Cryptography and Network Security

Network Security Model

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	25 June 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Basic terminology
- Model for Network security
- Summary
- Test your understanding
- References

Basic terminology

- Plaintext: original message to be encrypted
- Ciphertext: the encrypted message
- Enciphering or encryption: the process of converting plaintext into ciphertext
- Encryption algorithm: performs encryption
  - Two inputs: a plaintext and a secret key

5

Basic terminology

- Deciphering or decryption: recovering plaintext from ciphertext
- Decryption algorithm: performs decryption
  - Two inputs: ciphertext and secret key
- Secret key: same key used for encryption and decryption
  - Also referred to as a symmetric key

6

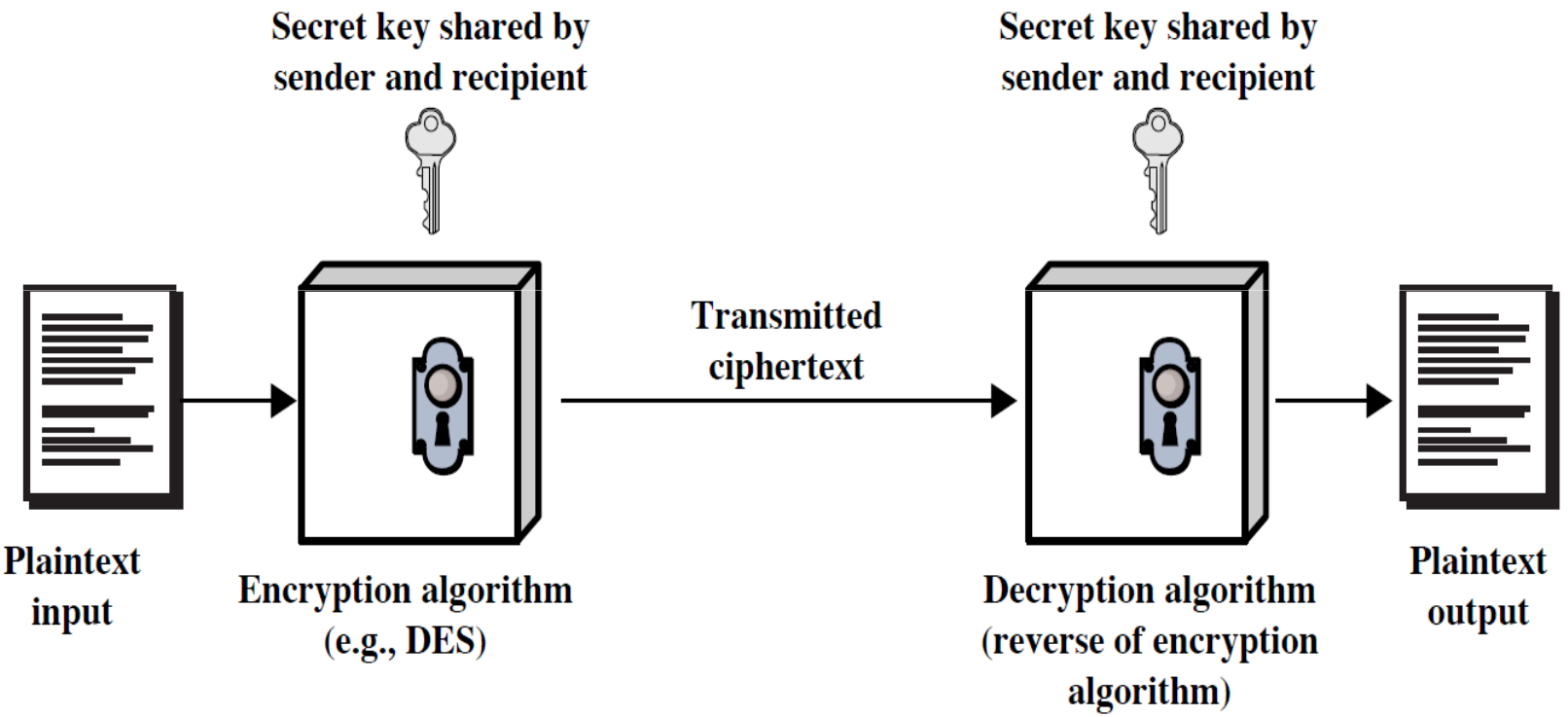
Basic terminology

- Cipher or cryptographic system : a scheme for encryption and decryption
- Cryptography: science of studying ciphers
- Cryptanalysis: science of studying attacks against cryptographic systems
- Cryptology: cryptography + cryptanalysis

