ELE2742 / ENG1467 - PUC-Rio, 2019.1

Lecture 1: Introduction

DATE

Lecturer: Yi-Fan Tseng *Scribe: Yi-Fan Tseng*

1 Terminology and Basic Assumption

We first briefly introduce the terms and some concepts for cryptography [1].

- **Cryptography** or **Cryptology** is a science about constructing and analyzing protocols that prevent third parties or the public from reading private messages.
  Cryptography = “kryptós”(hidden) + “graphein”(to write)
  Cryptology = “kryptós”(hidden) + “lógos” (message)
- **Encryption** is the process of converting ordinary message (called *plaintext*) into messy form (called *ciphertext*).
- **Decryption** is the reverse of encryption.
- **Key** is a piece if information (or a parameter) that determines the functional output of a cryptographic algorithm.
- **Cryptosystem** is a suit of cryptographic algorithms. For instance, a cryptsystem for encryption includes three algorithms: *Key Generation*, *Encryption*, *Decryption*.
- **Cryptalanalsys** is the study of methods for breaking cryptosystems.
- **Adversary**: The role who wants to break a cryptosystem. A.k.a. attacker.

Modern cryptography is the intersection of *mathematics*, *computer science*, *electric engineering*, *communication science*, and *physics*. Generally speaking, a cryptosystem provides the following functionality based on the requirements in practice [3, 5]

- Secrecy or Privacy: Preventing illegal receivers from discovering the plaintext
- Authenticity: Confirming the validity of the information source
- Integrity: Checking that the received message has not been tampered, paritally replaced, or deleted.
- Non-repudiation: Guaranteeing that an author of a statement is not capable of denying it authorship.

Basic Assumption. For the security of a cryptosystem, the adversary should be given the knowledge of the cryptosystem as much as possiple, and put restrictions as less as possiple.

Kerckhoffs's Principle [2, 4] A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

References

[1] Cryptography.

[2] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, Sept. 2006.

[3] W. Diffie and M. E. Hellman. Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, 67(3):397–427, March 1979.

[4] D. Kahn. *The Codebreakers, The Story of Secret Writing*. New York: Macmillan, 1967.

[5] D. E. Robling Denning. *Cryptography and Data Security*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1982.