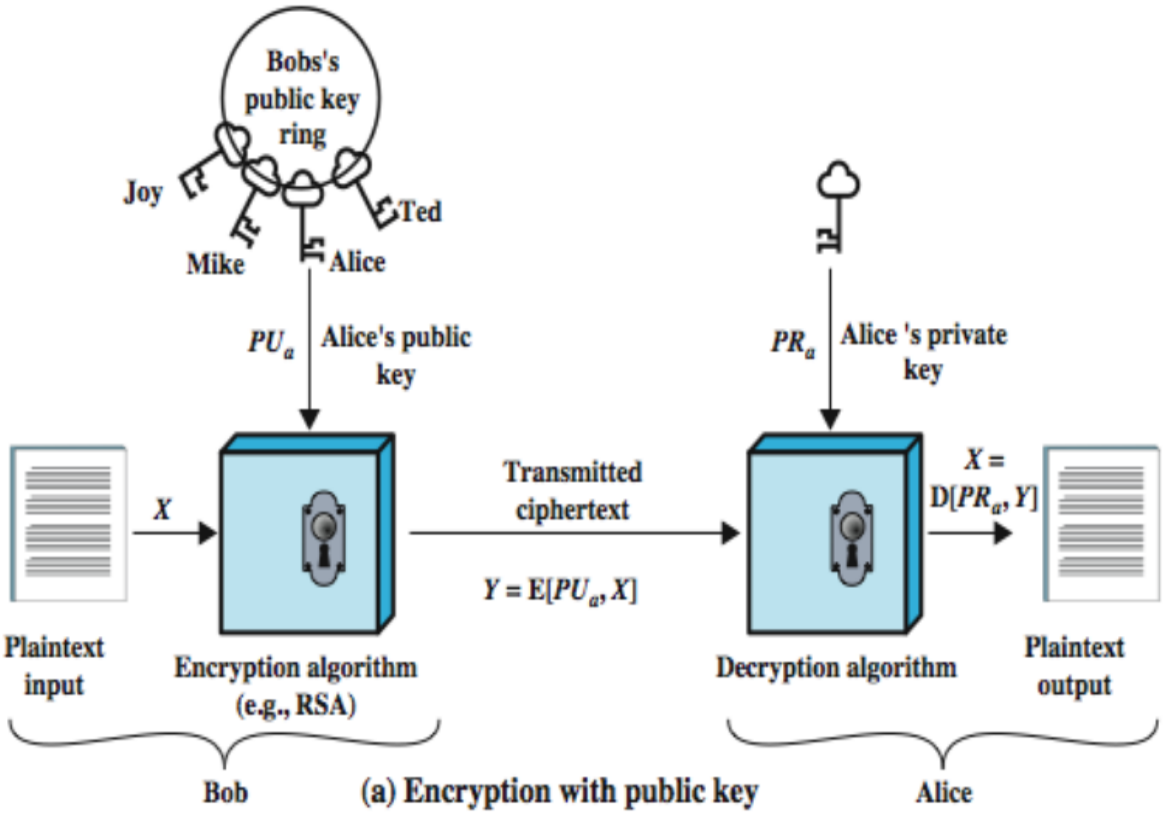
Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary