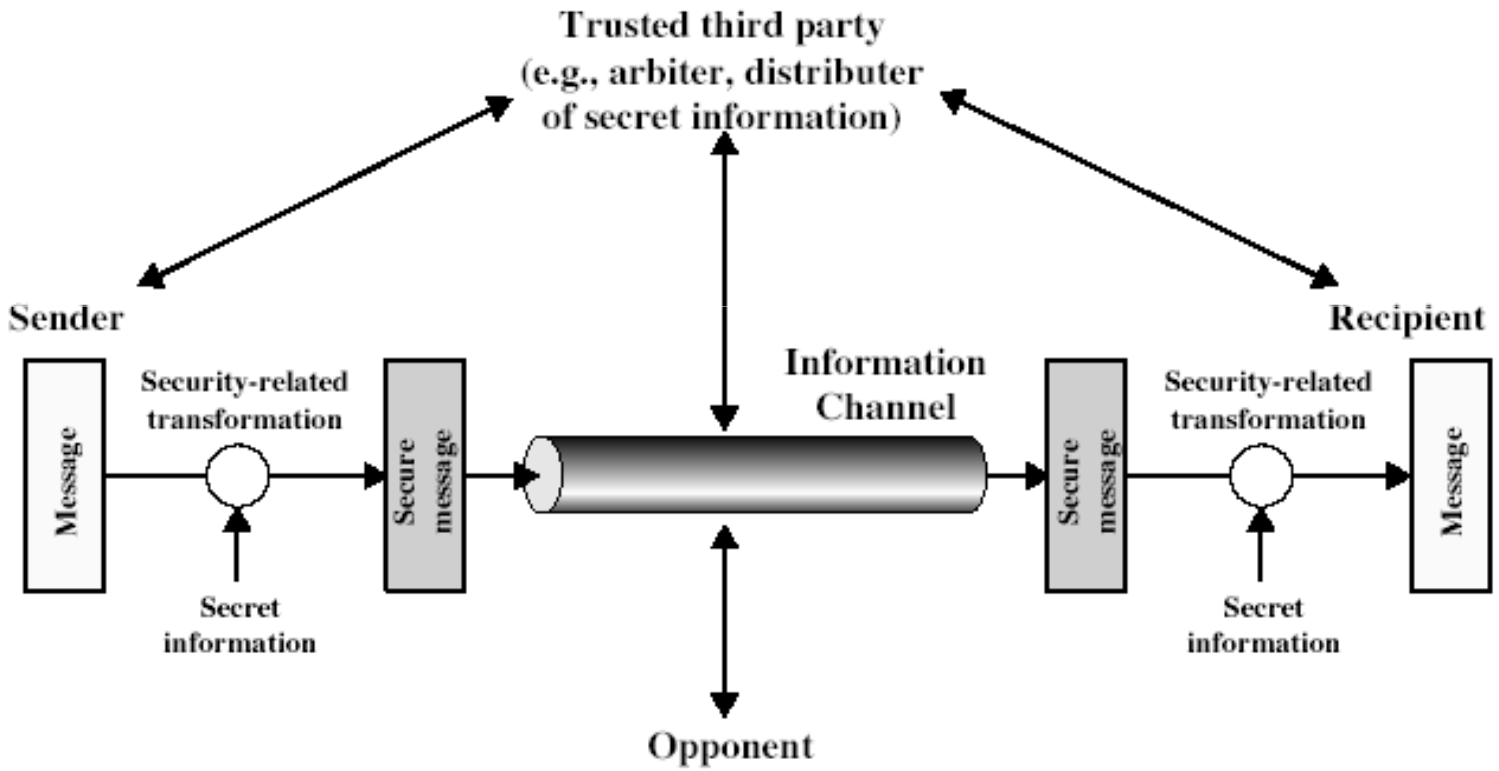
Agenda

- Basic terminology
- Model for Network security
- Summary
- Test your understanding
- References

