Introduction to Cryptography Teachers' Reference

Dear Teachers!

Here I have mentioned some guidelines for your good self so that your students can benefit form these modules. I am very hopeful that you will enjoy conducting the session.

After Module-1

1. Scytale Decryption
   In your class ask your students to devise a method to decrypt the message just been encrypted using Scytale. Encourage them to look around to find a decryption tool. Ask your students to cut a strip of paper some 4mm wide, 32cm long and light pencil lines drawn on it at 4mm distance. To give it the following shape.

   Now write cipher text on the paper strip in the following way.

s	t	b	a	e	i	e	h	r	y		t	e	e	i		w	e		

d	n	i		m	r	g	o	t	f	e	i	e	o	h	l		v		n

	a	a	e	t	c	a	g	t	r	o	o	w				d	m	h	

   Encourage them once again to find a tool around them to decrypt it. Ask them to look for a very familiar thing they must have been using right from their early school days to do their work. Now many of them must have figured out that you are asking for a pencil. Now ask them to use the pencil to decrypt the cipher text by using pencil and the only reasonable way would be to wrap the paper strip around the strip. The plain text will be visible along the six side faces of the pencil.

   Encourage them to reason that how did it work? There is a connection between six rows of the table in which the plain text was filled and the six faces of the pencil. Tell them that when the text was written in the table and rewritten on the strip column wise the consecutive letters in the plain text are separated by five other letters, and by wrapping it around a hexagonal pencil these separated letters come together once again.
   I have made the sample tape as Annex-I for your ease.

2. Caesar Cipher with Scytale
   Please encourage your students to use the Caesar Cipher and then further use Scytale to achieve a higher degree of encryption.

3. Caesar Cipher is a Shift Cipher
   Tell them Caesar Cipher is a shift/substitution cipher as it is obtained by shifting all the characters thrice in a cyclic way.

4. Beyond the box thinking
   While interactively working with them let them propose some other ciphers like
   a. Some other shift cipher by some arbitrary number of times.
   b. Some other shift cipher while including text and numeric characters.
   c. Encourage them to come up with some arbitrary permutations and tell them that such permutations would be the factorial of number of characters involved. Tell them that shift cipher is a special case of permutation cipher.

After Module -2

1. Decryption Startup
   Encourage the students to decrypt the given cipher text, for this purpose write the cipher text with double line spacing as shown below

   “gsv hgifxgfiv zmw lkvizgrlm lu gsv vbv rh evib hrnrozi gl zm vovxgilmrx

   xznviz,zmw rg rh mzgfizo gl wrhxfhh gsvn gltvgsvi. ylgs ziv yzhvw lm gdl nzqli

   xlnklmvmgh: z ovmh zhhvnyob, zmw zm rnztrmt hvmhli. gsv ovmh zhhvnyob

   xzkgfivh z kligrlm lu gsv ortsg vnzmzgrmt uiln zm lyqvxg, zmw ulxfh rg lmgl

   gsv rnztrmt hvmhli. gsv rnztrmt hvmhli gsvm gizmhulinh gsv kzggvim lu ortsg

   rmgl z rwvl hrtmzo, vrgsvi vovxgilmrx li mvfizo.”

   The above cipher text has been made available in Annex-III

2. Further guidance
   Guide them in the following ways.
   a. Tell them that the most frequently occurring letter is ‘e’. So let them guess the inverse transformation v → e. Also guide them that the most frequently occurring three letter word is “the”. Thus the inverse transformation g → t and s → h.
   b. The other frequently occurring three letter word starting with ‘a’ is “and”, hence the inverse transformation m → n and w → d. Tell them to fill the table at the given work sheet.

