POLYTECH
PARIS-SUD

Lecture 1
Introduction

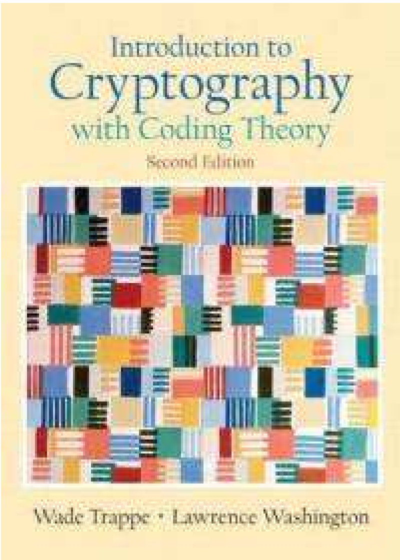
Système et Sécurité

Le Professeur

- Fabio Martignon
- Bureau :
  - LRI, Batiment 650
  - Bureau 244
- Tel. : 01.69.15.68.16
- E-mail : fabio.martignon@lri.fr

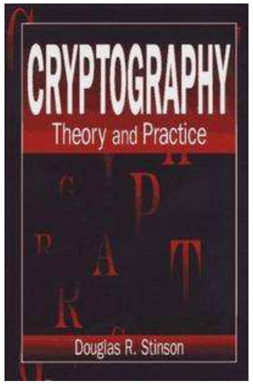
Matériel Didactique

- Livre Conseillé :
- Introduction to Cryptography with Coding Theory. W. Trappe, L. C. Washington.



☑ **2ème Edition**

☑ **… mais aussi l'édition précédente**



- Cryptography : Theory and Practice. Douglas R; Stinson.

Matériel Didactique

- Transparents
- Autre matériel signalé durant le cours et disponible sur la page Web du cours
- Internet

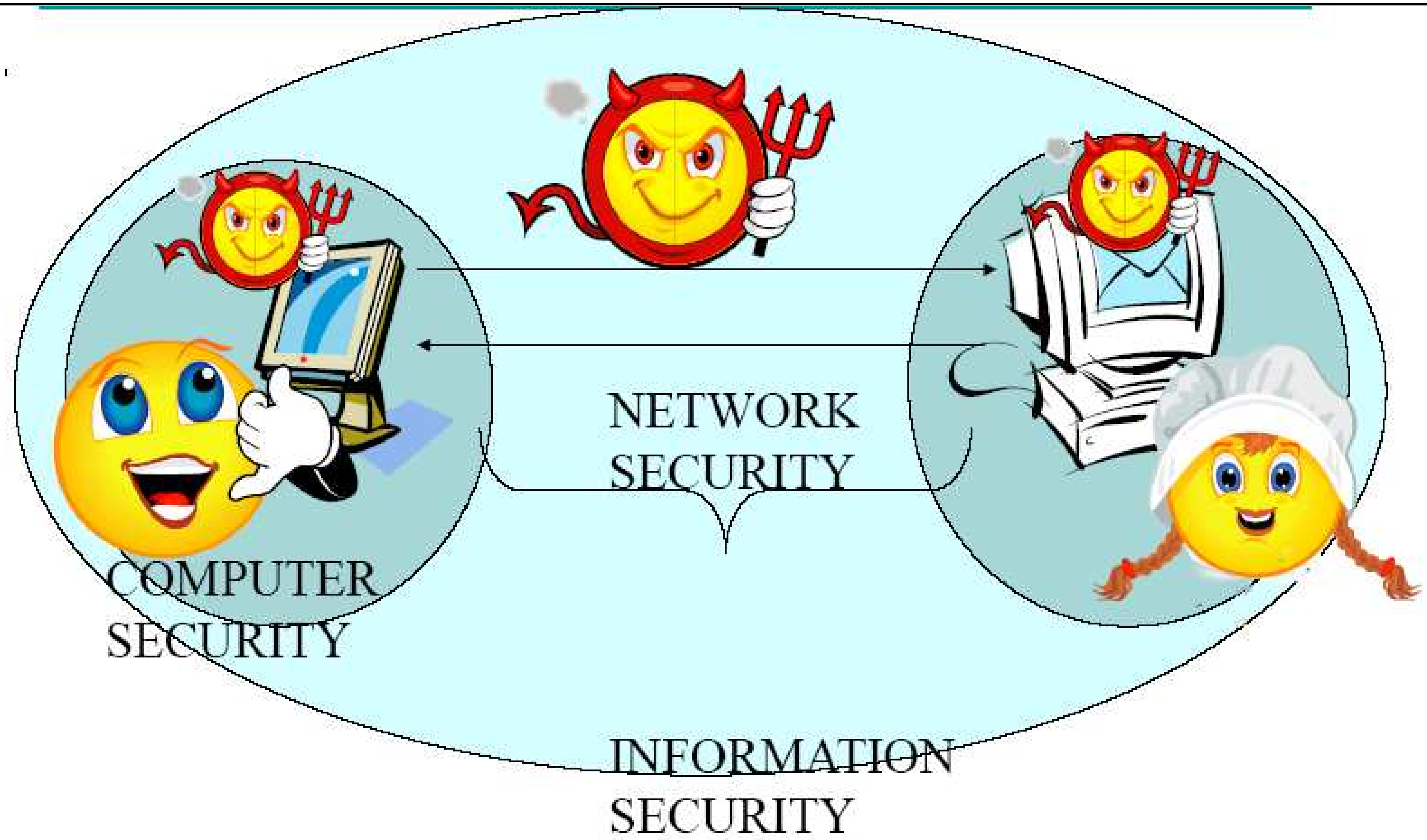
- Page Web du cours :

