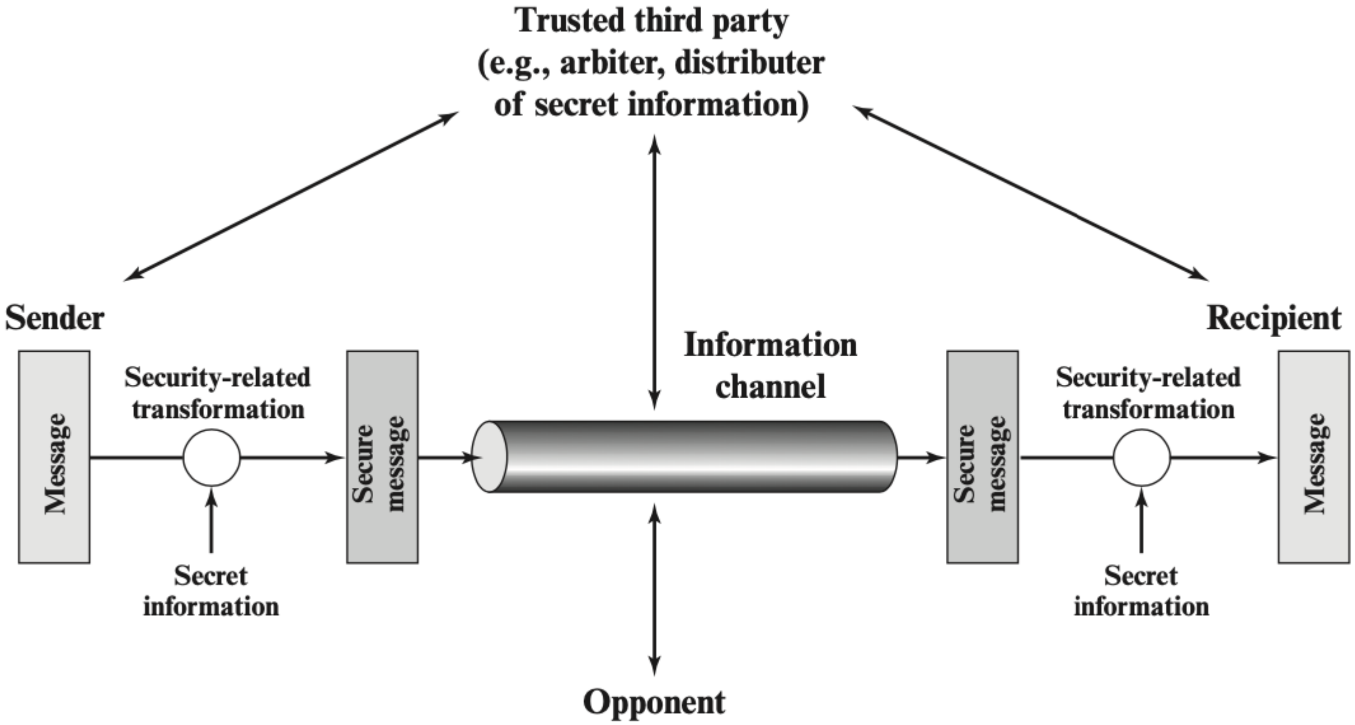
Symmetric Encryption and Message Confidentiality

