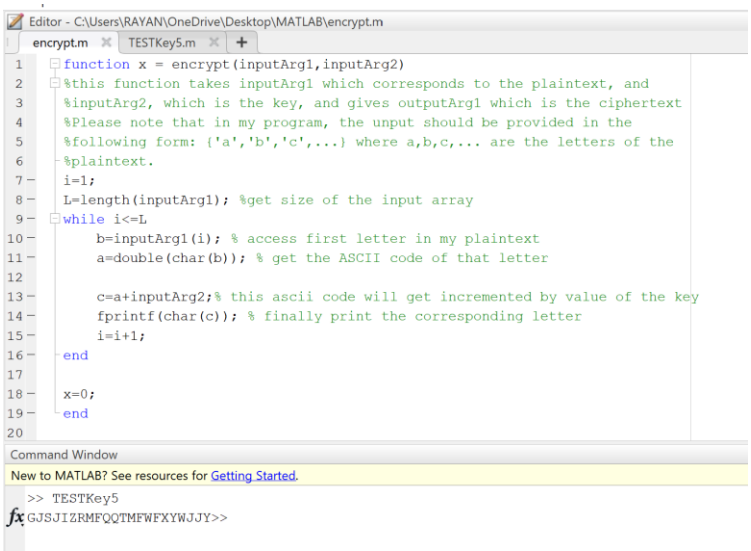
Rayan Hassan 4511021 – ECE 1155 – Homework 2

Question 1

a) Here is my function and my test results: (I also submitted the .m file but this is just in case)

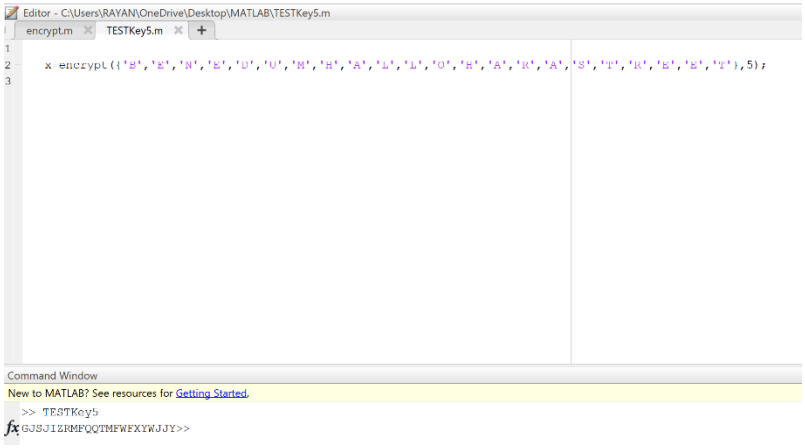


```
Editor - C:\Users\RAYAN\OneDrive\Desktop\MATLAB\encrypt.m
encrypt.m | TESTKey5.m
function x = encrypt(inputArg1,inputArg2)
%this function takes inputArg1 which corresponds to the plaintext, and
%inputArg2, which is the key, and gives outputArg1 which is the ciphertext
%Please note that in my program, the unput should be provided in the
%following form: {'a','b','c',...} where a,b,c,... are the letters of the
%plaintext.
i=1;
L=length(inputArg1); %get size of the input array
while i<=L
    b=inputArg1(i); % access first letter in my plaintext
    a=double(char(b)); % get the ASCII code of that letter

    c=a+inputArg2;% this ascii code will get incremented by value of the key
    fprintf(char(c)); % finally print the corresponding letter
    i=i+1;
end

x=0;
end

Command Window
New to MATLAB? See resources for Getting Started.
>> TESTKey5
GJSJIZRMFQQTMFWFXYWJJY>>
```



```
Editor - C:\Users\RAYAN\OneDrive\Desktop\MATLAB\TESTKey5.m
encrypt.m | TESTKey5.m
x = encrypt({'S','W','A','N','S','O','N','S','C','H','O','O','L','O','F','E','N','G','I','N','E','E','R','I','N','G'},5);

Command Window
New to MATLAB? See resources for Getting Started.
>> TESTKey5
GJSJIZRMFQQTMFWFXYWJJY>>
```

