To do: Receive a grade

Due: Monday, 16 December 2024, 11:59 PM

Practical assessment

The Scenario

You are provided with online resources (web sites), a primary resource and an additional set of resources, should you want to explore. These resources address cryptography and elements of cryptanalysis of ciphers and provide a means of demonstrating them online so you could interact with the ciphers by providing information samples and seeing the cipher text. After exploring the primary site, you will write a report using the guidelines mentioned.

The Primary Resource

(All resources are accessible through the **Reading list @ Liverpool**)

The 'CrypTool Portal' (*CrypTool Portal*) web site provides a practical approach to cryptography. There are collections of online tools for that demonstrate the working of various ciphers and the SHA256 hash (see the section titled "Ciphers" on the page). The section titled Cryptanalysis lists the typical approaches taken to guess the keys of classical and modern ciphers.

1. Pick up any THREE classical ciphers from
   - ADFG(V)X - CrypTool Portal
   - Beaufort - CrypTool Portal
   - Caesar / ROT13 - CrypTool Portal
   - Column transposition - CrypTool Portal
   - Vignéré and its variants - CrypTool Portal
   - Rail Fence - CrypTool Portal

understand the algorithms (Click the "Description" tab after choosing the cipher), try out the examples using your own text to generate the cipher text, and think about how you might go about attacking the cipher text to guess the keys.

1. Cryptanalysis describes automated techniques to break specific ciphers. Explore the types of cryptanalysis methods from the Cryptanalysis section on the web page. Give a thought to which of these you might deploy as a technique to crack your choice (above) of the classical ciphers?
2. Now, have a look at the modern cipher AES at 'AES (step-by-step)' (*CrypTool Portal)* on the web page in the Ciphers section. Follow it up with clicking on Distributed AES Analysis in the Cryptanalysis section('Distributed AES Analysis' (*CrypTool Portal*)). How complex would breaking the AES be compared to breaking the classical ciphers?
3. A cryptographic hash function is a procedure that takes an arbitrary block of data and returns a fixed-size bit string. Explore the SHA256 hash ('SHA256' (*CrypTool Portal*)), study the algorithm, and play with the implementation (create hashes automatically given any input).

Additional Resources

Here is a list of additional sites that you might want to explore if you require to:

- Ciphers | CryptoClub
- CyberChef | Github
- Crank | CRyptANalysis toolKit
- Modular conversion, encoding and encryption online | cryptii
- Online Cryptography Tools
- Online Cryptography Tools
- Online Cryptography Tools
- The Ciphertexts | Simon Singh
- Cipher Challenge | Simon Singh
- crypto101 | Githhub

Reading list @ Liverpool

Your task

You are required to produce a report regarding outcomes from engaging and attempting to use the cryptographic and the cryptanalytic methods. Your report should be structured as follows:

- Introduction to cryptography and cryptanalysis tools and techniques, describe the details of a range of cryptographic ciphers, and an overview of the methods and techniques used to cryptanalysis.
- Perform a comparative study and discussion on the cryptanalysis techniques for classical ciphers. The discussion should highlight the characteristics of the cipher and the associated technique to break the cipher, along with the reason for the suitability of the technique. You could additionally mention the strengths and weaknesses of the technique, performance, usefulness, real applications of these techniques and relevant tools. Following the discussion, illustrate the comparison concisely in a table.
- Briefly discuss the complexity of the cryptanalysis of a modern cipher such as AES and classical ciphers you have chosen to discuss.
- Reflect on your learning experience of using the ciphers and cryptanalysis techniques you have explored on the web site. Specifically, you should identify what went well, what you learned, how you solved issues, and how this experience will help you learn cryptography further, and help you design and implement security solutions in your future work potentially.
- A conclusion to summarise your findings is also necessary.

You could use the references listed below as well as any other relevant references.

References

Carter, B. and Magoc, T., 2007. Classical ciphers and cryptanalysis. space, 1000, p.1.

Kopal, N., 2018, June. Solving Classical Ciphers with CrypTool 2. In HistoCrypt (pp. 149-010).

Deliverable and deadline

You should submit your assignment as a PDF document by the end of week 08.

Please, use **this template document** to write your report.

Report - The maximum word count for this assessment is 2500 words. References, titles, and images are not included in the word count. **As per the assessment length policy, penalties will be applied to assessments which exceed this length.**

Add submission

Submission status

Attempt number	This is attempt 1.
Submission status	No submissions have been made yet
Grading status	Not marked
Time remaining	21 days 8 hours remaining