Encryption Algorithms for Secure Communication on the Internet

Prof. Dr. Thomas ENGEL*, PhD Student Asya MITSEVA†, BICS student: Desislava MARINOVA ‡
Faculty of Science, Technology and Communication, University of Luxembourg, Luxembourg

*Email: *thomas.engel@uni.lu, †asya.mitseva@uni.lu, ‡desislava.marinova.002@student.uni.lu*

***Abstract*—This document is a template for the scientific and technical report that is to be delivered by any BiCS student at the end of each Bachelor Semester Project (BSP). The Latex source files are available at: https://github.com/nicolasguelfi/lu.uni.course.bics.global**

This template is to be used using the Latex document preparation system or using any document preparation system. The whole document should be in between 6000 to 8000 words and the proportions must be preserved. The other documents to be delivered (summaries, . . .) should have their format adapted from this template.

1. Introduction (± 5% total words)

We are living in the information age enabled by computing and communication technologies whose rapid evolution is almost taken for granted today. This is an age dense with electronic connectivity, eavesdropping and fraud. Thus, information is an asset that has precious value like any other. Societys reliance on a changing panoply of information technologies and technology-enabled services, the increasing global nature of commerce and business, and the ongoing desire to protect freedoms all suggest that future needs for data security is vital. Network based attacks spring up every day, distance does not matter anymore since data has been digitalized and there is the issue of privacy being collected, processed and misrepresented. For this reason, the disciplines of cryptography and network security have matured. Thus, internet security is complex yet fascinating. To develop a security mechanism (algorithm or protocol) one must always consider potential attacks, take countermeasures, act like an intruder and go against ones own intuition and exploit eventual weaknesses in the algorithm.

We dive into the terminology that governs our topic in the next paragraph. The word cryptography comes from two Greek words meaning secret writing [1]. Cryptography is a vast, rich subject. It is the art and science of concealing meaning, of keeping the enciphered information secret and of designing and analyzing encryption schemes. It involves mathematics as a supporting tool. Cryptanalysis is the breaking of codes and uses statistical and mathematical approaches. The areas of cryptography and cryptanalysis together are called cryptology. The basic component of cryptography is a cryptosystem which is based on substitution (it changes characters in the plaintext to produce the ciphertext) and permutation (an ordered sequence of elements in a finite set with each character appearing only once). If someone wants to break the ciphertext, knowing the algorithm but not the specific cryptographic key, there are 3 main types of attacks [Ref: Stallings, 7th ed, p.90]: - ciphertext only attack ciphertext known, the goal is to find the corresponding plaintext. The key may be found as well if possible. (A Caesar cipher is susceptible to a statistical ciphertext-only attack) - known plaintext attack both ciphertext and plaintext and known; the goal is to find the key - chosen plaintext attack specific plaintexts are enciphered in order to find out the corresponding ciphertexts and the goal is to find the key. a good cryptosystem protects against all three types of attacks.

We often stumble upon impending security threats such as information leakage; integrity violation; denial of service; illegitimate usage; trojan horses; insider attacks; problems related to access or authentication control. Thus, there are instilled security requirements of utmost importance. We present them as follows: confidentiality; integrity; authentication; availability; access control; non-repudiation, which are often intermingled. Hence, encryption is promising to ensure these security mechanisms.

In order to make information secret, we use a cipher an algorithm that converts plain text into ciphertext, which is in unreadable form, unless we have a key that lets us convert back the cipher. The process of making text secret is called encryption, and the reverse process is called decryption.

There are two types of encryption: symmetric and asymmetric. For this project, we shall focus mainly on symmetric cryptography. It comprises a single key for both encryption and decryption and it is the preferred choice when we need to encrypt large amounts of data. On the other hand, asymmetric cryptography, also called public key and two-key, consists of two keys: public and private. The public key is used to encrypt the message, whereas the private key is used to reverse the encryption. This method cannot deal with large quantities of data due to the runtime of supporting processes employed. However, it is more secure when we want to transfer over an insecure channel. Nevertheless, the

choice to be made on which system to use for encryption and decryption depends on the purposes and on each algorithms functions.

2. Project description (± 10% total words)

2.1. Domain

The report draws on a variety of disciplines. However, it is impossible to appreciate the vastness and significance of the topic in a limited amount of content pages. Nevertheless, we attempt at making the report self-contained by providing the reader with an intuitive understanding of our survey and application results. The domains that are associated with our project are: - Internet security: ”measures to protect data during its transmission over a collection of interconnected networks” [Stallings, ed.3,] - Computer Security: ”generic name for the collection of tools designed to protect data and to thwart hackers and malicious software (viruses) ” [Stallings, ed.3,]; at its heart there are three key objectives: confidentiality, integrity and availability - Cryptographic primitives - Symmetric-key cryptography - cryptographic algorithms: ”study of techniques for ensuring the secrecy and/or authenticity of information =¿ 3 main studies of this category (1) symmetric encryption, (2) asymmetric encryption and (3) cryptographic hash functions” [Stallings, 5th ed, p. 3]

2.2. Objectives

The objectives of this project are three-fold. It We aim for a comprehensive survey of both principles and practice of cryptography and network security. In a first part, we address a highly needed background material. Our main focus falls on symmetric encryption, including classical and modern algorithms. We give a basic introduction to the concepts of block ciphers and stream ciphers and how they obtain their security. We put emphasis on DES, AES (+ other??) algorithms. Then, we implement an encrypted chat system that could be of use to provide network security.

2.3. Constraints

Our project takes into account substitution/transposition; block/stream ciphers but we do not consider: - Asymmetric ciphers (public-key algorithms, including RSA and elliptic curve); - Data integrity algorithms (cryptographic hash functions (message authentication codes (MACs); digital signatures)); - Authentication techniques: key management and key distribution topics (protocols for key exchange)

3. Background (± 15% total words)

3.1. Scientific

3.2. Technical

4. BSPro - A First Bachelor Semester Project in BiCS-land

4.1. Requirements (± 15% total words)

Describe here all the properties that characterize the deliverables you produce. It should describe what are those deliverables, who are the actors exploiting the deliverables, what are the expected functional and non functional qualities of the deliverables.

4.2. Design (± 20% total words)

Provide the necessary and most useful explanations on how those deliverables have been produced.

4.3. Production (± 20% total words)

Provide descriptions of the deliverables concrete production. It must present part of the deliverable to illustrate and explain its actual production.

4.4. Assessment (± 15% total words)

Provide any objective elements to assess that your deliverables reached or not the requirements described above.

Acknowledgment

The authors would like to thank the BiCS management and education team for the amazing work done.

5. Conclusion

The conclusion goes here.

References

[1] BiCS Bachelor Semester Project Report Template. https://github.com/nicolasguelfi/lu.uni.course.bics.global. University of Luxembourg, BiCS - Academic Bachelor in Computer Science (2017).
thebibliography1

[2] Wikipedia. Cryptography. https://en.wikipedia.org/wiki/Cryptography

6. Appendix

All images and additional material go there.