Ciphertext: GJSJIZRMFQQTMFWFXYWJJY

b) Key = 5

Plaintext: SWANSONSCHOOLOFENGINEERING

Question 2

Here is my code for this function (I also submitted the .m file separately)

```
Editor - C:\Users\RAYAN\OneDrive\Desktop\MATLAB\encryptmap.m
encryptmap.m | Untitled2.m
function [x] = encryptmap(inputArg1)
% Please note that inputArg1 (the plaintext) should be given in this format:
% ['a','b','c',...]
firstrow=['A', 'B', 'C', 'D', 'E', 'F','G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T',
i=0;
secondrow=[];
while i<=25
    x=randsample(33:126,1); % fill second row with 26 random letters and chatacters. I could have
                            % chosen randsample(0:255,1) to cover all ascii
                            % characters but I chose the ones that are more
                            % commonly used.
    y= char(x); % get the character/letter from the number randomly generated in x

    secondrow= [secondrow,y]; %fill the row with the randomly generated characters for each letter
    i=i+1;
end
disp('PlainLetters:')
disp(firstrow)  %this is the first row of the table (letters A --> Z)
disp('EncodeLetters:')
disp(secondrow)  % this is the second row of the table (corresponding randomly generated characters)
```

```
21
22 -  disp('Ciphertext:');
23 -  j=1;
24 -  L=length(inputArg1);
25 -  while j<=L
26 -      a=inputArg1(j); % get each letter in inputArg1 one at a time
27 -      b=strfind(firstrow,a); % find index of this letter in firstrow
28 -      a=secondrow(b); % substitute the letter by its corresponding character in table
29 -      fprintf(a);
30 -      j=j+1;
31 -  end
32 -  x=0;
33 -  end
34
35    % Please use the following function call to verify answer:
36    % x = encryptmap(['I','N','F','O','R','M','A','T','I','O','N']);
37
```

This is my mapping table + ciphertext:

```
Command Window
>> Untitled2
PlainLetters:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EncodeLetters:
m,\;{/zlHk^p`f^c;*bzJh2Jc:
Ciphertext:
Hf/^*`mzH^f>>
```

Plain Letter	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
Encode Letter	m	,	\	;	{	/	x	l	H	k	^	p	`	f	^	c	;	*	b	z	J	h	2	J	c	:

Plaintext: INFORMATION

Ciphertext: Hf/^*`mzH^f>>

Question 3

a) Monoalphabetic cipher is when we substitute a letter with another randomly. Polyalphabetic cipher is when multiple alphabets are used to encipher, so if two letters are the same in the ciphertext it doesn't mean that they decipher to the same letter in the plaintext.

b) The Enigma machine was much more secure because it randomly substituted a letter to another one and then change the encryption pattern every so that it doesn't repeat the same substitutions.

c) No because applying two monoalphabetic ciphers is really equivalent to just applying one. For example, if we map "b" to "a" and then "b" to "s", it's as if we simply mapped "b" to "s".

Question 4

a) If the passwords are 3 uppercase letters, then the hacker should try 26 x 26 x 26 combinations, which is equal to 17,576 combinations. If each one takes 5 seconds, the it would take him 17,576 x 5 = 87,880 seconds ≈ 24.4 hours.

b) 17,576 x 0.001 = 17.576 seconds.

