Introduction to Cryptography

(--Foundation of information security--)

By:
Arun Mishra

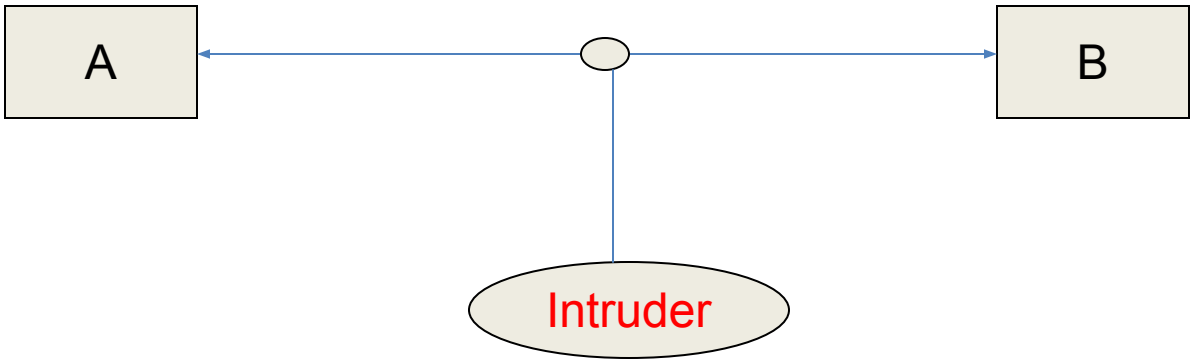
Acknowledgement:

- “Cryptography & Network Security” by William Stallings, Pearson Education Asia.
- Kahate A, “Cryptography & Network Security”, Tata McGraw Hill, 2004.
- Reference Books
- “Applied Cryptology” by Schiner Bruce, John Wiley & Sons, 2001.
- “Introduction to Cryptography with Coding Theory” by Wade Trappe & Lawrence CWashington, New Jersey, Pearson Education, 2006.
- Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: PrivateCommunication in a Public World”, Prentice Hall of India Private Limited.
- Behrouz A. Forouzan, “Cryptography and Network Security”, McGraw Hill

Marking

- **Internal Test– 30**
- **Lab Assigenments-20**
- **END SEM - 50**

Why study cryptography?



Communications security

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Who is the Opponent

- Computer/ Machine
- Person
- Application/ Process/Program

The Basic Problem

- We consider the confidentiality goal:
  - Alice and Bob are Friends
  - Eve is a rival
  - Alice wants to send secret messages (M_1,M_2,…) to Bob over the Internet
  - Rival Eve wants to read the messages (M_1,M_2,…) - Alice and Bob want to prevent this!
  - Assumption: The network is OPEN: Eve is able to eavesdrop and read all data sent from Alice to Bob.
  - Consequence: Alice must not send messages (M_1,M_2,…) directly – they must be “scrambled” or encrypted using a ‘secret code’ unknown to Eve but known to Bob.

The General Goals of Cryptography

- Confidentiality; assuring that only authorized parties are able to understand the data.
- Integrity; ensuring that when a message is sent over a network, the message that arrives is the same as the message that was originally sent.

Technical solutions include:

Encryption
Hashing algorithms

Goals (cont.)

- Authentication; ensuring that whoever supplies or accesses sensitive data is an authorized party.
- Nonrepudiation; ensuring that the intended recipient actually received the message & ensuring that the sender actually sent the message.

Technical solutions include:

