IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 12, December 2015.
www.ijiset.com
ISSN 2348 – 7968

Applications Of Encryptionand Decryption Scheme By Using Binary, Hexa And Octa Systems

G.Venkatasubbaiah,
Lecturer in Mathematics,
Government College for Men ,Kadapa
Email:venkat_g2010@yahoo.com

Prof. K. Rama Krishna Prasad
Department of Mathematics,
S.V. University, Tirupati.

Dr. V. Vasu
Department of Mathematics,
S.V. University, Tirupati.
Email:vasuvaralakshmi@gmail.com

Abstract:

The traditional topic of cryptography is encryption. Encryption scheme is used to keep messages or stored data secret. In this paper, we introduce three fundamental basic numbers convertion systems namely binary, octa and hexa decimal convertions that we need to describe encryption schemes in different ciphers and their cryptanalysis.

Key words:

Encryption, Decryption, Hexa, Octal, Hexa decimal numbers systems, convertions, cipher text, binary text, binary.

Introduction:

An encryption scheme or cryptosystem is a tuple (P, C, K, E, D) with the following properties.

1. P is a set. It is called the plaintext space. Its elements are called plain texts.
2. C is a set. It is called the ciphertext space. Its elements are called cipher texts.
3. K is a set. It is called the key space. Its elements are called keys.
4. E= $\{E_k : k \varepsilon K\}$ is a family of functions E_k: P→C. its elements are called encryption functions.
5. D= $\{D_k : k \varepsilon K\}$ is a family of functions D_k : P→C. Its elements are called decryption functions.

ISSN 2348 – 7968

6. For each e ε K there is d ε K such that $D_d(E_e(p))=p$ for all p ε P.

- Alice can use an encryption scheme to send a confidential message m to BOB. She uses an encryption key e. Bob uses the corresponding decryption key d. Alice compute the ciphertext $c=E_e(m)$ and sends it to bob. Bob can obtain the plain text as $m=D_d(e)$. clearly the decryption key must be secret.

As first example of an encryption scheme, we describe the Caesar cipher. The plaintext space, cipher text space and key space are [(A,B…Z). we identify the letters A, B…Z according to table with numbers 0,1,…25 respectively. This enables us to compute with letters.

For $e\in Z_{26}$ the encryption functions E_e is $E_e:\Sigma\rightarrow \Sigma$, $\psi\rightarrow(\psi+e)$ mod 26. Analogously, for $d\in Z_{26}$ the decryption function D_d is

$D_d:\Sigma\rightarrow \Sigma$, $\psi\rightarrow(\psi-d)$ mod 26

The decryption key for the encryption key e is d=e. this is however not true for every cryptosystem.

The Caesar cipher can easily be modified such that the plaintext space and sequences $W=(W_1, W_2\ldots W_n)$ with $Wi\in\Sigma$, $1\leq i\leq n$. again the key space is Z_{26}. The encryption function E_e replaces each letters W_i by W_i+e mod 26, $1\leq i\leq n$.This also is called the Caesar cipher.

Definition of binary:

Binary is the natural way most digital circuits represent and multipulate numbers. (common misspellings are “binary”, “Bienary” (or) “binery”) binary

ISSN 2348 – 7968

numbers are something represented by preceeding the values with “ob” as in ob101. Binary is sometimes abbreviated as BIN.

Binary counting :

0,1,10,11,100,101,110, 111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111, 10000, 10001, and so on.

Definition of Octal:

Octal (Base 8) was previously a popular choice for representing digital circuits numbers in a form that is more compact than binary. Octal is sometimes abbreviated as OCT.

Octal counting goes as 0,1,2,3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17, 20, 21 and so on.

Definition of Hexa Decimal :

Hexa decimal (base 16) is currently the most popular choice for representing digital circuits numbers in a form that is more compact than binary (common misspellings are “Hexadecimal”, or Hex decimal)

Hexa decimal numbers are sometimes represented by preceding the value with “OX” as in OX1 B84. Hexadecimal is sometimes abbreviated as Hex:

Hexa decimal counting goes as 0,1,2,3,4,5,6,7,8, 9, A, B, C, D, E, F, 10 and 11.