http://www.lri.fr/~fmartignon/systeme_securite.html

ou, alternativement :

http://129.175.15.11/~fmartignon/systeme_securite.html

Cryptography



Approaches to Secure Communication

- Steganography
  - "covered writing"
  - hides the *existence* of a message

- Cryptography
  - "hidden writing"
  - hide the *meaning* of a message

Goals of Cryptography

- The most basic problem: ensure security of communication over insecure medium
- Basic security goals:
- **privacy** (secrecy, confidentiality)
  - only the intended recipient can see the communication
- **authenticity** (integrity)
  - the communication is generated by the alleged sender

Example: Using Your Cell Phone

- Service provider goals:
  - Make sure the right client is billed for the service
  - Only clients that paid get the service
- Client goals:
  - Privacy, nobody can understand his communication
  - Anonymity, nobody can reveal his identity to unauthorized parties or track him
  - He’s not charged for other’s people conversations
- Cryptography can provide the tools to achieve these goals

Basic Terminology in Cryptography

- cryptography
- cryptanalysis
- cryptology
- plaintexts
- ciphertexts
- keys
- encryption
- decryption

What Cryptography is About?

- Constructing and analyzing **protocols** which enable **parties** to achieve objectives, overcoming the influence of **adversaries.**
  - a protocol (or a scheme) is a suite of algorithms that tell each party what to do
- How to devise and analyze protocols
  - understand the threats posed by the adversaries and the objectives (goals)
  - think as an adversary

Actually

- **Cryptography:** the study of mathematical techniques related to aspects of providing information security services (construct).
- **Cryptanalysis:** the study of mathematical techniques for attempting to defeat information security services (break).
- **Cryptology:** the study of cryptography and cryptanalysis (both).

Phases in Cryptography's Development

- Cryptography is driven by computing and communication technology

1) First stage, paper and ink based scheme
2) Second stage, use cryptographic engines
3) Third stage, modern cryptography
   – relying on mathematics and computers
   – information-theoretic security
   – computational security

Secret-key vs. Public-key Cryptography

- Secret-key cryptography (a.k.a. symmetric cryptography)
  - encryption & decryption use the same key
  - key must be kept secret
  - key distribution is very difficult
- Public-key cryptography (a.k.a. asymmetric cryptography)
  - encryption key different from decryption key
  - cannot derive decryption key from encryption key
  - higher cost than symmetric cryptography

Some Goals of Modern Cryptography

- Pseudo-random number generation
- Non-repudiation: Digital signatures
- Zero-knowledge proof
- E-voting
- Secret sharing

Example: Cellular Networks Authentication

- Focus:
  - **Provide authentication, confidentiality and anonymity of the communication**
- Assumptions
  - There is a long-term relationship between the client and the network operator (home network) in the form of a contract
  - The long-term relationship is represented by a long-term secret key shared by the client and the network, which serves as basis for identification