3. Start writing the plain text
   Tell them to start writing the decrypted letters below the ciphered letters to get a shape as shown below.

```
gsv hgifxgfiv zmw lkvizgrlm lu gsv vbv rh vcgivnvob hrnrozi gl zm vovxgilmrx
the  t   t  e and     at  n    the e e    e t e e       a   t  an e e t  n
xznviz, zmw rg rh mzgfizo gl wrhxfhh gsvn gltvgsvi. ylgs ziv yzhvw lm gdl nzqli
 a e a, and  t    nat  a  t  d       the  t  ethe .   t  a e  a ed  n t    a
xlnklmvmgh: z ovmh zhhvnyob, zmw zm rnztrmt hvmhli. gsv ovmh zhhvnyob
     nent   a  ens a  e      and an   a  n   en   . the  en  a  e
xzkgfivh z kligrlm lu gsv ortsg vnzmzgrmt uiln zm lyqvxg, zmw ulxfh rg lmgl
 a t  e  a    t  n    the     t e anat n       an    e t, and        t  nt
gsv rnztrmt hvmhli. gsv rnztrmt hvmhli gsvm gizmhulinh gsv kzggvim lu ortsg
```

the a n en . the a n en then t an the atte n ht
rmgl z rwvl hrtmzo, vrgsvi vovxgilmrx li mvfizo.
t a de na , e the e e t n ne a .

4. Beyond the box thinking
   Encourage them to find the missing letters by using their blanks filling skills like "e_e" is "eye". Tell them that the least occurring letters are 'x' and 'z' so c → x for a meaningful world "extremely" and this will suggest some other inverse permutations. Sh! To tell you the truth, all I have done in this cipher is "a ←→ z", "b ←→ y", "c ←→ x" and so on. Thus the following would be the plain text.

   gsv hgifxgfiv zmw lkvizgrlm lu gsv vbv rh vcgivnvob hrnrozi gl zm vovxgilmrx
   The structure and operation of the eye is extremely similar to an electronic

   xznviz, zmw rg rh mzgfizo gl wrhxfhh gsvn gltvgsvi. ylgs ziv yzhvw lm gdl nzqli
   camera, and it is natural to discuss them together. Both are based on two major

   xlnklmvmgh: z ovmh zhhvnyob, zmw zm rnztrmt hvmhli. gsv ovmh zhhvnyob
   components: a lens assembly, and an imaging sensor. The lens assembly

   xzkgfivh z kligrlm lu gsv ortsg vnzmzgrmt uiln zm lyqvxg, zmw ulxfh rg lmgl
   captures a portion of the light emanating from an object, and focus it onto

   gsv rnztrmt hvmhli. gsv rnztrmt hvmhli gsvm gizmhulinh gsv kzggvim lu ortsg
   the imaging sensor. The imaging sensor then transforms the pattern of light

   rmgl z rwvl hrtmzo, vrgsvi vovxgilmrx li mvfizo.
   into a video signal, either electronic or neural.

After Module-3

1. Practice to write in 1's and 0's
   Ask your students to turn the text mentioned at the end of the last module into 1's and 0's. You may help them with the part of the EASCII table I have given as Annex-III along with this document. Following will be the conversion.

Plain Text								S								e								e							
EASCII (P)								0	1	0	1	0	0	1	1	0	1	1	0	0	1	0	1	0	1	1	0	0	1	0	1
								y								o								u							
0	0	1	0	0	0	0	0	0	1	0	1	1	0	0	1	0	1	1	0	1	1	1	1	0	1	1	1	0	1	0	1
								a								t															
0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	1	0	1	1	1	0	1	0	0	0	0	1	0	0	0	0	0
2																o								'							
0	0	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	1	1	0	1	1	1	1	0	0	1	0	0	1	1	1
								c								l								o							
0	0	1	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	1

c								k								.															
0	1	1	0	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	1	0								

To reduce the bits you may encourage them to find out a bit which carry's no information, after a while further hint them to figure out a bit which remains constant. Hopefully bye this time many of your students must have determine that it's the most significant bit of each character. So we can drop it without any loss of information.

