Brandenburg University of Technology
Cottbus-Senftenberg
IT Security Group

Exercise Class
"Introduction into Cyber Security"
Winter Term 2018/2019

Introduction into Cyber Security – Secret Key Cryptography

Deadline: 26th November, 2018

Topics

The main goals of cryptography are confidentiality, integrity, non-repudiation and authenticity. This first practical exercise is a study of historical and modern cryptographic algorithms and the methods to analyze encrypted text. The books listed in the attachment [2] [3] will expand your knowledge of basic cryptographic methods.

In this exercise we will work with the open source tool *CrypTool*. The tool serves as a demonstration and reference program to cryptography. You can either download the tool from the website [1] or use the preinstalled version in the computer pool (VG1C, room 0.03). The following tasks assumes the usage of *CrypTool*, *Version 1.4.41* and is not 100% compatible with other versions!

CrypTool provides a lot of historical and modern cryptographic algorithms and adequate analysis methods to study and break weak encrypted messages. Brute-Force attacks against strong symmetric key cryptography are possible as well. The tool also offers visualization capabilities. This makes *CrypTool* a handy tool to understand the complex world of cryptography.

1 Preparation

To get familiar with *CrypTool* you should start with the pre-installed scenarios offered by *CrypTool*. You can find these scenarios under *Help* → *Scenarios (Tutorials)*. Try to understand the demonstrated analysis/attack for every scenario presented below. Think about reasons why these attacks were possible at all.

1.1 Using CrypTool in the computer pool

If you were not able to solve this lab exercises on your personal computer, you can use the pre-installed CrypTool in the computer pool (VG1C, room 0.03) by using the following instructions:

1. Log in with your BTU-Account to one of the computers and choose Windows as your operating system.

2. You can find CrypTool in the system menu or on the desktop.

3. The manual page of CrypTool can be opened by pressing F1.

If you want to solve the task on your own computer, please use CrypTool in the version $1.4.41$ The program can be downloaded from this website [1].

1.2 Caesar Cryptography

This scenario introduces you to the classical Caesar algorithm and its possible methods of analysis.

Hints:

1. To de- and encrypt the Caesar-Cipher choose the menu *Encrypt/Decrypt* $\rightarrow$ *Symmetric (classic)* $\rightarrow$ *Caesar/Rot-13*.

2. To calculate and visualize entropy use *Analysis* $\rightarrow$ *Tools for Analysis*.

3. The Cyphertext-only attack can be started by using *Analysis* $\rightarrow$ *Symmetric Encryption (classic)* $\rightarrow$ *Cyphertext-only*.

1.3 Vignère Cryptography

This scenario introduces you to the classical Vignère algorithm and its possible analysis methods.

1.4 Mono-alphabetic Substitution

The mono-alphabetic substitution is a generalization of the Caesar algorithm presented before. It substitutes the underlying alphabet of plain text by an arbitrary chosen alphabet. The scenario (tutorial) shows that there is still the possibility for an easy cryptanalysis.

Hints:

1. To analyze the cypher you have to choose the menu entry *Analysis* → *Symmetric Encryption (classic)* → *Cyphertext-only* → *Substitution*.

2. If you know the language of the text to analyze it is recommended to use *Method 2* in the analysis dialog.

3. The option for the extended analysis may not be helpful in any scenario. Please consider potential negative results of your chosen option.

1.5 XOR Cryptography

This scenario introduces you to the compression algorithms and how they could significantly improve the security of the cypher.

Hints:

1. To compress enter the menu entry *Indv. Procedures* → *Tools* → *Compress*.

2. After compression a XOR encryption can be added.

1.6 Vernam Cryptography

The vernam cryptography is just a different name for the one-time-pad where the key and the plain text have the same length. Please, walk through the scenario provided by CrypTool.

1.7 Triple DES Cryptography

This scenario presents the widespread DES-EDE3-CBC algorithm and how it can be attacked by brute force attacks in case of short keys. How does the program know if the tested key is the right one?

2 Main Task

The following three tasks are mandatory and must be submitted via moodle before the end of the deadline. The number of submitted files is limited to three files. Submit a separate compressed file (.7z, .tar, .tgz, .zip) for each of the three tasks.

Task 01

The file *Cry-Rijndael-groupXY.hex* has been encrypted by using mono-alphabetic substitution and the AES algorithm. Mono-alphabetic substitution is the first method used, followed by AES. The AES encryption is based on a weak key (key length of 128 bit), which only uses the first 24 bits of the key. The rest of the key was padded by zeros. Your task is to decrypt both stages of *Cry-Rijndael-groupXY.hex*. Submit the resulting plain text and both keys.

Task 02

From the files *sentences1.txt* and *sentences2.txt* generate two keys A and B which fulfill the following requirements: the key A applied to the file *groupXX.cryp* (cypher-text) results in the plain text of *sentences1.txt*. They key B applied to the same cypher-text should result in the plain-text of *sentences2.txt*. Submit both keys A,B as well as the used decryption algorithm.

Task 03

Along with this task sheet you have received the file *groupXX.zip*. This compressed zip file was encrypted by an 8-byte long XOR-key. The compression was done with the default option. Due to the standardization of the zip-format there are certain parts (header, footer, . . .) that occur within

the file. Find and use this additional information to decrypt the given file. Your task is to decrypt the given file. Submit the 64-bit key used for the encryption.

Hint:

1. All tasks can be solved within CrypTool.

   Use Analysis to Generate 8 Byte keys -> Use Zip Header 40 bit Info to generate 5 bit keys,

References

[1] CrypTool. *CrypTool: Cryptography for everybody. Download section*. 2018. URL: https://www.cryptool.org/en/ct1-downloads (cit. on pp. 1, 2).

[2] P. B. Esslinger and C. Team. *Learning and Experiencing Cryptography with CrypTool and SageMath*. 2018. URL: https://www.cryptool.org/images/ctp/documents/CT-Book-en.pdf (cit. on p. 1).

[3] W. Stallings. *Cryptography And Network Security : Principles And Practice*. 7th. Pearson Education, 2016. ISBN: 9788178089027 (cit. on p. 1).

Good luck!