

# MAS433 Cryptography

## Tutorial 1 Classical Ciphers

26.08.2011

### Instructions.

1. Submission of tutorial solution is compulsory.
2. Submission deadline: 25 Aug 2011, 6PM
3. Please submit your solution by sending email to wuhj@ntu.edu.sg (If your solution is handwritten, you can scan and convert it into digital format, such as .pdf document.)
4. Tutorial solution will not be provided after the tutorial class.

**Question 1.** Suppose that the key letter is “D”. Encrypt the following message using shift cipher: “Tanjung Pagar”.

**Question 2.** Use exhaustive key search to decrypt the following ciphertext, which is encrypted using a shift cipher (hint: the value of the encryption key is less than 7):

QFXYYWFNSTZYLJYXWTFQXJSITKK

**Question 3.** Suppose that the following substitution table is used.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Y	G	C	M	B	X	L	D	A	V	H	T	S	N	R	O	P	U	E	I	J	Q	W	K	Z	F

3.1 Encrypt the message: “smartphone”

3.2 Decrypt the ciphertext

AIEMAXXACJTIIREWAICD

**Question 4.** Attack substitution cipher

4.1 Describe how to attack the substitution cipher.

4.2 (Bonus Question) The ciphertext given in the file “ciphertext\_substitution.txt” is encrypted using a substitution cipher. Decrypt the first line of the ciphertext. (In this exercise, the size of the ciphertext is a bit large so that the attack can be relatively easy. To define a large array in C, you may define the array as a global variable.)

**Question 5.** Suppose that the key “many” is used in Vigenere cipher, decrypt the ciphertext: OICFQRGCJT.

**Question 6.** Attack Vigenere Cipher

6.1 Describe how to attack the Vigenere cipher.

6.2 The ciphertext given in the file “ciphertext\_vigenere.txt” is encrypted using a Vigenere cipher. Find the first sentence of the plaintext. Write down the details of your attack. (Hint: You can refer to the file “vigenere\_cipher\_example.c” that implements a Vigenere cipher. Note the use of ASCII table.)

**Question 7.** Suppose that the key “nanyang” is used in playfair cipher.

7.1 Encrypt the message: “follows a strongly scientific approach”

7.2 Decrypt the ciphertext: “PX AB CL NZ MI EZ HR KY AC WL RF QW FW”

**Question 8.** Suppose that  $\pi$  is the following permutation of  $\{1, 2, \dots, 8\}$  :

$x$	1	2	3	4	5	6	7	8
$\pi(x)$	2	4	6	1	8	3	5	7

8.1 Compute the permutation table  $\pi^{-1}$  (the inverse of  $\pi$ ).

8.2 Decrypt the following ciphertext, which is encrypted using a transposition (permutation) cipher with  $m = 8$ , and with the key  $\pi$  given above.

ETEGENLMDNTNEOORDAHATECOESAHLRMI

**Question 9.** Cipher Composition

9.1 Two substitution ciphers,  $S_1$  and  $S_2$ , are applied to encrypt a message as follows:  $c_i = S_2(S_1(p_i))$ . Discuss how to attack it.

9.2 Denote the encryption of a Vigenere cipher as  $C = V_K(P)$ . Two Vigenere ciphers are applied to encrypt a message as follows:  $C = V_{K_2}(V_{K_1}(P))$ . Discuss how to attack it. Comparing to the attack on  $V_{K_1}$  or  $V_{K_2}$ , does the attack complexity increase? (Hint: consider the Least Common Multiple of the lengths of  $K_1$  and  $K_2$ ) Discuss the security of using more than two Vigenere ciphers.

**Question 10.** If an attacker knows the ciphertext and part of the plaintext, how to attack the shift cipher, substitution cipher, Vigenere cipher and Playfair cipher, and how to break the composition of Vigenere ciphers in Question 9.2 efficiently?