The University of Queensland
School of Information Technology and Electrical Engineering

Semester 2, 2017

COMS3000/7003 – Tutorial 9, Answers

Q1) Encrypt the following text with a Caesar cipher with a key 'E', i.e. with a shift of 4, which means the letter A in the plaintext will be mapped to the letter E in the ciphertext.

HELLOWORLD

Answer:
Use the following mapping:

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

```
Plaintext:  H E L L O W O R L D
Ciphertext: L I P P S A S V P H
```

Q2) Decrypt the following ciphertext, which was encrypted using a Vigenère cipher with the key ART. (Hint: Use the Vigenère table provided below.)

YFN GFM IKK IXA T

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

You need to perform the reverse operation of the encryption. For example, to decrypt the second letter (F), which was encrypted using the key R, you have to look up the letter F in the row R of the Vigenère table and see which letter it maps to in the top row.

YFN GFM IKK IXA T
ART ART ART ART A

YOU GOT ITR IGH T

Q3) The following ciphertext has been encrypted with a Vigenère cipher. Use the Kasiski test to determine the likely key length. (Some repeated trigrams have been highlighted).

(45 characters per line)

```
KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
CWHJVLNHIQIBTKHJVNPIST
```

The trigram HJV occurs 5 times, at positions 108, 126, 264, 318, and 330.
The distances between each pair of consecutive occurrences are 18, 138, 54, and 12. (You may want to do the same for other repeating trigrams.)The greatest common divisor of these numbers is 6, so that is very likely the keyword length.

The factors of these distances are:

12: 1, 2, 3, 4, **6**, 12
18: 1, 2, 3, **6**, 18
54: 1, 2, 3, 4, **6**, 9, 18, 27, 54
138: 1, 2, 3, **6**, 23, 46, 69, 138

The greatest common divisor of these numbers is 6, so that is very likely the keyword length.

Q4) Encrypt the following plaintext word using a simple transposition cipher with 3 columns (no permutation of column order).

Plaintext: TRANSPOSITION

```
TRA
NSP
OSI
TIO
N
```

Answer:
Ciphertext: TNOTNRSSIAPIO

Q5) Alice has the following secret message that she wants to send to Bob:

M1 = 10011101

Previously, Alice and Bob created a shared random Key K = 01011000, which they have not used yet.

a) Encrypt the message M1 with a one-time pad using key K.

XOR table:
1 xor 1 = 0
1 xor 0 = 1
0 xor 0 = 0
0 xor 1 = 1

Answer:
C1 = M1 xor K

```
M1 =  10011101
K  =  01011000
C1 =  11000101
```

b) Eve is eavesdropping on the channel and obtains the ciphertext C1. What can she do to find the secret message M1?

Answer:
The best she can do is directly guessing the message M1. Knowing the ciphertext C1 does not give her any information about the message, i.e. the one-time pad is perfectly secure, irrespective of the amount of computing resources and time an attacker has.

c) Now let's assume Alice wants to send another secret message M2 to Bob. The problem is that Alice and Bob have run out of secret keys to use, so Alice decides to reuse key K for the new message M2. The resulting ciphertext is C2 = M2 xor K.

```
M2 = 11100010
K  = 01011000
C2 = 10111010
```

Eve has been eavesdropping all the time and she has observed both C1 and C2. Through some other means (e.g. social engineering or guessing), she managed to obtain the message M1. With her knowledge of M1, C1 and C2, she can easily find M2. How?

You might use the following properties of xor:

A xor B = B xor A	(Commutativity)
A xor (B xor C) = (A xor B) xor C	(Associativity)

A xor A = 0
A xor 0 = A

Answer:
M1 = C1 xor K
K= M1 xor C1

```
M1 =  10011101
C1 =  11000101
```
K = 01011000

Now Eve has the secret key K which she can use to decrypt M2.
M2 = C2 xor K

```
C2 = 10111010
K  = 01011000
M2 = 11100010
```

Alternatively, Eve can use the following relationship:

M2 = M1 xor (C1 xor C2)
```
C1 =        11000101
C2 =        10111010
C1 xor C2 = 01111111

C1 xor C2 =         01111111
M1 =                10011101

M1 xor C1 xor C2  = 11100010 which is indeed = M2
```

This example illustrates the danger of reusing keys in a one-time pad.

