The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security

GAME 4

28th March 2019

Solutions

Number of Questions: 5
Time allowed: 50min
Total marks: 5

In order to score marks you need to show all working/reasoning and not just the end result.

	Student Number	*Student Name*
Student 1		
Student 2		
Student 3		
Student 4		
Student 5		
Student 6		
Student 7		

Question 1	Question 2	Question 3	Question 4	Question 5	Total

1. Can the ciphertext ZQLMO be obtained by using a **transposition** cipher if the plaintext is a 5 letter English word? If so, provide a possible plaintext. If not, explain why there is no valid plaintext that could produce the ciphertext.

   Solution:
   (Not possible, no vowels)

2. Can the ciphertext ZQLMO be obtained by using a **substitution** cipher if the plaintext is a 5 letter English word? If so, provide a possible plaintext. If not, explain why there is no valid plaintext that could produce the ciphertext.

   Solution:
   (Any five letter word with all different letters – TRICK, TAKEN, NODES, GRAPH)

3. Ciphertext is C = DROXOHDAEOCDSYXECOCKZOBSYNYPPSFO. The frequency distribution of the ciphertext (given below) suggests this is a shift (Caesar) cipher. Find the matching plaintext.

```
                            *
                            *
                            *
    * *                     *       *           *
    * * *                   * *     *         * *
* * * * * *   *     *     * * *   * *         * * *
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
```

   Solution:
   (This is a shift cipher. To decrypt, shift each letter by 10, so that O becomes E Plaintext: the next question uses a period of five)

4. Ciphertext is C = QIVWSEEUOEOALNENKRSLASFEDAIMTIYITTE. The frequency distribution of the ciphertext (given below) suggests this is a transposition cipher. Find the matching plaintext.

```
        *
        *
        *       *
*       *       *                   * *
*       *       *     *   * *       * *
*     * * *     *   * * * * *   * * * * * * *   *
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
```

Solution:
Columnar Transposition, period d = 5

QUEST
IONFI
VEKEY
WORDI
SASAT
ELLIT
ENAME

(Plaintext: question five keyword is a satellite name)

5. A disadvantage of the general monoalphabetic cipher is that both sender and receiver must remember the permuted cipher alphabet. A common technique for avoiding this is to use a keyword from which the cipher alphabet can be generated. For example, using the keyword CIPHER, write out the keyword followed by unused letters in alphabetic order, and match this against the plaintext letters.

plain	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
cipher	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z

If it is felt that this process does not produce sufficient mixing, write the ciphertext alphabet on successive lines and then generate the sequence by reading down the columns:

C	I	P	H	E	R
A	B	D	F	G	J
K	L	M	N	O	Q
S	T	U	V	W	X
Y	Z				

This yields the sequence C A K S Y I B L T Z P D M U H F N V E G O W R J Q X

plain	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
cipher	C	A	K	S	Y	I	B	L	T	Z	P	D	M	U	H	F	N	V	E	G	O	W	R	J	Q	X

Such a system is used to encrypt

“It was disclosed yesterday that several informal but direct contacts have been made with political representatives of the Viet Cong in Moscow”

yielding the following ciphertext:

“UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZS
HZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJ
UDTMOHMQ”.

Determine the keyword that was used.

Solution: SPUTNIK

plain	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
cipher	S	A	H	V	P	B	J	W	U			X	T	D	M	Y		E	O	Z	I	F	Q		G	

S	P	U	T	?	I	?
A	B	?	D	E	F	G
H	J	?	M	O	Q	?
V	W	X	Y	Z		

S	P	U	T	N	I	K
A	B	C	D	E	F	G
H	J	L	M	O	Q	R
V	W	X	Y	Z		

plain	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
cipher	S	A	H	V	P	B	J	W	U	C	L	X	T	D	M	Y	N	E	O	Z	I	F	Q	K	G	R