The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security

GAME 4

29th 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

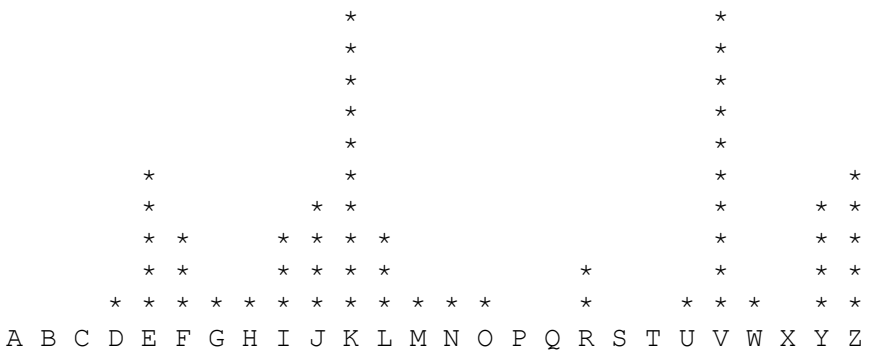
1. Can the ciphertext AILVD be obtained by using a **transposition** cipher if the plaintext is a 5 letter English word? If so, provide a possible plaintext. If not, explain why there is no valid plaintext that could produce the ciphertext.

Solution:
VALID

2. Can the ciphertext AILVD 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 = KYVGV IDLKR KZFEL JVUZE KYVEV OKHLV JKZFE JKRIK JNZKY WZMVF EVKYI VV
(note that blanks are there for readability only).
The frequency distribution of the ciphertext (given below) suggests this is a shift (Caesar) cipher. Find the matching plaintext.



Solution:
(This is a shift cipher. To decrypt, shift each letter by r, which is 17, so that A becomes R, etc.
Plaintext: the permutation used in the next question starts with five one three)

4. Ciphertext is C = EDUOE ALTYF ENINE ORTIA MKRQI VNAHW OSFSI. The frequency distribution of the ciphertext (given below) suggests this is a transposition cipher. Find the matching plaintext.

Solution:
Columnar Transposition, period d = 5 – columns are taken in the following order: 5,1,3,4,2

The keyword for question five is an animal.

T	H	E	K	E
Y	W	O	R	D
F	O	R	Q	U
E	S	T	I	O
N	F	I	V	E
I	S	A	N	A
N	I	M	A	L

(Plaintext: the keyword for question five is an animal)

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

“A woman is fighting a hefty parking fine because the road rules changed while her car was left on a Sydney street.”

yielding the following ciphertext:

“ETRIE JHSFH PWZHJ PEWCF ZMYEK QHJPF HJCBC OENSC ZWCKR EVKNX CSOWE JPCVT WHXCW CKOEK TESXC FZRJE SMVJC MSZKC CZ”

Determine the keyword that was used.

Solution: ECHIDNA

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

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

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