

20/05/2021  
M Shahid Siddiqi

# 1. One Time Pad

(a) Assuming nibble (4 bits) as space for each letter

hello: 0x 6 8 6 5 6c 6c 6f

XOR (0b) 0110 1000 0110 0101 0110 1100 01101100

key key: 0110 1111

(0x) 6b 65 79 6b 65 79

0110 1011 0110 0101 0110 1001 0110 1011 0110 0101

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

(1) 0000 0000 0110 1000 0110 0101 0110 1100 0110 1100 2

0110 1111

(2) 0110 1011 0110 0101 0110 1001 0110 1011 0110 0101

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

0110 1001 0110 1001 0110 1001 0110 1001 0110 1001

Observed that ' ' in ascii has binary (0110 000)

i.e 0x30 so padding with 0 in code

will break (or add the logical error

(c) - Name: Shahid Siddiqui

hex:(ox) 5 3 6 8 6 1 6 8

Name	hex(ox)	6	9	binary	Key	hex	binary	SRK
0 S	5 3			0101 0011	t	74	0111 0100	0010 0111
1 h	6 8			0110 0100	h	68	0110 1000	0000 0000
2 a	6 1			0110 0001	e	65	0110 0101	0000 0100
3 h	6 8			0110 0100	o	6f	0110 1111	0000 0111
4 i	6 9			0110 0101	n	6e	0110 1110	0100 0111
5 d	6 4			0110 0100	e	65	0110 0101	0000 0001
6	2 0			0010 0000	t	74	0111 0100	0101 0100
7 S	5 3			0101 0011	i	69	0110 1001	0011 1010
8 i	6 9			0110 1001	m	6d	0110 1101	0000 0100
9 d	6 4			0110 0100	e	65	0110 0101	0000 0001
10 d	6 4			0110 0100	p	70	0111 0000	0001 0100
11 i	6 9			0110 1001	q	61	0110 0001	0000 1000
12 v	7 1			0111 0001	d	64	0110 0100	0001 0101
13 u	7 5			0111 0101	i	69	0110 1001	0001 1100
14 i	6 9			0110 1001	s	73	0111 0011	0001 1010

in hex string: 0x 27 00 04 07 07 01 5 4

3a 04 01 14 08 15 1c 1a