CSE 2203 (2018-2019)

### TUTORIAL 2 – CRYPTOGRAPHIC PRINCIPLES

**SUBSTITUTION AND TRANSPOSITION – CIPHERS & CRYPTANALYSIS**

Tutorial 1 is divided into two activities –1) a Series of Videos and 2) a Transposition Cipher Exercise activity (Permutation Cipher).

***Videos***

1. Substitution and Transposition

Tutor Note: The substitution and transposition techniques are used for converting a plaintext into ciphertext.

The substitution technique ***replaces*** the characters whereas the transposition technique ***rearranges*** the characters to form a ciphertext.

Ask the students, as they watch the video, to answer the question: what is the difference between ***substitution*** and ***transposition***?

Video Link: https://www.youtube.com/watch?v=Gl-xb03YdzM

1. Cryptanalysis of Substitution Ciphers: Frequency Analysis

Tutor Note: This video is linking the technique of ***Frequency Analysis*** to ***cryptanalysis*** of ***substitution ciphers***. Cryptanalysis is another term for ***‘breaking’*** a cipher.

Video Link: https://www.youtube.com/watch?v=1P8Xpxm76e8

1. Transposition Ciphers:

Tutor Note: Transposition Ciphers tries to find creative ways to permute the characters. They can be done without a key – simply using the number of rows and columns – or with a key – using a keyword to add complexity.

Video Links: <https://www.youtube.com/watch?v=Iwf4rZXVXjw>

<https://www.youtube.com/watch?v=sHsnH1u03e4>

***Activity Session***

1. Navigate to https://crypto.interactive-maths.com/permutation-cipher.html#ex

Read the Activity and Complete the Exercises.

**REFERENCES**

1. Transposition and Substitution in Ciphers

Reference: <https://www.youtube.com/watch?v=r7BRTOgPh4Q>

1. <http://www.cryptoprograms.com/home>
2. https://crypto.interactive-maths.com/downloadable-resources.html