After Module-4

1. Decrypting the cipher text
   Please share the following table with your students.

P	0	0	1	1
K	0	1	0	1
$P\oplus K = C$ (Sender did it)	0	1	1	0

Give them a copy of Annex-IVcontaining the cipher text. Ask them to devise a simple way to get 'P' row from 'C', facilitate them think on the line to $\oplus$ C with some thing to get 'P' back. Some of them should have guessed that $C\oplus K$ gives us 'P'. Praise them and show them the following table…

P	0	0	1	1
K	0	1	0	1
$P\oplus K = C$ (Sender did it)	0	1	1	0
K	0	1	0	1
$C\oplus K = P$ (Recipient's operation)	0	0	1	1

2. Now ask them to use XOR in Annex-IV, to get the cipher text back.

After Module-5

1. Debate to for key exchange
   Facilitate a debate that whether it's possible to share a key in public, so that eavesdropper can't get it. Hopefully, they won't be able to figure out a method to do so☺. Now with a question in their mind lead them to the next module.

After Module-6

1. Take up the first problem $2^x = 27 \bmod (29)$
   Encourage them to do some guess work, which will not work hopefully. Lead them to the systematic way to find it out and it is to tabulate all the powers of 2 in mod (29) and then by table lookup we will be able to get x = 15. Tell them that to get x is time consuming when compared with raising the power of '7' in mod (29). Tell them that the bigger that value of prime the more would the process be time consuming.

2. Take up the second problem $7^y = 16 \bmod (29)$
   Now similarly take up the second problem, make a similar **complete** table to get y = 5, 12, 19, 26. Let the students feel the difference between the two tables. The

first table has all the numbers from 1 to 28 while the second table contains only 1/4th of them.

A worksheet has been provided as Annex-V to solve these two problems.

After Module-7

1. Play Alice and Bob
   Encourage your students to practice some key exchange by using p = 89 and g = 30 with a and b = 10, 20, 18, 19 etc. etc. You may stage a play with the help of two students acting as Alice and Bob and rest of the class as Eve. But be sure that the selection of "a", "b" and the relevant calculation is privately done by them. I am also sending you a small computer program to you by which you can take the power of a number in mod (p), please see Annex-VI. In my presentation I have taken a = 1551 and b = 1231

2. About the Module Challenge
   Now $A = g^a \bmod (p)$ and $B = g^b \bmod (p)$
   And $A^b \bmod (p) = (g^a)^b \bmod (p)$ which is the same as $B^a \bmod (p) = (g^b)^a \bmod (p)$
   Guide them to figure it out.

Thank you very much for all your efforts to conduct this presentation. I am very hopeful that your students have enjoyed it. I would be looking forward to your suggestions and feedback, thank you very much once again.

Aurangzeb
aurangzeb@nu.edu.pk

Annex-I

Use these strips to play Scytale

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

□□

Encrypted text to work with at the end of Module-II
Hint!

- It is a permutation cipher
- ‘a’ has been permuted to ‘z’, so you need to map z → a to get the plain text back

gsv hgifxgfiv zmw lkvizgrlm lu gsv vbv rh

evib hrnrozi gl zm vovxgilmrx xznviz,zmw rg

rh mzgfizo gl wrhxfhh gsvn gltvgsvi. ylgs

ziv yzhvw lm gdl nzqli xlnklmvmgh: z ovmh

zhhvnyob, zmw zm rnztrmt hvmhli. gsv ovmh

zhhvnyob xzkgfivh z kligrlm lu gsv ortsg

vnzmzgrmt uiln zm lyqvxg, zmw ulxfh rg

lmgl gsv rnztrmt hvmhli. gsv rnztrmt hvmhli

gsvm gizmhulinh gsv kzggvim lu ortsg rmgl z

rwvl hrtmzo, vrgsvi vovxgilmrx li mvfizo.

In Cipher	to	In Plain
a	to	
b	to	
c	to	
d	to	
e	to	
f	to	
g	to	
h	to	
i	to	
j	to	
k	to	
l	to	
m	to	

In Cipher	to	In Plain
n	to	
o	to	
p	to	
q	to	
r	to	
s	to	
t	to	
u	to	
v	to	
w	to	
x	to	
y	to	
z	to	a

