Cryptography and Security Applications

Teacher: Dipanwita Roy Chowdhury

TA: Tapadyoti Banerjee

Class Schedule

Monday: 11 AM - 12 PM

Tuesday: 8 AM – 10 AM

Recommended Texts

1. *William Stallings*, Cryptography and Network Security. PHI-old edition, Pearson – New edition
2. *Douglas R. Stinson*, Cryptography, Theory and Practice. any Edition, CRC Press
3. *Alfred J. Menezes, Paul C. vanOrtshot, Scott A. Vanstone.* Handbook of Applied Cryptography. CRC Press

What is Cryptography ?

Cryptography is the science of using mathematics to encrypt and decrypt data.

- Phil Zimmermann

Cryptography is the art and science of keeping messages secure.

- Bruce Schneier

Definition:

The art and science of using mathematics to provide secrecy in information is termed as cryptography.

Cryptography is the study of techniques for secure communication in the presence of adversarial behavior.

Cryptography Terminologies

- A message (or information) is plaintext
- The process of hiding a message is encryption.
- An encrypted message is ciphertext.
- The process of turning ciphertext back into plaintext is decryption.
- Key is a secret
- A cipher is an algorithm for performing encryption or decryption
- Cryptanalysis is the study of analyzing and breaking secure communication.
- Cryptology means both cryptography and cryptanalysis.

What is Cryptography?

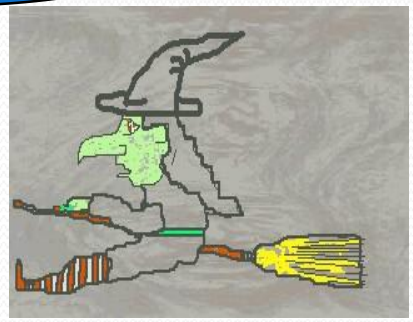
Data Integrity

Dear Alice,

Bob

Confidentiality

Alice



Authentication

Non Repudiation

Eve

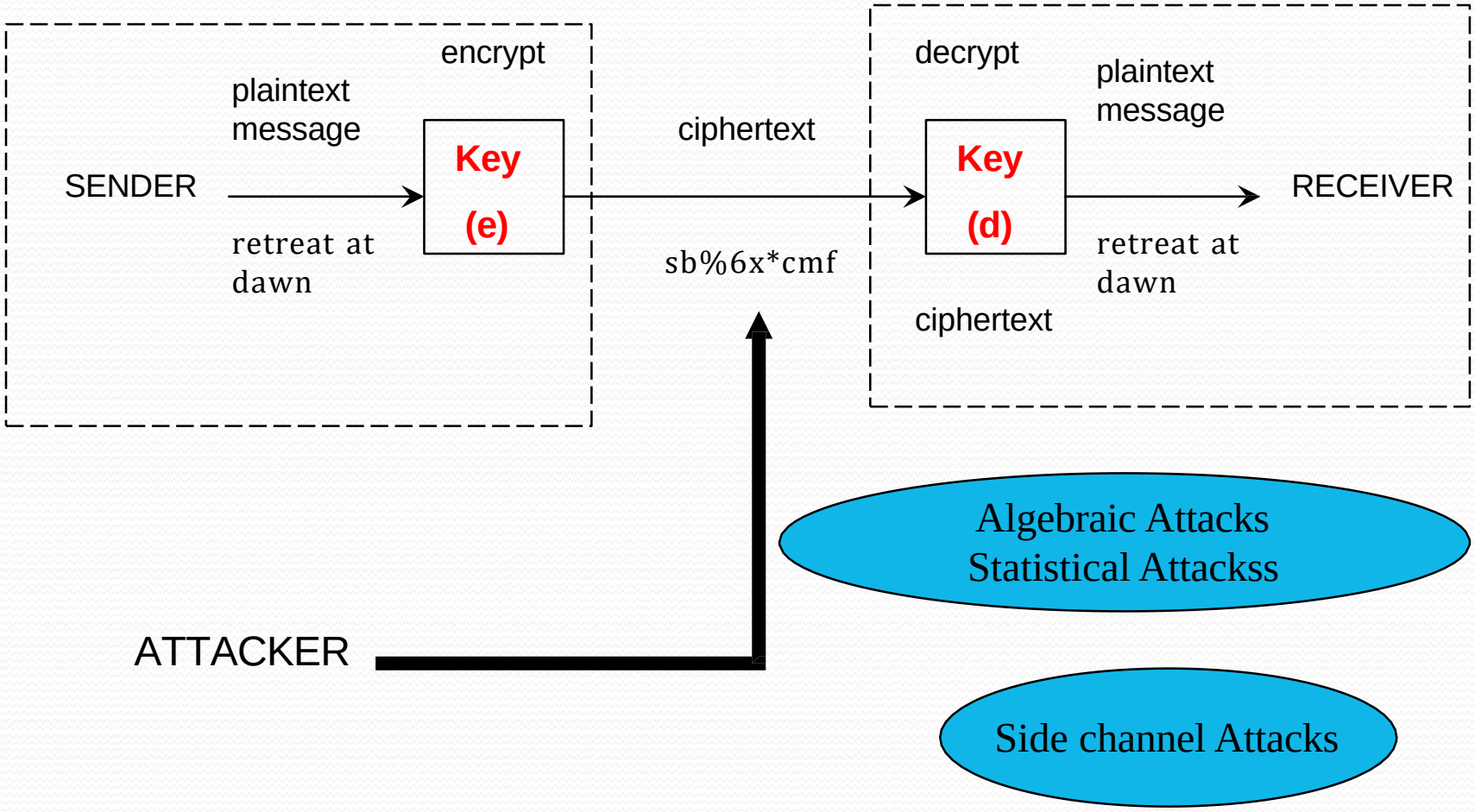
Dept. of Computer Science & Engg.
IIT Kharagpur, India

What is Cryptography?

- The primary goal of cryptography is to secure important data on transit or data on store

- Confidentiality ensures that no one can read the message except the authorized receiver, even if that data is transferred through an insecure medium
- Integrity assures that the received message has not been altered in any way from the original message sent.
- Authentication establishes identity, entity or message authentication.
- Non-repudiation proves that the sender really sent this message

Cryptographic Algorithms



Types of Cryptography

- Symmetric Key/Private Key : The encryption key and decryption key are easily derivable from each other
  - Block Cipher : Fixed blocks of data
  - Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES)
  - Stream Cipher : Block Size = 1
  - eStream Winners Trivium, Grain, MICKEY, Rabbit
  - Hash Function : Variable message
  - SHA3 : Keecak, Grostel
- Asymmetric Key/Public Key : Infeasible to determine the decryption key, d from the encryption key, e
  - Diffie- Hellman, RSA, Elliptic Curve Cryptography

Cryptanalysis/Attacks of Ciphers

Parameters to successfully execute the attack.

- Amount of required input data:
  - Number of input/output data required
- Number of necessary operations:
  - Amount of necessary computations required
- Storage complexity:
  - Amount of memory required
- Number of necessary physical actions :
  - Number of necessary measurements in the case of side channel analysis

Types of Cryptanalysis/Attacks

- Algebraic Analysis

  Linear Cryptanalysis, Differential Cryptanalysis

- Algorithmic / Structural Analysis

  Man-in-the-Middle Attack, Related Key Attack

- Side Channel Analysis

  Power Attack, Timing Attack, Fault Analysis etc.