Introduction

Debdeep Mukhopadhyay
IIT Kharagpur

Cryptography: Definition

- **Cryptography** or *cryptology* is the practice and study of techniques for secure communication in the presence of third parties.
- Constructing and analyzing protocols that overcome the influence of adversaries.
- It is the **scientific study of techniques** for securing digital information, transactions any distributed computations.
- Secure: Related to various aspects such as data confidentiality, data integrity, and authentication.

Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Classical to Modern Cryptography

- Transformation from art to science.
  - Late 20th century significant results appeared.
- Impact:
  - Who uses crypto?
    - Before even 80's largely in the realm of war mongers (so called military leaders) and their support (intelligence organizations).
    - Now it is ubiquitous (exists everywhere).
      - even our ERP has a password.

A wide range of applications

- With the development of distributed computing the applications have grown.
- E-commerce (e-shopping, online payment, online banking)
- Secrecy of mobile communications
- Secure website: https
- Software Privacy: IP protection
- Preventing the thief (not always) from getting access of laptop information.

Setting of Encryption

Encryption

KEY

Decryption

????

- **Kerckhoff's Principle:**
  The cipher must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

Reasons

- This is contrast to a principle called "security by obscurity"
- There are several reasons however a "public"-ly known cipher is preferred:
  1. It is difficult to keep an algorithm secret, compared to say a 128 bits arbitrary string.
  2. A program can be "reverse engineered", not the key which is not part of the program.

Reasons

- Difficult to design ciphers: History has taught that proprietary algorithms have been hopeless.
  - Examples:
    - CMEA (used in CDMA)
    - A5 :

    "A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard. It was initially kept secret, but became public knowledge through leaks and reverse engineering. A number of serious weaknesses in the cipher have been identified."

Reasons

- Consider a company: It is easy to use a single algorithm and share the keys.
- The keys can be (and should be) refreshed at periodic intervals.

State affairs: A prudent approach

- Develop an algorithm after opening it to scrutiny by cryptographers (who are trusted by the Govt).
- Then keep it even secret:
  - Combining the idea of “Kerckhoff;s principle” and “security by obscurity”
- For business purposes, we may use several public algorithms which are not patented.

Attack Models

- Ciphertext only attack: adversary just observes ciphertext
- Known plaintext attack: adversary knows some pairs of plaintexts/ciphertexts under the same key. Then computes the plaintext for a new ciphertext.
- Chosen plaintext attack: Adversary has the ability to obtain the encryptions of plaintexts of its choice.
- Chosen ciphertext attack: The adversary is able to obtain the decryption of some ciphertexts, and then provides the plaintext for a new ciphertext.

Formalism of these concepts

- The initial phases of crypto, have seen several new ciphers and their breaks.
- It was felt necessary to formalize these concepts to give better constructions:
- 4 Principles:
  - **Principle 1:** Formulation of a rigorous and precise definition of security.
  - **Principle 2:** Clearly state the assumptions (unproven facts) on which the security of a cryptographic construction relies.
  - **Principle 3:** Cryptographic constructions should be accompanied by a rigorous proof of security wrt. the security definitions (Principle 1) and assumptions (Principle 2)

Formalization is non-trivial

- Formalize encryption. What is encryption?
  - It is a scheme which keeps the key secret.
  - It is a scheme which keeps the plaintext secret.
  - It is a scheme which keeps all the bits of the plaintext secret.
  - It is a scheme which does not reveal any meaningful information of the plaintext.
  - **It is a scheme which does not allow to compute any function of the plaintext.**

More information needed

- Formalism needs to define the goal: the previous attempt
- Formalism needs to incorporate the power of the adversary:
  - computational power
  - access of information (the attack model)

Rest of the class

- We shall be trying to develop these formalisms for various security notions.