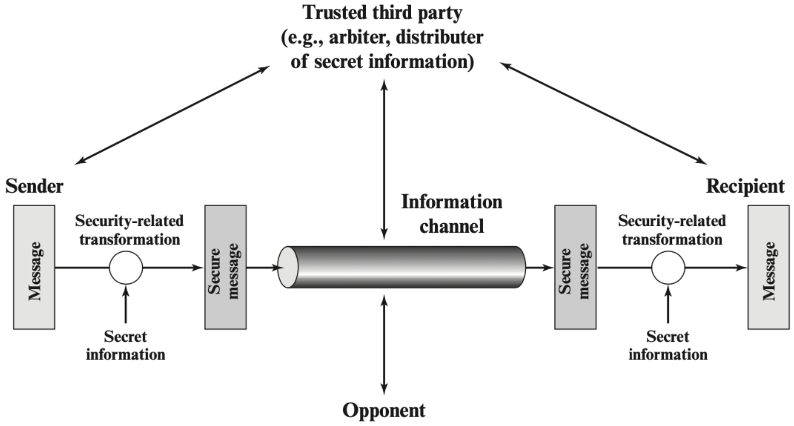
Chapter 2

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

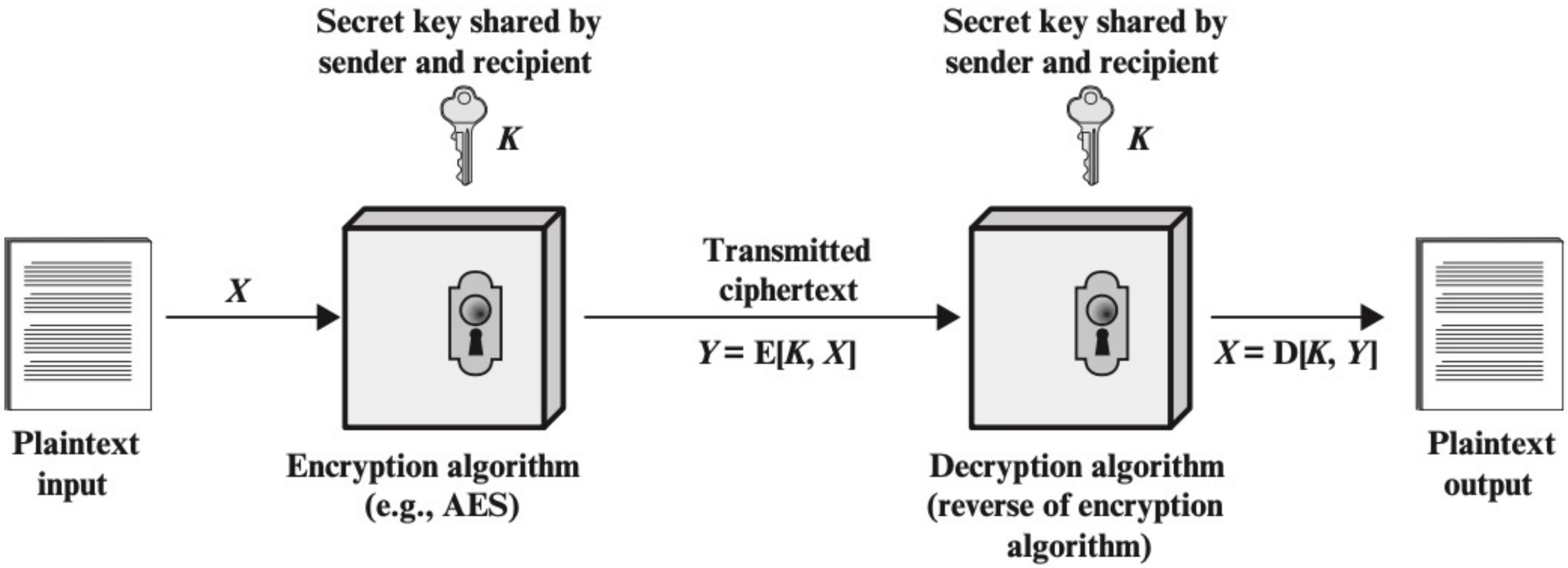


Symmetric Encryption Principles

Symmetric encryption

- Sender and recipient share a common/same key
- Was the only type of cryptography, prior to invention of public-key in 1970's

Simplified model of symmetric encryption


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E[K, X]
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Symmetric encryption

- Has five ingredients
  - **Plaintext**: the original message or data
  - **Encryption algorithm**: performs various substitutions and transformations on the plaintext
  - **Secret key**
  - **Ciphertext**: the coded message
  - **Decryption algorithm**: takes the ciphertext and the same secret key and produces the original plaintext