Cellular Networks Authentication

- SIM (Subscriber Identity Module): secret PIN (personal identification number) and the long term secret key
- Storing the key on the SIM allows the portability of the service from one phone to another
- Authentication is based on a *challenge response* protocol (in this way the secret key is *not* sent on the radio channel) - this is where cryptography plays its role: we will study such protocols

A Symmetric Cipher

- A Cipher (*K, P, C*, **E**, **D**)
  - *K* : the key space
  - *P* : the plaintext space
  - *C* : the ciphertext space
  - **E**: $K \times P \rightarrow C$: the encryption function
  - **D**: $K \times C \rightarrow P$: the decryption function
    - Given a key K and a plaintext P,

$$\mathbf{D}(K, \mathbf{E}(K,P)) = P$$

Kerckhoffs's Principle

- The security of a protocol should rely *only* on the secrecy of the keys, while protocol designs should be made public (1883)
  - **security by obscurity does not work**

  (there are many examples, WEP, voting machines…)

Auguste Kerckhoffs (19 January 1835 – 9 August 1903) was a Dutch linguist and cryptographer who was professor of languages at the School of Higher Commercial Studies in Paris in the late 19th century.

How Do You Know a Cipher is Secure?

- Show that under the considered attack model, security goals are NOT achieved (break it)
- Show that under the considered attack model, security goals are achieved (evaluate/prove)

Breaking Ciphers…

- There are different methods of breaking a cipher, depending on:
  - the type of information available to the attacker
  - the interaction with the cipher machine
  - the computational power available to the attacker

Breaking Ciphers…

- **Ciphertext-only attack**:
- The cryptanalyst knows **only the ciphertext**. Sometimes the language of the plaintext and the used cipher are also known.
- The goal is to find the plaintext and the key.

- **NOTE**: any encryption scheme vulnerable to this type of attack is considered to be completely insecure.

Breaking Ciphers (2)

- **Known-plaintext attack**:
  - The cryptanalyst knows **one or several pairs of ciphertext and the corresponding plaintext.**
  - The goal is to find the key used to encrypt these messages or a way to decrypt any new messages that use that key.
  - How does the cryptanalyst get the pairs of ciphertext and plaintext?

Breaking Ciphers (3)

- **Chosen-plaintext attack**
  - The cryptanalyst has obtained temporary access to the <u>encryption</u> machinery
  - Hence he **can choose a number of messages and obtain the corresponding ciphertexts for them**
  - The goal is to deduce the key used in the other encrypted messages or decrypt any new messages using that key.
- It can be **adaptive**, the choice of plaintext depends on the ciphertext received from previous requests.

Breaking Ciphers (4)

- **Chosen-ciphertext attack**
- The cryptanalyst has obtained temporary access to the <u>decryption</u> machinery
- Similar to the chosen-plaintext attack, but the cryptanalyst **can choose a number of ciphertexts and obtain the corresponding plaintexts.**
- It can also be **adaptive**: the choice of ciphertext may depend on the plaintext received from previous requests.

Breaking Ciphers

- Obviously these 4 types of attacks have been enumerated in *increasing* order of strength
- Note that a chosen-ciphertext attack is relevant to public-key cryptosystems

Models for Evaluating Security

- **Unconditional (information-theoretic) security**
  - **Assumes that the adversary has unlimited computational resources**.
  - Plaintext and ciphertext modeled by their distribution
  - Analysis is made by using probability theory.
  - For encryption systems: **perfect secrecy** concept, observation of the ciphertext provides no information to an adversary.

Models for Evaluating Security (2)

- **Provable security:**
  - Prove security properties based on assumptions that it is difficult to solve a well-known and supposedly difficult problem (example: computation of discrete logarithms, factoring).

Models for Evaluating Security (3)

- **Computational security (practical security)**
  - Measures the amount of computational effort required to defeat a system using the best-known attacks.
  - More formally: we might define a cryptosystem to be *computationally secure* if the **best** algorithm for breaking it requires at least N operations, where N is some specified, very large number
    - The problem is that no known practical cryptosystem can be proved to be secure under this definition
  - In practice, people call a cryptosystem "computationally secure" if the **best <u>known</u>** method for breaking it requires an unreasonable large amount of time.
  - Sometimes related to hard problems, but no proof of equivalence is known.

Models for Evaluating Security (4)

- **Ad hoc security (heuristic security):**
  - Variety of convincing arguments that every successful attack requires more resources than the ones available to an attacker.
  - Unforeseen attacks remain a threat.
  - **THIS IS NOT A PROOF**