Q6) Given is a Feistel Cipher with the following parameters:

8 bit blocks
Ki=1010
F(Ri-1,Ki) = 1111 = const

The output of F is always 1111, no matter what the input. This does not make sense for a real cipher, but it allows us to demonstrate some important characteristics of Feistel ciphers.

Plaintext block: 1001 1100

Calculate the ciphertext using two rounds.
Decrypt the ciphertext by applying two Feistel rounds to the ciphertext. You should get the original plaintext.

Remember, at the end of each encryption and decryption process, the left and the right half are swapped one more time.

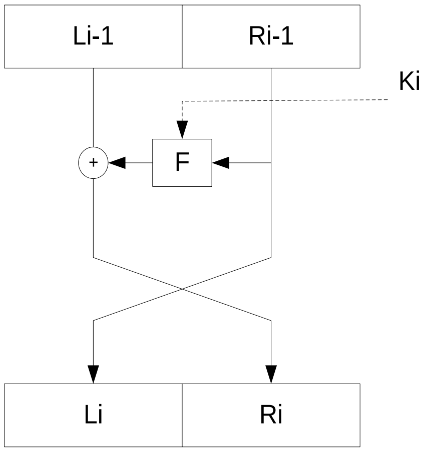
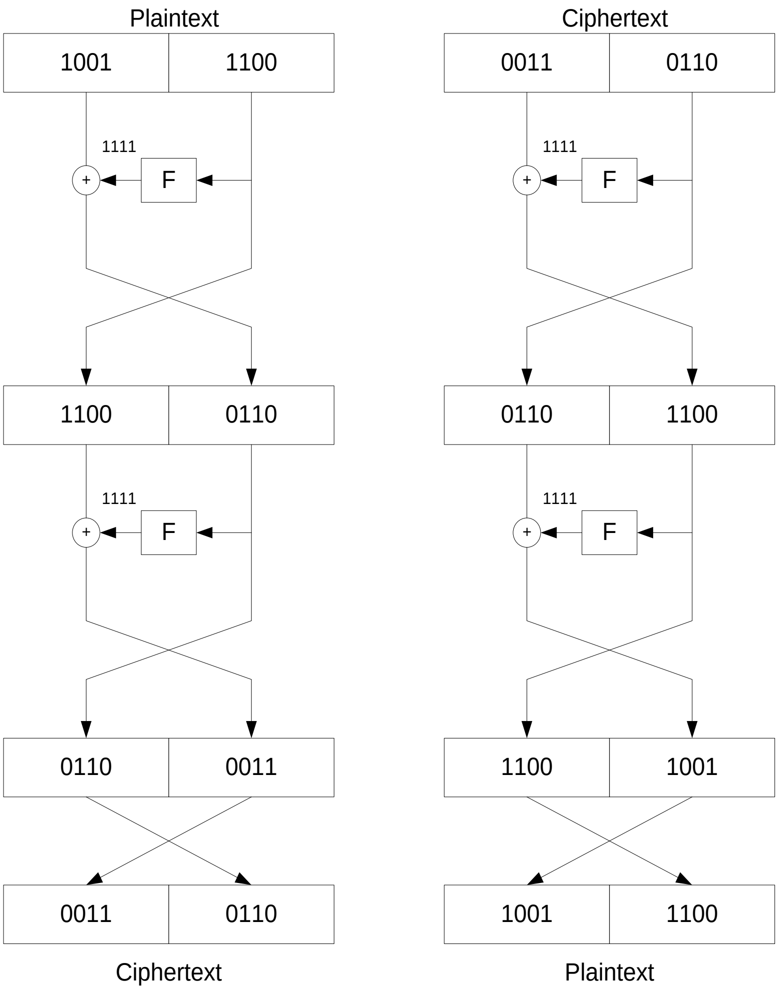


Figure 1 A Feistel Round

Answer:



The example shows that a Feistel cipher is reversible, even if F is not a reversible function. The security of a Feistel cipher relies on the properties of F. The constant function in our example is obviously not a very secure choice.