CSE 2203 (2018-2019)

### TUTORIAL 1 – INTRODUCTION TO CRYPTOGRAPHY

**SYMMETRIC CRYPTOGRAPHY – CLASSICAL CIPHERS**

Tutorial 1 is divided into two activities –1) a Series of Videos and 2) a practical activity.

***Videos***

1. Cryptography Introduction (Alice, Bob and Eve)

Tutor Note: Communicating without hiding the fact of the communication: just hiding the ***meaning*** of the communication. Steganography is the opposite – hiding the fact of the communication.

Video Link: <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography>

1. Caesar Cipher (Explanation of Cipher with cryptanalysis through Frequency Analysis)

Tutor Note: ***Frequency Analysis*** uses the patterns inherent in each language. For example, in the English Language, ‘E’ is the most common letter that is used. Hence, if we use Caesar Cipher and encode ‘E’ as ‘H’, in the ciphertext, ‘H’ will be the most commonly used letter. A cryptanalyst can deduce that ‘H’ corresponds to ‘E’ and thus begin to crack the cipher.

Video Link: <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher>

1. Frequency Fingerprint Exploration Activity

Tutor Note: This is an activity to help students deepen their understanding of Frequency Analysis. All of us use certain words more frequently than others. There is an underlying pattern to the way we communicate, though we realise it not.

Activity Link: <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/pi/frequency-fingerprint-exploration>

1. Polyalphabetic Ciphers

Tutor Note: With Caesar Cipher – each letter of plaintext is encrypted using the same key (3). This led to successful cryptanalysis of Caesar Cipher using Frequency Analysis. Hence the move to using more than one alphabetic to encrypt a message. In the Khan Academy example, they used the word SNAKE as a key. S uses a shift of 19. N uses a shift of 13. A uses a shift of 1, K uses a shift of 11 and E uses a shift of 5. Hence, ***‘polyalphabetic’***.

Video Link: <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/polyalphabetic-cipher>

1. One-time Pad

Tutor Note: The problem with ciphers is that they can be cryptanalysed. Any patterns in the keys that can be detected will be used to break the cipher. For example, using the same key (eg. Shift of 3 in Caesar Cipher) to encrypt an entire message leaks frequency information. Using a randomly generated key for each letter is one way to avoid leaking information. If there is no information leak, then the only option available to a cryptanalyst is the brute force attack – they have to try every single possibility, and this is time consuming.

Video Link: <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/one-time-pad>

1. Perfect Secrecy

Tutor Note: Perfect Secrecy is a desired property of every cipher.

Video Link: https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/perfect-secrecy

1. Pseudorandom Number Generator

Tutor Note: Perfect Secrecy requires randomness. If we cannot access true randomness, we can generate a close approximation – pseudorandomness. In security, ***perfect*** secrecy may not be feasible, but we can have ***practical*** security.

Video Link: https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/random-vs-pseudorandom-number-generators

***Practical Session***

**Please note that downloading and installing software on the laboratory computers is strictly forbidden and if found doing so, you will be penalized. Special permission was sought to conduct this tutorial session. Please install ONLY the tools specified in this tutorial.**

1. Navigate to cryptool.org
2. Download and Install CrypTool 1
3. Complete the following exercises:
   1. Help / Scenarios: Work through the examples for Classic Encryption Algorithms.

**REFERENCES**

1. Videos: Khan Academy Teaching Videos

Reference: <https://www.khanacademy.org/computing/computer-science/cryptography>

1. http://practicalcryptography.com/ciphers/caesar-cipher/