Passwords
Digital signatures

Security Threats and Attacks

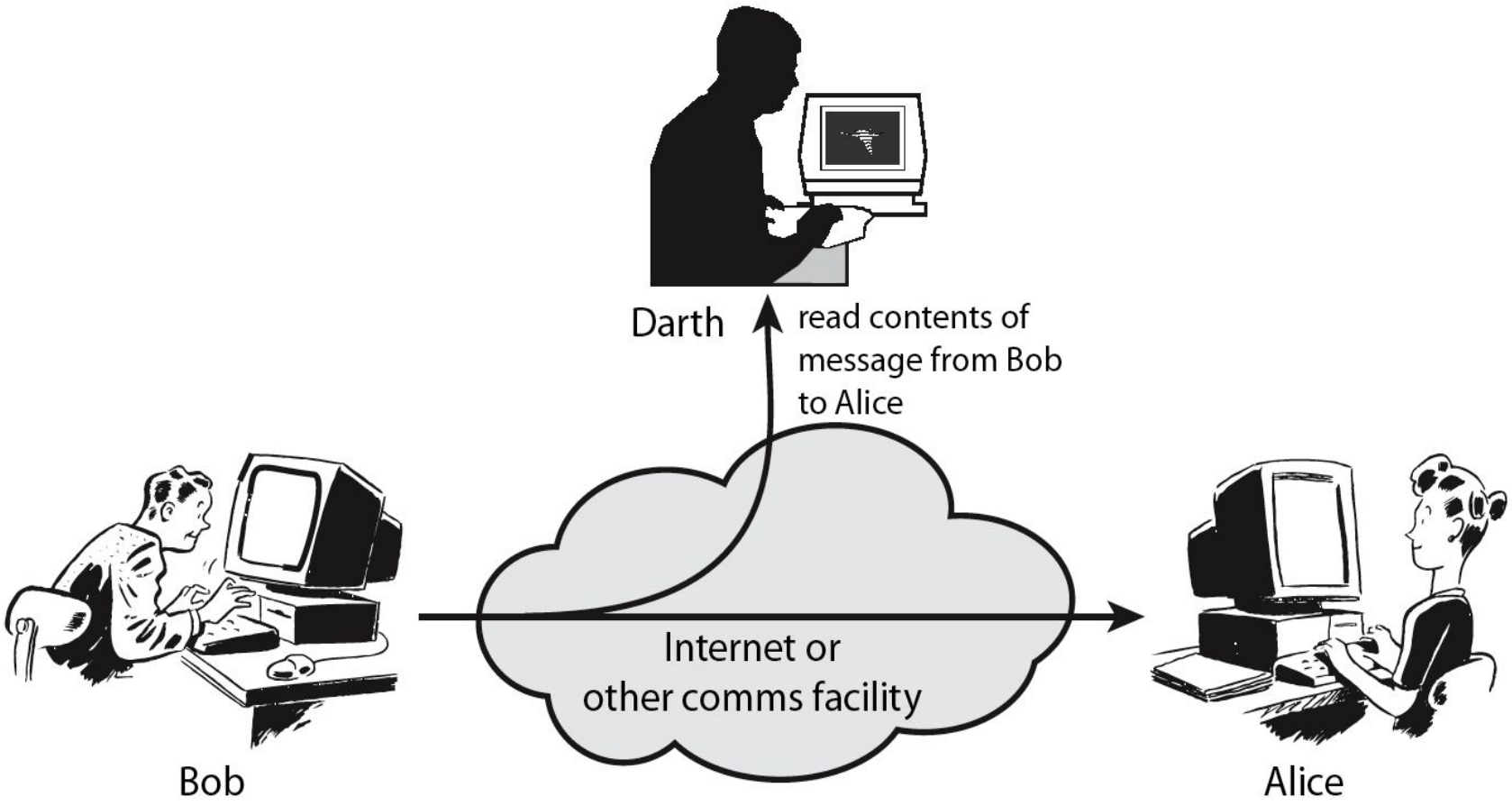
- A threat is a potential violation of security.
  - Flaws in design, implementation, and operation.
- An attack is any action that violates security.

