2018 ACG Tutorial 1

**School of Digital Media and Infocomm Technology ST2504 Applied Cryptography**

1. What are the two basic techniques of transforming plain text into cipher text?

**Substitution and Transposition(permutation).**

1. Briefly define the Caesar Cipher.

**Caesar Cipher is replacing each letter of the alphabet with the letter standing three places further down the alphabet. First attested use in military affairs.**

1. The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. Try to decipher the following examples by using Caesar Cipher: -

* 1. KDFNHU - **hacker**
  2. HASORLWV - **exploits**
  3. VHFXULWB - **security**

1. Briefly define the Playfair Cipher.

**The Playfair Cipher is an approach where it encrypts multiple letters, this is to improve the security of the encryption.**

1. (a) Construct the Playfair cipher matrix using PRINCETON

**P R I N C**

**E T O A B**

**D F G H K**

**L M Q S U**

**V W X Y Z**

(b) With the matrix in part (a), show how the following plaintext will be encrypted (use X for the filler symbol if necessary):

* + 1. HELLOHELLOHELLOHELLO

**HE LX LO HE LX LO HE LX LO HE LX LO**

**DA QV QE DA QV QE DA QV QE DA QA QV**

* + 1. THE ART OF SECRET WRITING

**TH EA RT OF SE CR ET WR IT IN GX**

**AF TB TF TG LA PI TO RT RO NC QI**

1. Briefly define the Vigenère Cipher.

**Vigenère Cipher is the simplest polyalphabetic substitution cipher. It aligns the plaintext and key, repeat the key letters to match the plaintext length. Improving the security of having multiple ciphertext letters for each plaintext letter.**

* Simplest polyalphabetic substitution cipher
* Effectively multiple Caesar ciphers
* Key is multiple letters long K = k1 k2 … kd
* Ith letter specifies ith alphabet to use
* Repeat from start after d letters in message
* Use each alphabet in turn
* Decryption simply works in reverse

1. Try to encrypt the following examples by using Vigenère Cipher: -

Ciphertext Key

* 1. FOOTBALL CAPTAIN OF ENGLAND SINGAPORE

**SINGAPORESINGAPORESINGAP**

**Ciphertext: XWBZBPZCGSXGGICCWIFOYGNS**

* 1. HAPPY HOLIDAYS ORCHARD

**ORCHARDORCHAR**

**Ciphertext: VRRWYYRZZFHYJ**

1. What are the problems associated with one-time pad?

**Practical difficulties in generation and safe distribution of the key that can be used once only. This is due to the preconditions for the one-time pad which the key must be as long as the plain text, truly random and only be used once. These conditions cause problems for the one-time pad compromising in their credibility and reliability.**

* **It becomes insecure when the key is reused more than once.**
* **A computer-based pseudo-random number generator that acts as one-time pad may become insecure due to its deterministic properties.**
* **Safe distribution of key.**

ACG/ST2504 1-1 Apr 2018