Question 5

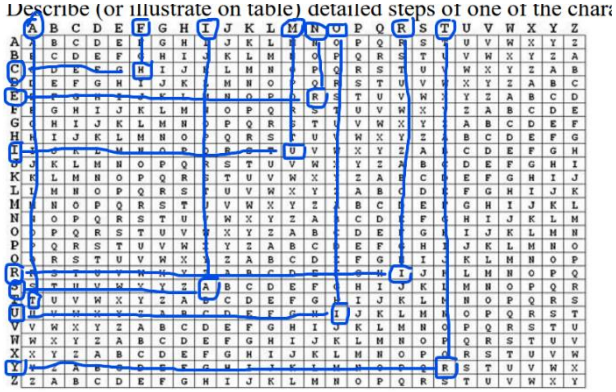
Plaintext: Information

Key = security

The key should be same length as plaintext, it repeats: so it's like securitysecuritysecurity…). So we need: Information → securitysec

We have to see the intersection of every letter in column (from plaintext) and its corresponding letter in the row (from key).

Ciphertext: ARHIIUTRASP



Please note that I didn't represent the intersections for the last 3 letters because it was going to look very mess, but it's the same concept.

Question 6

The main reasons as to why one-time pads are rarely used are that they require a lot of keys that need to be distributed securely (so a lot of management required too). Also, they need to have a perfect synchronization between the sending and receiving.

Question 7

a) This is a stream cipher since every bit in the plaintext will be XORed with its corresponding bit in the key.

b) If bits are different → result is 1, else its 0

111 001 101 010 100 100

XOR

110 011 010 110 111 101

---

001 010 111 100 011 001

So cipher text is: 001 010 111 100 011 001

c) A known plaintext attack is when only the plaintext and the cipher text are available for the attacker. This scheme is vulnerable because the attacker can easily know what the key is by inverting the process → XORing the plaintext with the cyphertext will give him the key. (inverse of XOR is XOR itself)

d) 110 101 000 011 100 110

XOR

110 011 010 110 111 101

---

000 110 010 101 011 011

Plaintext is: 000 110 010 101 011 011

Question 8

1) Confusion means that the relationship between ciphertext and plaintext is complex. Diffusion is that a slight change in the plaintext highly impacts the ciphertext.

2) Caesar Cipher where for example after each left shift of 3 letters, A would be replaced by D, B by C, and so on…

3) A simple column transposition where for example the word HOMEWORK is arranged as a matrix:

HOME

WORK

Therefore ciphertext is HW OO MR EK

A slight change in plaintext will highly change the ciphertext.

c) ex: plaintext: AVALANCHE

AVA

LAN

CHE

→ ALC VAH ANE → RLC VRH ANE (A+4 letters = R)

Question 9

a) If key size is 88bits, then we have 2^{88} possible combinations.

If the computer takes 1 second to try 2^{40} keys, it will take $(2^{88})/2^{40} = 2^{48}$ seconds to try all 2^{88} combinations.

If 1 year is 60(sec) x 60(minutes) x 24(hours) x 365(days) = 31536000 seconds, then 2^{48} seconds is equal to $2^{48}/31536000$ = 8925512.96 years

b) If key is 112 bits, we get 2^{112} combinations. So the computer will take $(2^{112})/2^{40} = 2^{72}$ seconds.

Which is equal to almost 1.497 x 10^14 years.

Question 10

a) DES and AES are block cipher since the message is fragmented into blocks of plaintext with 64 bits each.

b) In DES, the key is 56 bits (it's actually 64 but because of parity of bits, it's 56bits). The key is divided into 16 sub-keys of 48 bits for each round following this mapping: the 16^{th} key goes to round 1, the 15^{th} to round 2, and so on… There are 16 rounds in total. The Feistel structure refers to the structure of each round, which is the following:

The input is divided into left part and right part (32 bits each). The left part of the output is the right part of the input, and the right part of the output is the left part of the input XORed with the output of function F, where F is the right part of the input extended to 48 bits, XORed with the key, passing through S-box and finally permuted.

c) The keys must be used in the reversed order.

d) Main operations is AES are: Substitution, shifting rows, mixing columns and round key generation.