  Note: Router mis-configuration or server crash can also cause loss of availability, but they are not attacks

Security Attack

- Two generic types of attacks
  - Passive
  - Active

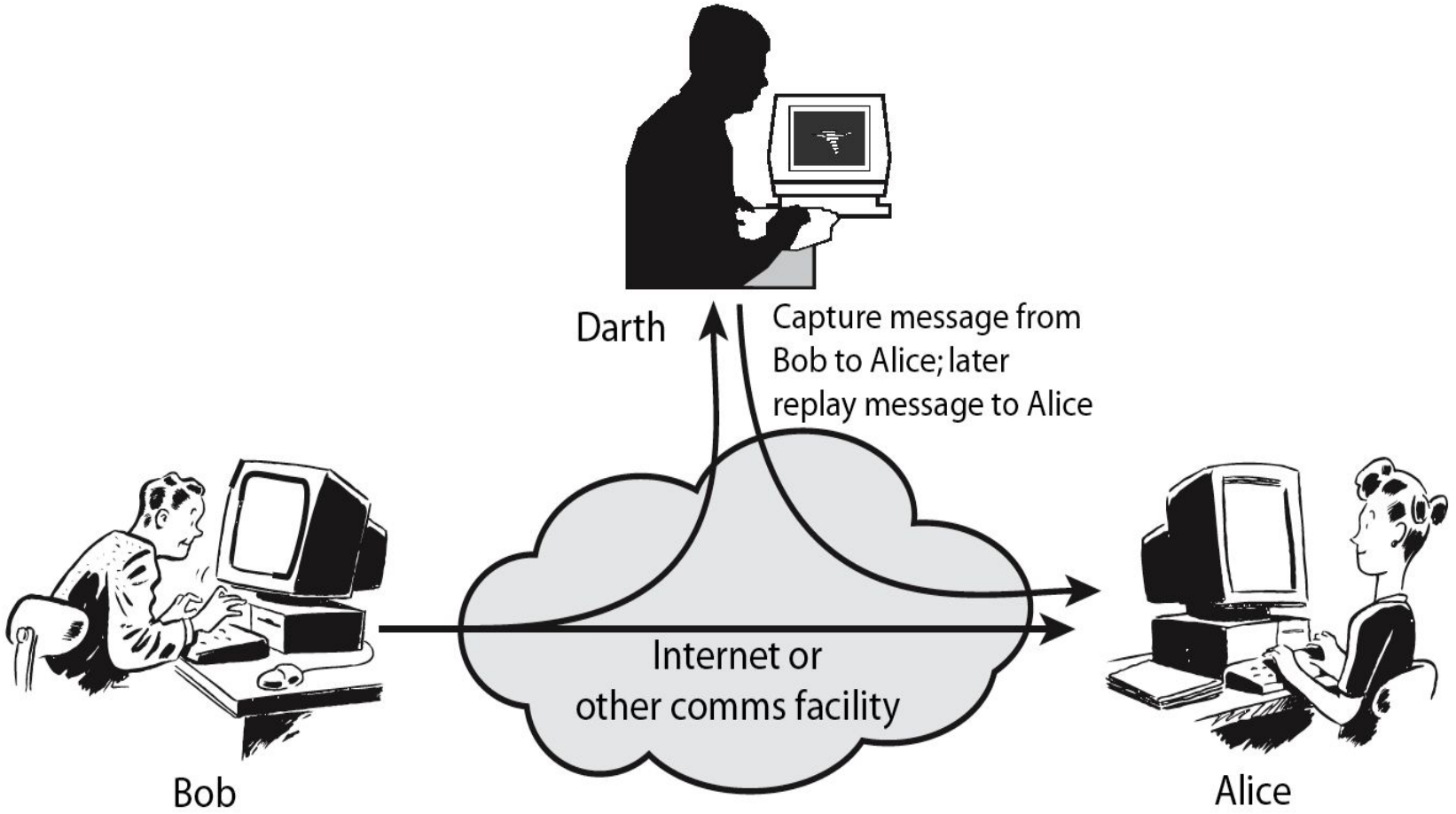
Passive Attacks



Example

- The Release of message contents
- Traffic Analysis

Active Attacks

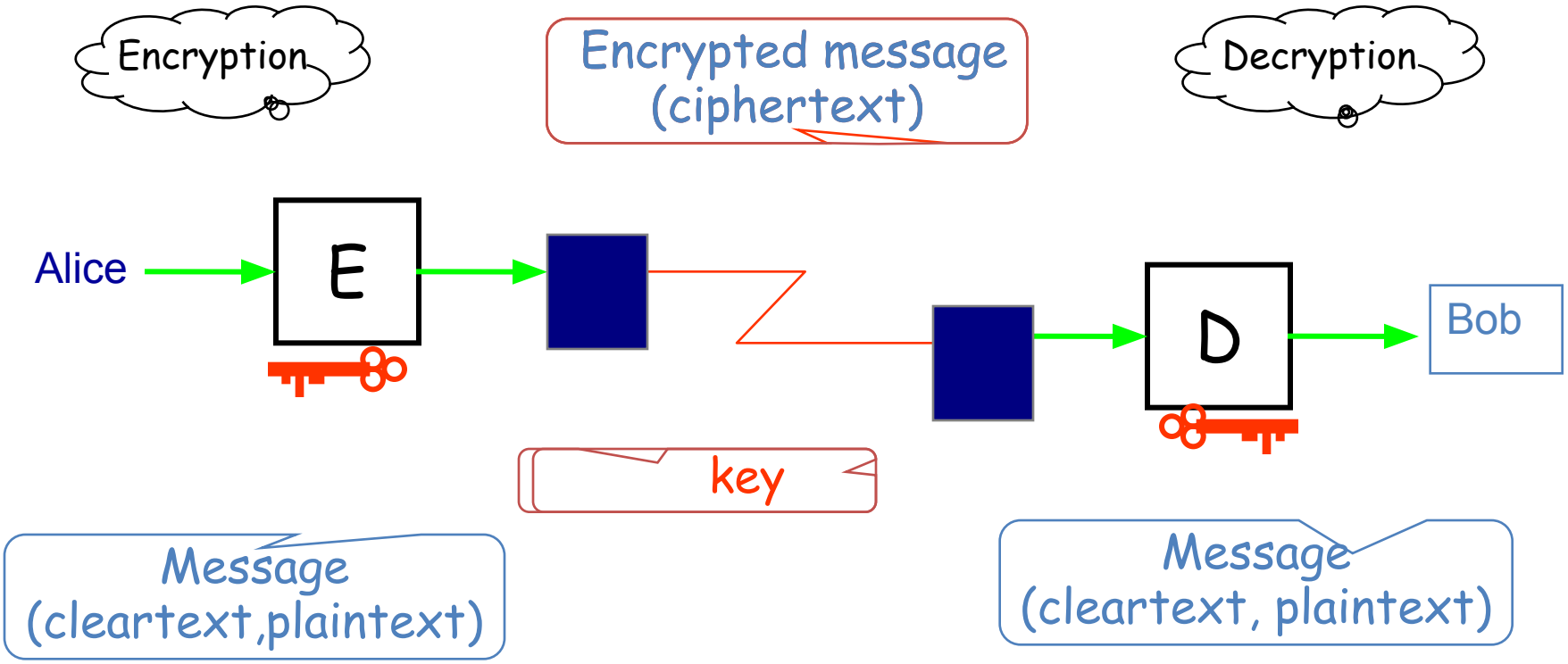


Example

- Masquerade
- Replay
- Modification of messages
- Denial of service

Continue….

Private key cipher



Basic Terms

- Encryption: scrambling a message or data using a specialized cryptographic algorithm.
- Plaintext: the message or data before it gets encrypted.
- Ciphertext: the encrypted (scrambled) version of the message.
- Cipher: the algorithm that does the encryption

Classical Ciphers

- Plaintext is viewed as a sequence of elements (e.g., bits or characters)
- Substitution cipher: replacing each element of the plaintext with another element.
- Transposition (or permutation) cipher: rearranging the order of the elements of the plaintext.
- Product cipher: using multiple stages of substitutions and transpositions

