TUTORIAL 4

CRYPTOGRAPHY

Purpose

Understand the importance of checksum value to check file integrity
Understand principles of encryption (XOR operations, binary conversion)
Able to send encrypted message & decrypt the encrypted message

Class Activities

1. Encryption and Decryption using XOR

Students lookups part 2. to see the binary and hexadecimal code corresponding to each ACSII character and study it.

Discussion 1: Students are expected to answer the following questions after reading (20 mins)

- Convert plaintext ‘Hello world’ into binary and hexadecimal.

- How many bits are there?

- Using key “itsimplekey” and XOR operator to create a cipher.

Hints: Convert both plaintext and key into binary to make XOR operation.

- Covert the result to Hexadecimal.

- Check it out at: http://www.rapidtables.com/convert/number/ascii-to-binary.htm and http://xor.pw/

2. ACSII to hexadecimal and binary

ASCII Character	Binary	Hexadecimal
NUL	00000000	00
SOH	00000001	01
STX	00000010	02
ETX	00000011	03
EOT	00000100	04
ENQ	00000101	05
ACK	00000110	06
BEL	00000111	07
BS	00001000	08
HT	00001001	09

ASCII Character	Binary	Hexadecimal
LF	00001010	0A
VT	00001011	0B
FF	00001100	0C
CR	00001101	0D
SO	00001110	0E
SI	00001111	0F
DLE	00010000	10
DC1	00010001	11
DC2	00010010	12
DC3	00010011	13
DC4	00010100	14
NAK	00010101	15
SYN	00010110	16
ETB	00010111	17
CAN	00011000	18
EM	00011001	19
SUB	00011010	1A
ESC	00011011	1B
FS	00011100	1C
GS	00011101	1D
RS	00011110	1E
US	00011111	1F
Space	00100000	20
!	00100001	21
"	00100010	22
#	00100011	23
$	00100100	24
%	00100101	25
&	00100110	26
'	00100111	27
(	00101000	28
)	00101001	29

ASCII Character	Binary	Hexadecimal
*	00101010	2A
+	00101011	2B
,	00101100	2C
-	00101101	2D
.	00101110	2E
/	00101111	2F
0	00110000	30
1	00110001	31
2	00110010	32
3	00110011	33
4	00110100	34
5	00110101	35
6	00110110	36
7	00110111	37
8	00111000	38
9	00111001	39
:	00111010	3A
;	00111011	3B
<	00111100	3C
=	00111101	3D
>	00111110	3E
?	00111111	3F
@	01000000	40
A	01000001	41
B	01000010	42
C	01000011	43
D	01000100	44
E	01000101	45
F	01000110	46
G	01000111	47
H	01001000	48
I	01001001	49

ASCII Character	Binary	Hexadecimal
J	01001010	4A
K	01001011	4B
L	01001100	4C
M	01001101	4D
N	01001110	4E
O	01001111	4F
P	01010000	50
Q	01010001	51
R	01010010	52
S	01010011	53
T	01010100	54
U	01010101	55
V	01010110	56
W	01010111	57
X	01011000	58
Y	01011001	59
Z	01011010	5A
[	01011011	5B
\	01011100	5C
]	01011101	5D
^	01011110	5E
_	01011111	5F
`	01100000	60
a	01100001	61
b	01100010	62
c	01100011	63
d	01100100	64
e	01100101	65
f	01100110	66
g	01100111	67
h	01101000	68
i	01101001	69

ASCII Character	Binary	Hexadecimal
j	01101010	6A
k	01101011	6B
l	01101100	6C
m	01101101	6D
n	01101110	6E
o	01101111	6F
p	01110000	70
q	01110001	71
r	01110010	72
s	01110011	73
t	01110100	74
u	01110101	75
v	01110110	76
w	01110111	77
x	01111000	78
y	01111001	79
z	01111010	7A
{	01111011	7B
|	01111100	7C
}	01111101	7D
~	01111110	7E
DEL	01111111	7F