Cryptography Basics

Prof.dr. Ferucio Laurențiu Țiplea

Fall 2021

Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Cryptography

Cryptography is a handy tool in information security, being the basis of many security mechanisms that offer services such as:

1. confidentiality
2. integrity
3. authentication
4. non-repudiation

However:

- Cryptography is not the solution to all security problems!
- If not properly implemented, cryptographic tools may leak information very subtly without you realizing it!

Cryptographic technologies

There are two main cryptographic technologies:

1. Symmetric key (also called secret key, single key, conventional)

   Rough meaning: uses the same secret key to encrypt and also decrypt

2. Asymmetric key (also called public key)

   Rough meaning: uses a public key to encrypt and a private key to decrypt

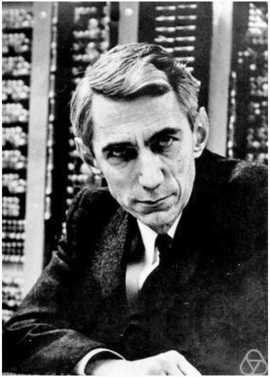
Symmetric key technology usually requires a key distribution mechanism!

Proving security in cryptography

Two main approaches to security:

1. Try to exhibit an attack, such as: brute-force, man-in-the-middle, meet-in-the-middle, frequency analysis, replay, birthday, dictionary etc. attack. Then:
   - attack found $\Rightarrow$ system insecure
   - attack not found $\Rightarrow$???
2. Try to prove security (provable security). Two milestones:
   2.1 Perfect security (Shannon (1949))
   2.2 Computational security (Goldwasser and Micali (1984))

Perfect security



Claude Shannon: "The father of Information Theory"

C. Shannon. Communication Theory of Secrecy Systems, Bell System Technical J., vol. 28, no. 4, 1949, pp. 656–715.

Perfect security or unconditional security or information-theoretic security means that the ciphertext reveals no information about the plaintext to an adversary with unlimited power.

Computational security

Shafrira Goldwasser: Gödel Prize (1993, 2001), Turing Award (2012)

Silvio Micali: Gödel Prize (1993), Turing Award (2012)

Semantic security: an adaptation of Shannon's perfect security to the computational setting, considering only adversaries having bounded computational resources.

Provable security

Provable security also known as reductionist security: security can be proven by reduction to well-studied (hard) problems.

Provable security entails:

- A security model $\mathcal{S}$ for the cryptographic scheme
  1. Security goal, such as semantic security (SS), indistinguishability (IND), non-maleability (NM), collision resistance, non-forgery etc.
  2. Attack model, such as chosen plaintext attack (CPA) or chosen ciphertext attack (CCA1 and CCA2)
- A problem together with a hardness assumption $\mathcal{H}$ about it
- A reductionist proof: $\mathcal{H} \leq \mathcal{S}$

Many of the ciphers used today in practice are not proven secure nor known attack methods against them!

References

Goldwasser, S. and Micali, S. (1984). Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715.