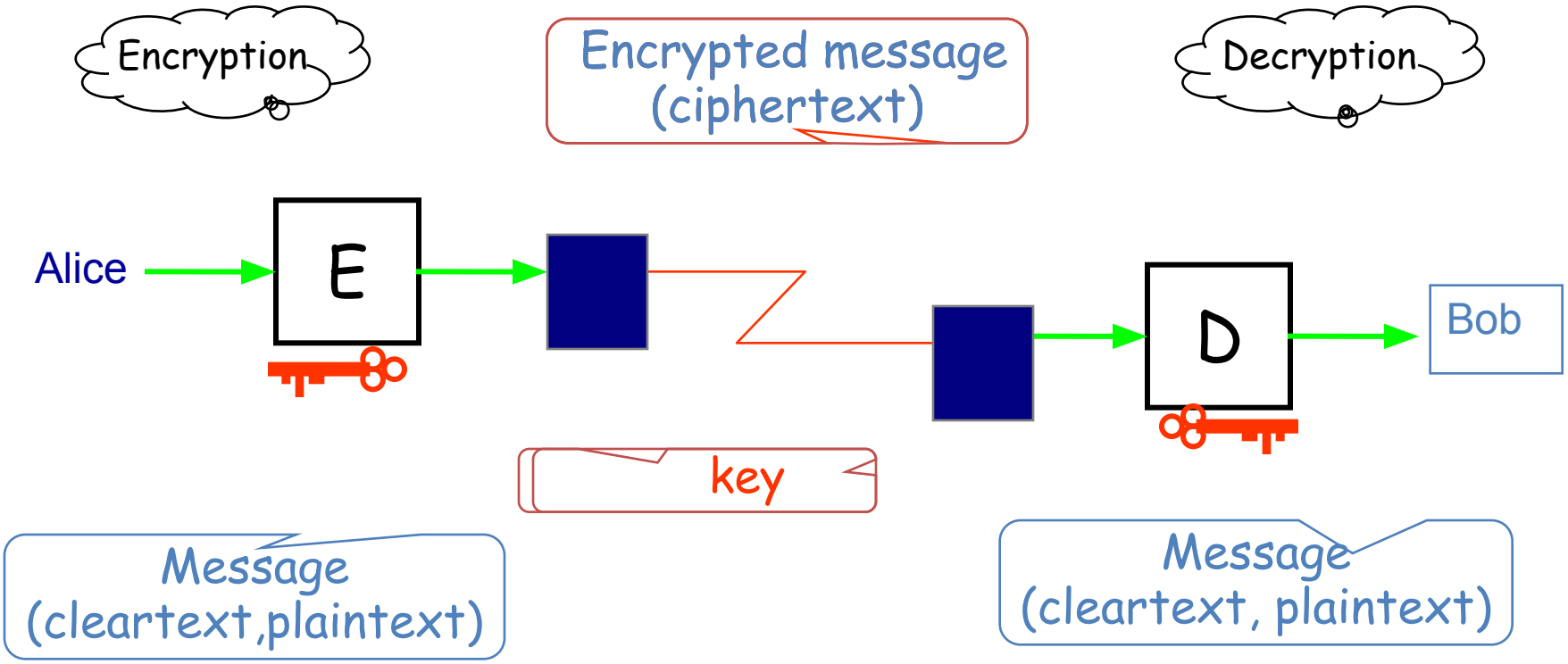
Basic Terms (cont.)

- Decryption: the process of converting ciphertext back to the original plaintext.
- Cryptanalysis: the science of breaking cryptographic codes/algorithms.
- Cryptanalyst: a person who breaks cryptographic codes; also referred to as “the attacker”.

Types of ciphers

- Private key cryptosystems/ciphers
  - The secret key is shared between two parties
- Public key cryptosystems/ciphers
  - The secret key is not shared and two parties can still communicate using their public keys

Contd..