Other basic terminology

- **cipher** - algorithm for transforming plaintext to ciphertext
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key

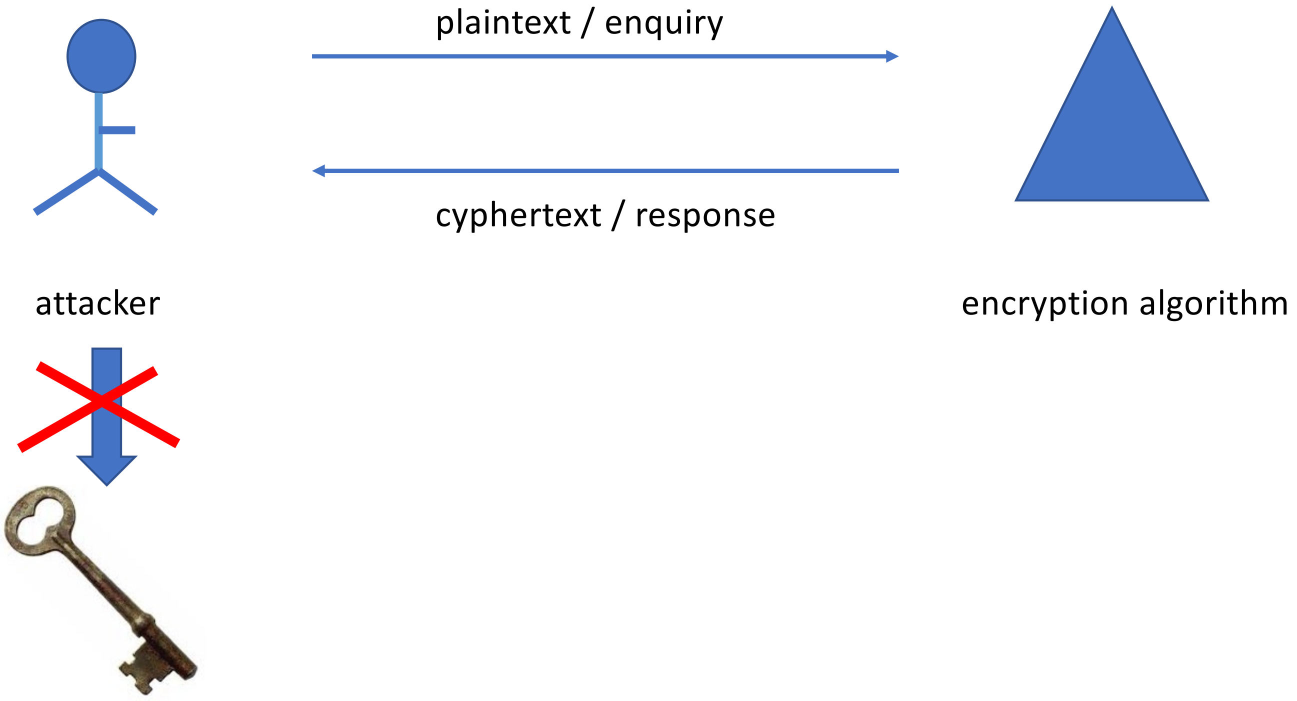
Requirements

- Two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver

    $Y = \mathrm{E}_K(X)$

    $X = \mathrm{D}_K(Y)$
- assume encryption algorithm is known
- the security of symmetric encryption depends on the secrecy of the key
- implies a secure channel to distribute key

A strong encryption algorithm



plaintext / enquiry

cyphertext / response

attacker

encryption algorithm

TA & Grader

- TA Name: Faiyaz, Amir (Project, Review & Quiz)
- Email: afaiyaz@ttu.edu
- Reminder: Submit the names and emails of your group members to

  FALL 2024 CS5342 PROJECT GROUP NAMES.xlsx

- Grader Name: Han, Namgyu (Homework, Quiz, Exam grading)
- Email: Namgyu.Han@ttu.edu