Symmetric Cipher Model



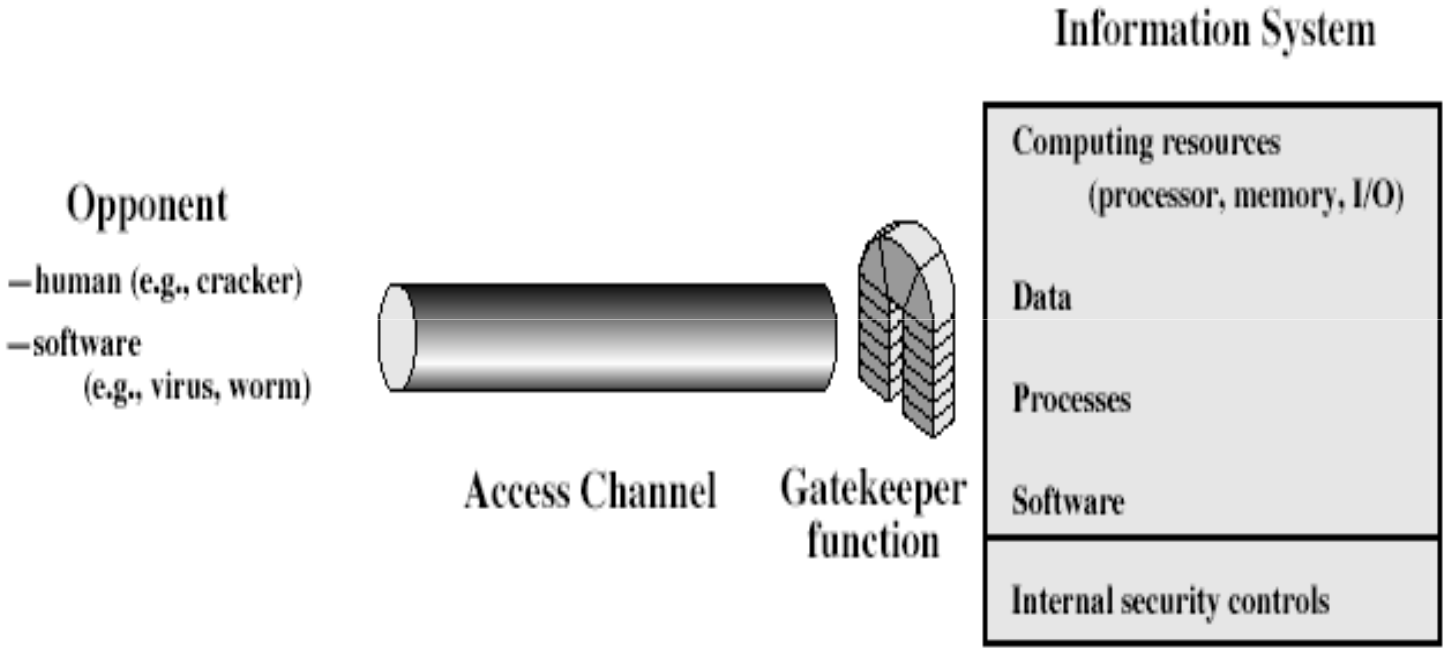
Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems can be used to implement this model

Agenda

- Basic terminology
- Model for Network security
- Summary
- Test your understanding
- References

Summary

- Define basic terminologies used in cryptography
- Discuss models for network (access) security

Agenda

- Basic terminology
- Model for Network security
- Summary
- Test your understanding
- References

Test your understanding

1. Discuss the model for network security
2. Define cryptography.
3. Define cryptanalysis.
4. What is deciphering?
5. What is enciphering?

Agenda

- Basic terminology
- Model for Network security
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.