Encryption
Encrypted message
(ciphertext)
Decryption
Alice
E
D
Bob
key
Message
(cleartext,plaintext)
Message
(cleartext, plaintext)

Concepts

- A private key cipher is composed of two algorithms
  - encryption algorithm E
  - decryption algorithm D
- The same key K is used for encryption & decryption
- K has to be distributed beforehand

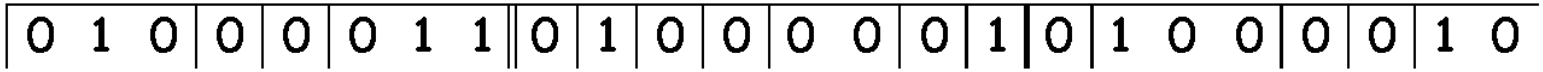
Notations

- Encrypt a plaintext P using a key K & an encryption algorithm E
  C = E(K,P)
- Decrypt a ciphertext C using the same key K and the matching decryption algorithm D
  P = D(K,C)

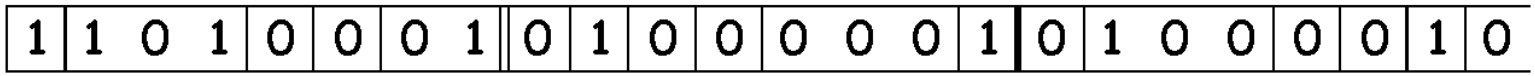
- Note: P = D(K,C) = D(K, E(K,P))

A Simple Example

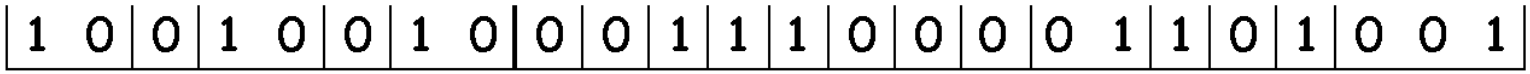
The plaintext:



The key:



The ciphertext



Example Contd..

ciphertext:

1	0	0	1	0	0	1	0	0	0	1	1	1	0	0	0	0	1	1	0	1	0	0	1

XOR'd with key

1	1	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0

yields plaintext

0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0

Model for Network Security

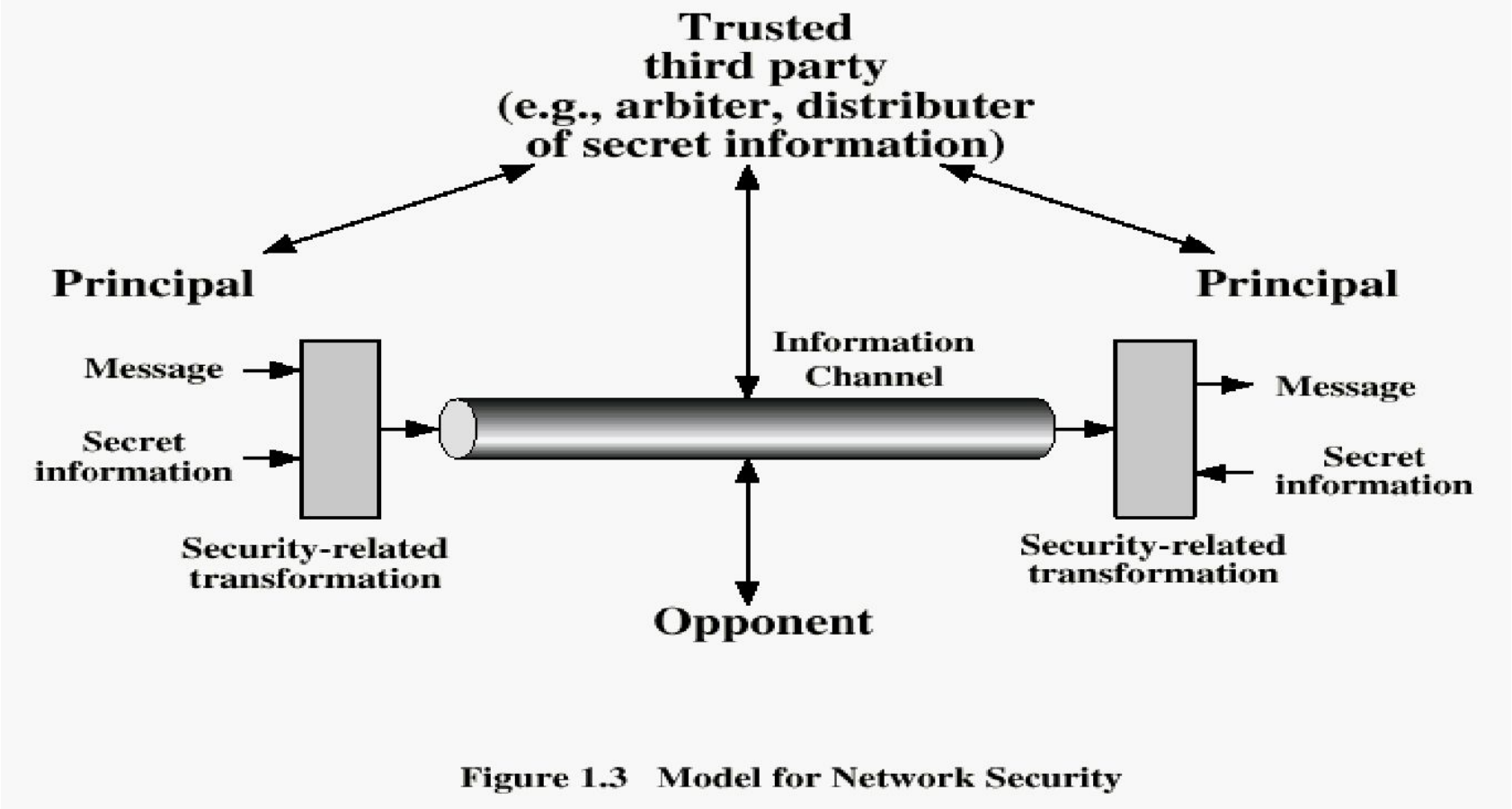


Figure 1.3 Model for Network Security

Model Contd..

Using this model requires us to:

1. Design a suitable algorithm for the security transformation
2. Generate the secret information (keys) used by the algorithm
3. Develop methods to distribute and share the secret information
4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Requirements

- Characterize cryptographic system by:
  - Type of encryption operations used
    - substitution / transposition
  - Number of keys used
    - single-key or private / two-key or public
  - Way in which plaintext is processed
    - Block (typically 64 or 128 bits) / stream (1 bit)

Cryptanalysis

- Objective to recover key not just message
- General approaches:
  - Cryptanalytic attack
  - Brute-force attack

Brute Force Attack

- Always possible to simply **try every key**
- **Example:**

  Key Size (bits) 32 bits,

  Number of Alternative Keys = $2^{32} = 4.3 \times 10^9$

  at 1 decryption / micro second

(Time required depends on kind of processing power)

Common Types of Cryptanalytic Attacks

- Known cipher attacks: the attacker has the ciphertext and she tries to decrypt the message by generating all possible keys.

  Rarely successful because the number of possible keys is enormous.

Attacks Contd..

- Known plaintext attack: the attacker has both the ciphertext and the plaintext.
  - Again, this is difficult because there are so many keys, but the plaintext information may make experimentation easier than in the previous case.
  - We are assuming that the attacker knows the algorithm that was used for the encryption.

Attacks Contd..

- Chosen plaintext attacks: The cryptanalyst introduces the plaintext into the system and then watches for how that plaintext will be encrypted.

The Allies used this approach by sending out false messages about allied troop movements.

Example: chosen-plaintext attack

- In 1942, US Navy cryptanalysts discovered that Japan was planning an attack on “AF”.
- They believed that “AF” means Midway island.
- Pentagon didn’t think so.
- US forces in Midway sent a plain message that their freshwater supplies were low.
- Shortly, US intercepted a Japanese ciphertext saying that “AF” was low on water.
- This proved that “AF” is Midway.

Chosen-ciphertext attack

- Eve choose some ciphertext and decrypts it to form a ciphertext/plaintext pair.

Contd..

- Side channel attacks use seemingly incidental information that can reveal important information about the key being used.

  Attacker analyzes the power output from a processor performing an encryption algorithm in order to get information about the key being used by that algorithm.

More Definitions

- **Unconditional security**
  - No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **Computational security**
  - Given limited computing resources (eg time needed for calculations is greater than age of universe), the cipher cannot be broken