Introduction

BİL 448/548

Internet Security Protocols

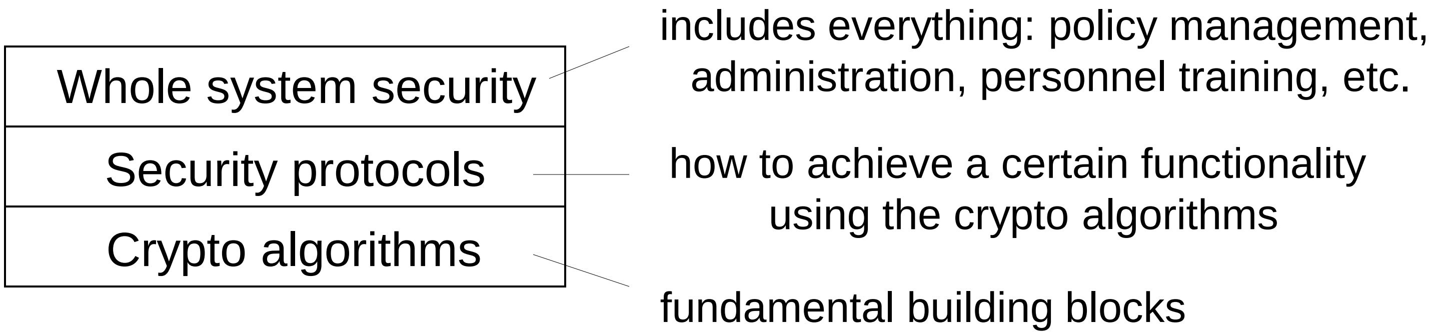
Ali Aydın Selçuk

Information Security

InfoSec:

- Computer Security: deals mostly with access control
- Network Security: deals with communications security

Layers of a Security System:



Whole system security — includes everything: policy management, administration, personnel training, etc.

Security protocols — how to achieve a certain functionality using the crypto algorithms

Crypto algorithms — fundamental building blocks

Network Security

Main Issues:

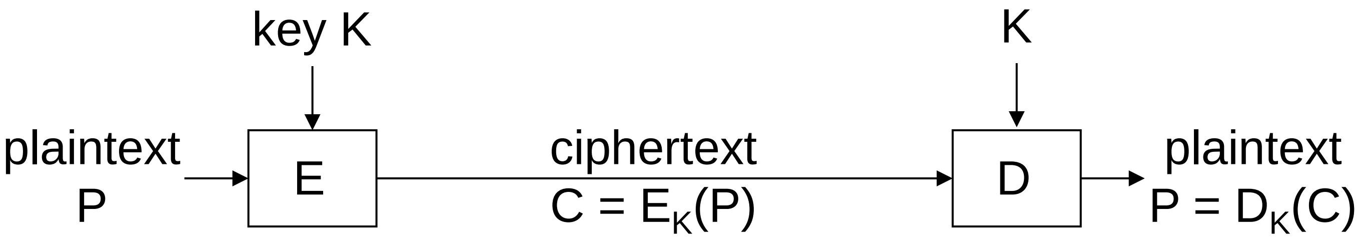
- confidentiality
- authentication
- data integrity

*

- privacy
- anonymity
- non-repudiation
- availability
- traceability

Cryptographic Fundamentals

- Basic encryption:



Key: An easy-to-change, variable parameter of the encryption algorithm.

- Kerckhoffs' principle (1883):
  Security should not rely on the secrecy of the algorithm; everything may be known but the key.

Some Historical Examples

- Shift Cipher:
  - For an n-letter alphabet,
    $P, C, K \in \mathbb{Z}_n$
    $E_K(P) = P + K \bmod n$
    $D_K(C) = C - K \bmod n.$
  - Cryptanalysis: exhaustive key search
- Substitution Cipher:
  - $P, C \in \mathbb{Z}_n$; K is a bijection, f, over $\mathbb{Z}_n$
    $E_K(P) = f(P)$
    $D_K(C) = f^{-1}(C).$
  - Cryptanalysis: frequency analysis

Some Historical Examples

- Vernam Cipher (1917):
  - $P, C, K \in \{0,1\}^{\ell}$, for some $\ell \geq 1$.
    $E_K(P) = P \oplus K$
    $D_K(C) = C \oplus K$
  - Problem: Key needs to be transmitted, which is as long as the message.
  - Used for top-secret applications (E.g., Washington-Moscow red line)

Vernam Cipher (cont.)

Definition (Shannon, 1949): "Perfect Secrecy": Ciphertext leaks no info about the message.

Theorem: Vernam cipher has perfect secrecy if each key bit is generated uniformly randomly.

Theorem: For perfect secrecy, the entropy of the key has to be at least as high as the entropy of the message. (i.e. the key has to be at least as long as the message.)

Modern Ciphers

Shortcomings of historical systems:

- Substitution cipher: Small size of the input domain, which enables frequency analysis.
- Vernam cipher: Unlimited key size, which makes key generation and exchange a problem.

Modern ciphers:

- Block ciphers: Increasing the size of the input alphabet (i.e. blocks) for substitution
- Stream ciphers: Using a PRNG for generating the key stream