(a) Encryption with public key

Presentation Outline

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

1 Private-Key Cryptography

2 Public-Key Cryptography

3 Symmetric vs Public-Key

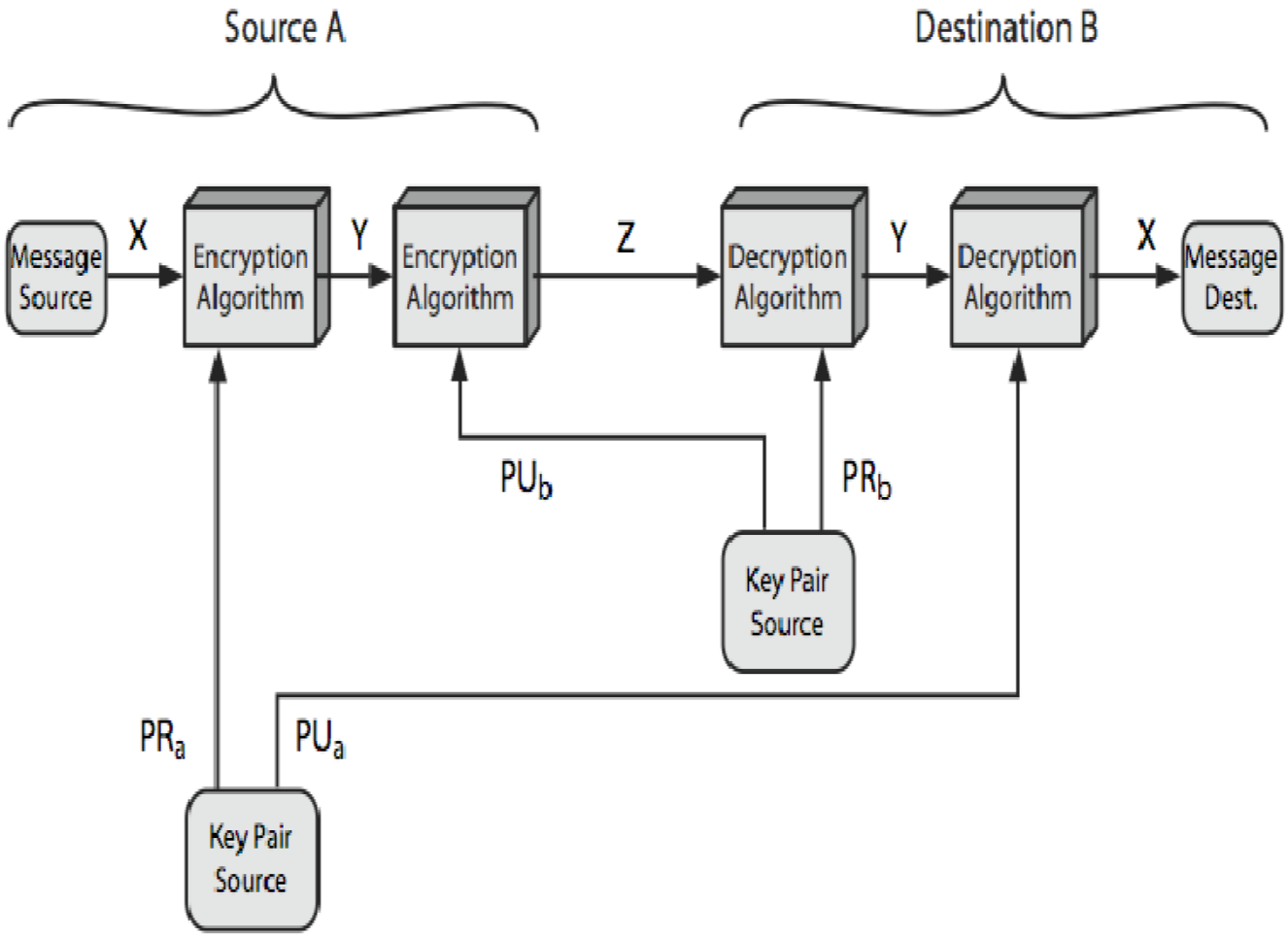
4 Public-Key Requirements

5 Summary

Symmetric vs Public-Key

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 no other information is available. 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 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 no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Public-Key Cryptosystems



Public-Key Applications

- can classify uses into 3 categories:
  - encryption/decryption (provide secrecy)
  - digital signatures (provide authentication)
  - key exchange (of session keys)
- some algorithms are suitable for all uses, others are specific to one

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

Presentation Outline

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

1 Private-Key Cryptography

2 Public-Key Cryptography

3 Symmetric vs Public-Key

4 Public-Key Requirements

5 Summary

Public-Key Requirements

Public Key Cryptography

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

- Public-Key algorithms rely on two keys where:
  - it is computationally infeasible to find decryption key knowing only 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)
- these are formidable requirements which only a few algorithms have satisfied

Public-Key Requirements

Public Key Cryptography

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

- need a trapdoor one-way function
- one-way function has
  - **Y = f(X) easy**
  - **X = f^{-1}(Y) infeasible**
- a trap-door one-way function has
  - **Y = f_k(X) easy, if k and X are known**
  - **X = f_k^{-1}(Y) easy, if k and Y are known**
  - **X = f_k^{-1}(Y) infeasible, if Y known but k not known**
- a practical public-key scheme depends on a suitable trap-door one-way function

Security of Public Key Schemes

- like private key schemes brute force exhaustive search attack is always theoretically possible but keys used are too large ($>$512bits)
- security relies on a large enough difference in difficulty between easy (en/decrypt) and hard (cryptanalyse) problems
- more generally the hard problem is known, but is made hard enough to be impractical to break
- requires the use of very large numbers
- hence is slow compared to private key schemes

Presentation Outline

Private-Key Cryptography

Public-Key Cryptography

Symmetric vs Public-Key

Public-Key Requirements

Summary

1 Private-Key Cryptography

2 Public-Key Cryptography

3 Symmetric vs Public-Key

4 Public-Key Requirements

5 Summary

Summary

Discussed

- Principles of public key cryptography
- Various applications and security of public key cryptography