All four number systems are equally capable of representing any numbers. Further more, a number can be perfectly converted between the various number systems without any loss of numeric values.

At first binary, it seems like using any number systems. Other than binary number system is complicated and unnecessary. However, since the job of electrical and software engineers is to work with digital circuits, engineer’s require number

ISSN 2348 – 7968

system that can best transfer information between the human world and the digital circuits world.

If turns out that the way in which a number is represented can make it easier for the engineer to perceive the meanings of the numbers as it applies to a digital circuits.

In other words, the appropriate number system can actually make things less complicated.

Correspondence between letters and binary sysertem numberss.

A	B	C	D	E	F	G	H	I	J	K	L
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011
M	N	O	P	Q	R	S	T	U	V	W	X
01100	01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111
Y	Z										
11000	11010										

2. Corresponding between letters and octa decimal system

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	10	11	12	13
M	N	O	P	Q	R	S	T	U	V	W	X
14	15	16	17	20	21	22	23	24	25	26	27
Y	Z										
30	31										

3. Corresponding between letters and Hexa decimal system

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	A	B

ISSN 2348 – 7968

M	N	O	P	Q	R	S	T	U	V	W	X
C	D	E	F	10	11	12	13	14	15	16	17
Y	Z										
18	19										

Problem 1

Suppose Subash wants to encrypt the plaintext message "CRYPTANALYSIS " using one time pad. He first convert the letters into Binary bit string.

C	R	Y	P	T
00010	10001	11000	01111	10011
A	N	A	L	Y
00000	01101	00000	01011	11000
S	I	S		
10010	01000	10100		

The one – time pad requires a Key Consisting of a Randomly selected string of Bits that is the same length as the message suppose we use key e=

11000	10100	11001	01100	11001
00001				
00011	00001	10100	00111	01101
01101				

The encryption function E_e is $E_e : \Sigma \rightarrow \Sigma$ defined by $\Psi_i \rightarrow (\Psi_i + e_i) \pmod{26}$

Plain Text	Key	Cipher Text
C = 00010	11000	00001 = B
R = 10001	10100	01011 = L
Y = 11000	11001	10111 = X
P = 0111	01100	00001 = B

ISSN 2348 – 7968

T = 10011	11001	10010 = S
A = 00000	00001	00001 = B
N = 01101	00011	10000 = Q
A = 00000	00001	00001 = B
L = 01011	10100	00101 = F
Y = 11000	00111	00101 = F
S = 10010	01101	00101 = F
I = 01000	10111	00101 = F
S = 10010	01101	00101 = F

Converting the ciphertext bits back into letter the cipher text message to be transmitted is “BLXB SBQBFFFFF “

When he wants decrypts it using same key

Cipher Text	Key	PlainText
00001 = B	11000	C = 00010
01011 = L	10100	R = 10001
10111 = x	11001	Y = 11000
00001 = B	01100	P = 0111
10010 = S	11001	T = 10011
00001 = B	00001	A = 00000
10000 = 16	00011	N = 01101
00001 = B	00001	A = 00000
00101 = F	10100	L = 01011
00101 = F	00111	Y = 11000
00101 = F	01101	S = 10010
00101 = F	10111	I = 01000
00101 = F	01101	S = 10010

ISSN 2348 – 7968

Decryption function D_d is $D_d : \Sigma \rightarrow \Sigma$ defined by $\Psi \rightarrow (\Psi - d) \pmod{26}$

d = e (key)

and there by recovers the original message.

Problem - 2

Suppose a person wants the plain text message" PROBABILITY" to encrypt using one time pad.He first consults OCTA DECIMAL SYSTEM table to convert the letters to the octa system.

