1 Introduction

Terminology

Cryptography: the act or art of writing in secret characters.

Cryptanalysis: the analysis and deciphering of secret writings.

Cryptology: the scientific study of cryptography and cryptanalysis.

Encryption: method for encoding messages.

Decryption: method for decoding messages.

Plaintext: unencrypted message (in the clear).

Ciphertext: encrypted message.

Applications of Cryptography

Example applications:

1. Secure communications
2. Digital Signatures
3. End-to-end encryption
4. Protecting data
5. Storing passwords
6. Online payment
7. Online auctions
8. Electronic voting
9. Digital cash
10. Blockchain

Encryption/Decryption

Encryption is a means of transforming plaintext into ciphertext

- Under the control of a secret key

We write $c = e_k(m)$, where

- m is the plaintext
- e is the encryption function
- k is the secret key

- c is the ciphertext

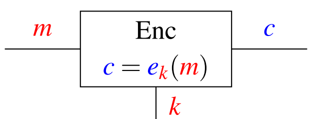
Decryption $m = d_k(c)$, where

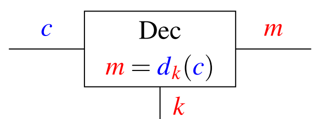
- d is public
- the secrecy of m given c depends totally on the secrecy of k
- each party needs access to the secret key
- This needs to be known to both sides, but needs to be kept secret

Participants

Alice

Bob





- Alice and Bob: two parties who want to communicate securely.
- Eve: an eavesdropper who wants to listen/modify their communication.

Adversarial Model
The number of keys must be large to prevent exhaustive search
Worst case assumptions - assume attacker has:

- Full knowledge of the cipher algorithm
- A number of plaintext/ciphertext pairs associated to the target key

Kerchoff's Principle (1883)
System should be secure even if algorithms are known, as long as key is secret.

The cipher designer must play the role of the cryptanalyst:

- In practice ciphers are used which are believed to be strong
- All this means is that the best attempts of experienced cryptanalysts cannot break them.

Attacks
There are two basic types of attack:

- Passive
- Active

With a passive attack, information is accessed but not modified.

- An administrator reading mail messages being sent across the Internet.
- A hacker gaining access to information contained in bank accounts.

With an active attack, information or the system is modified.

- An administrator modifying mail messages.
- A hacker withdrawing money from a bank account.

Attacks
Some example types of attack:

Ciphertext only attack: ciphertext known to the adversary (eavesdropping)

Known plaintext attack: plaintext and ciphertext are known to the adversary

Chosen plaintext attack: the adversary can choose the plaintext and obtain its encryption (for example, has access to the encryption system)

Chosen ciphertext attack: the adversary can choose the ciphertext and obtain its decryption

Dictionary attack: the adversary builds a dictionary of ciphertexts and corresponding plaintexts

Brute force attack: the adversary tries to determine the key by attempting all possible keys

What is a secure system?

- Every system is susceptible to attack.
- Security is about ensuring that attacks will not be successful.
- A security mechanism prevents an attack from being successful.
  - A password can prevent unauthorized access to a computer.
  - A hand-written signature can prevent someone denying that they entered into a contract.
  - Watermarking in bank notes can prevent forgery.
- A security mechanism detects, prevents, or recovers from a attack.
- A secure system is one in which known threats have been considered and suitable security mechanisms have been incorporated to prevent successful attacks.

Trust

- In any secure system, certain components need to be trusted.
- A trusted component is assumed to behave correctly, i.e., we do not need security mechanisms to prevent it misbehaving.
  - It is common to trust operators of secure systems.
  - It is common to trust software within secure systems.
  - Of course, such trust is based on operators being vetted and software having been assured.
- In general, the number of trusted components in a system should be as small as possible.
- It is common to have components that have limited trust.
  - For example, they may be trusted within a limited part of a system.
  - In addition, their actions may be audited.
- It is also common to divide trust between a number of components.
  - Certain actions may require a number of individuals to agree.
  - For example, cheques may require two signatures.

Security Policies

- To build a secure system we need to:
  - Assess threats.
    - What threats exist?
    - What is the cost if there is a successful attack?
  - Identify trusted components.
  - Determine appropriate security mechanisms to counter threats.
    - What mechanisms will work and what will they cost?
    - How will these various mechanisms work together?
  - Define procedures to ensure the correct operation of the system.
  - Define review and audit mechanisms.
- All this requires a security policy.
- A system is only secure relative to the security policy that it enforces.

Security Objectives
These were originally summarised as the CIA triad:

- Confidentiality: keeping information secret from those not entitled to see it.
- Integrity: ensuring that information has not been altered.
- Availability: ensuring that information can be accessed in an appropriate time-frame.
  - This includes preventing denial of service (DoS) attacks.

The following security objectives are also important:

- Authentication:
  - Entity Authentication: ensuring that the purported identity of an entity is correct.
  - Message Authentication: ensuring that the purported source of information is correct.
- Non-repudiation: ensuring that an entity cannot deny a previous action.

Depending on the particular system, these security objectives can be met by using a combination of cryptographic and non-cryptographic security mechanisms.

Types of Security

- Physical Security: most security is based on ensuring that the physical access to resources is restricted.
- Secrecy: by keeping the existence or details of a system secret, then it may be more secure.
- Personnel Security: personnel who build and operate secure systems need to be trusted.
- IT Security: non-cryptographic mechanisms used in computers, networks, etc.
- Cryptographic Security: mechanisms based on the use of cryptography.

Perfect Security
Is perfect security possible?

- The security of a system is a negative attribute.
  - In general, it is impossible to demonstrate absolute security.
- Security mechanisms have limited applicability.
  - A security mechanism will only prevent a limited number of possible attacks.

- Security mechanisms have associated costs.
  - There is no point using security mechanisms that cost more than the outcome of a successful attack.
- In many circumstances, security requirements evolve.
  - Security is not a static attribute of a system and typically, security must be ”tightened” as attacks occur or threats increase.
- Prevention verses Detection.
  - The ideal is to prevent attacks becoming successful.

Therefore, except for the most trivial of systems, there is no perfectly secure system.

What is a Security Protocol?

- Let us assume that we are operating some system in an environment consisting of a collection of entities or players.
- Some of these entities will be good guys trying to achieve one or more security objectives as part of the system.
- Others will be bad guys trying to attack the system and overcome the security objectives.
- A security protocol is a description of how the good guys should interact with each other to achieve the stated security objectives.
- A security protocol should be able to achieve the security objectives no matter what attacks are mounted by the bad guys.

Security and Networks

- A network is like any other system, except that it is distributed.
- In addition to being physically distributed, ownership may also be distributed.
- The internet is the prime example of the problems associated with network security.
- How can security be realized in such a chaotic environment?
  - The answer is to use security protocols based on cryptography.
- Is cryptography sufficient?
  - No - cryptography is necessary, but it is not sufficient.
  - We still need to use other forms of security.