Annex-III

Part of the EASCII table

Binary	Value
00100000	SP (Space)
00100001	!
00100010	"
00100011	#
00100100	$
00100101	%
00100110	&
00100111	'
00101000	(
00101001	)
00101010	*
00101011	+
00101100	,
00101101	-
00101110	.
00101111	/
00110000	0
00110001	1
00110010	2
00110011	3
00110100	4
00110101	5
00110110	6
00110111	7
00111000	8
00111001	9
00111010	:
00111011	;
00111100	<
00111101	=
00111110	>
00111111	?
01000000	@
01000001	A
01000010	B
01000011	C
01000100	D
01000101	E
01000110	F
01000111	G
01001000	H
01001001	I
01001010	J
01001011	K
01001100	L
01001101	M
01001110	N
01001111	O

Binary	Value
01010000	P
01010001	Q
01010010	R
01010011	S
01010100	T
01010101	U
01010110	V
01010111	W
01011000	X
01011001	Y
01011010	Z
01011011	[
01011100	\
01011101	]
01011110	^
01011111	_
01100000	`
01100001	a
01100010	b
01100011	c
01100100	d
01100101	e
01100110	f
01100111	g
01101000	h
01101001	i
01101010	j
01101011	k
01101100	l
01101101	m
01101110	n
01101111	o
01110000	p
01110001	q
01110010	r
01110011	s
01110100	t
01110101	u
01110110	v
01110111	w
01111000	x
01111001	y
01111010	z
01111011	{
01111100	|
01111101	}
01111110	~
01111111	DEL (delete)

Annex-IV

Work Sheet for Module-4

C(Cipher)	F								{								y							
C (Cipher in bin.)	0	1	0	0	0	1	1	0	0	1	1	1	1	0	1	1	0	1	1	1	1	0	0	1
? (What?)																								
P																								
P																								

5								g								s								`							
0	0	1	1	0	1	0	1	0	1	1	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1	1	0	0	0	0	0

>								}								a								>							
0	0	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	0	0	0	0	1	0	0	1	1	1	1	1	0

.								5								q								;							
0	0	1	0	1	1	1	0	0	0	1	1	0	1	0	1	0	1	1	1	0	0	0	1	0	0	1	1	1	0	1	1

5								}								q								z							
0	0	1	1	0	1	0	1	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	1	1	1	1	0	1	0

}								w								;															
0	1	1	1	1	1	0	1	0	1	1	1	0	1	1	1	0	0	1	1	1	0	1	1								

Key

0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0

Annex-V

Work Sheet for Module-6 (we are working in **mod (29)**)

2^x	**Working**	**Result**
2^1		2
2^2		4
2^3		8
2^4		16
2^5	32=3	3
2^6	$(2^5)2 = 3x2$	6
2^7		
2^8		
2^9		
2^{10}		
2^{11}		
2^{12}		
2^{13}		
2^{14}		
2^{15}		
2^{16}		
2^{17}		
2^{18}		
2^{19}		
2^{20}	$(2^5)^4= (3)^4 = (9)^2 = 81$	23
2^{21}		
2^{22}		
2^{23}		
2^{24}	$(2^4)(2^{20}) = 16x23 =$ 8x2x23=8x17=4x2x17=4x5	20
2^{25}		
2^{26}		
2^{27}		
2^{28}		

2^x	**Working**	**Result**
7^1		
7^2		
7^3		
7^4		
7^5		
7^6		
7^7		
7^8		
7^9		
7^{10}		
7^{11}		
7^{12}		
7^{13}		
7^{14}		
7^{15}		
7^{16}		
7^{17}		
7^{18}		
7^{19}		
7^{20}		
7^{21}		
7^{22}		
7^{23}		
7^{24}		
7^{25}		
7^{26}		
7^{27}		
7^{28}		

Annex-VI

//C++ code to get the power of a number mod (p)

```
#include <iostream>
#include <conio.h>
#define N 100
using namespace std;

void main()
{
      long int p;
      long int g;
      long int a;
      long int b;

cout << "Enter the value of prime:";
cin >> p;

cout <<endl;
cout <<"Enter the number whose power you want to raise:";
cin >> g;

cout <<endl<<"Enter the power you want to raise:";
cin >> a;
cout <<endl;

      b=g;
      for(int i = 1; i < a; i++)
          b=(b*g)%p; //Comments:Current value of b is divided by p and
                     //the remainder is assigned to it
      cout << g << " Raised to the power " << a <<" is " << b<< endl;
}
```