P	R	O	B	A	B	I	L	I	T	Y
17	27	16	1	0	1	11	13	10	23	31

the encryptin function E is $E : f \rightarrow f$ by $\Psi_i \rightarrow (\Psi_i + e_i) \pmod{26}$

Plain Text	Key	Cipher Text
17 = P	011	20 = Q
27 = R	010	3 = D
16 = O	000	16 = O
1 = B	011	4 = E
0 = A	101	4 = E
1 = B	110	7 = H
11 = I	100	12 = K
13 = L	011	16=O
10 = I	11	17=P
23 = T	111	4=E
31 = Y	001	6=G

Convertign the ciphertext OCTA bits back to letters the cipher text is "QDOEEHKOPEG"

When we wants decrypts it using same key.

ISSN 2348 – 7968

Cipher Text	Key	Plain Text
20 = Q	011	17 = P
3 = D	010	27 = R
16 = O	000	16 = O
4 = E	011	1 = B
4 = E	101	0 = A
7 = H	110	1 = B
12 = K	100	11 = I
16=O	011	13 = L
17=P	11	10 = I
4=E	111	23 = T
6=G	001	31 = Y

decryption function D_d is $D_d : f \to f$ defined by $\Psi \to (\Psi - d) \pmod{26}$

and there by recovered the orginal message "PROBABILITY" where d = e

Problem – 3

Suppose a person wants the plain text message "TELEVISI" to encrypt using one – time pad .we first convert the letters to the Hexa bit string.

Plain Text	Key	Cipher Text
T = 13	001	U
E = 4	010	V
1 = 8	010	Q
E = 4	100	I
V = 5	110	R
I = 8	100	S
S = 12	001	T
I = 8	100	S

ISSN 2348 – 7968

Converting the ciphertext Hexa, bits back to letters ciphertext is "UVQIRSTS"

Now we wants decrypt it using same key.

Cipher Text	Key	Plain Text
U	001	T = 13
V	010	E = 4
Q	010	1 = 8
I	100	E = 4
R	110	V = 5
S	100	I = 8
T	001	S = 12
S	100	I = 8

Deccrypting function D_d is $D_d : f \to f$ by $\Psi \to (\Psi - d) \pmod{26}$

and there by recovers the original message as "TELEVISI"

Problem – 4

Now we use two plain text message P_1 & P_2 encrypted as $C_1 = P_1 + e$ and $C_2 = P_2 + e$ that is we have two messages encrypted with same key one time (e)

In this cryptanalysis we have

$C_1 \oplus C_2 = P_1 \oplus e \oplus P_2 \oplus e = P_1 \oplus P_2$

and key has disappeared from problems.

Lets consider using one – time pad in depth using binary bit encoding.

Suppose we take

P_1 = MAN = 01100 00000 01101, P_2 = CAN = 00010 00000 01101

and both are encrypted with same key 11000 10101 11100

Plain Text P_1	Key	Cipher Text C_1
001100 = M	11000	01010 = K

ISSN 2348 – 7968

00000 = A	10101	10101 = V
01101 = N	11100	10000 = Q
Plain Text P_2	Key	Cipher Text C_2
00010=C	11000	00000 = A
00000=A	10101	10101 = V
01101=N	11100	10000 = Q

Now $C_1 \oplus C_2$

Cipher text $C_1 \oplus C_2$	Plain Text $P_1 \oplus P_2$
01010 ⊕ 00000	K
10101 ⊕ 10101	Q
10000 ⊕ 10000	G

References :

1. **Advanced Encryption standard**
   http:// csrc.nist. gov/encryption/aes/
2. Data encryption standard (DES) ,Federal information processing Standards publication 46-3-1999
3. Oded Goldreich,Foundations of cryptography Volume – II Basic applications
4. Mark Stamp, Information Security principles and practice , 2002.
5. A.R. Vasishtha ,Modern Algebra, Krishna Prakashan Mandir, Meerut.
6. Advanced encryption standanred (AES) ,Federal information processing Standards publications ,197,2001.
7. SergeLang,Introduction to linear algebra ,Second edition, springer
8. Oded Goldreich, Foundations of cryptography, volume I, Basic applications.

ISSN 2348 – 7968

9. Dr. B.S. Grewal, Higher engineering mathematics, 40th edition, Khanna Publications.