Study and analysis of data encryption techniques and implementation using MATLAB programming.

Ananya Banerjee, Swarnendu Moitra, Urmee Karmakar, Sayan Chowdhury, Saheli Datta, SandipanDebnath,
Dr.*Sudhir Chandra Sur degree Engineering College*

***Abstract* :**

This paper is mainly concerned with cyclic code encoding using matrix and polynomial techniques, as well as syndrome decoding utilizing matlab programming. The (7,4) Hamming block which follows the cyclic property is considered here for executing the coding-decoding functions. Systematic code words are produced by convolving message bits with the Generator matrix. Non-systematic codewords develop as a result of polynomial multiplication of message polynomial and generator polynomial expression of (7,4) Hamming code.

Key words— Cyclic Code, Error Syndrome, Hamming Code, Linear Block Code, Nonsystemetic encoding, decoding, Systematic Encoding, .

I. INTRODUCTION :

Data Encryption – Encryption or Coding is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that prevent third parties or the public from reading private messages, various aspects in information security such as data confidentiality, data integrity, authentication, are central to modern cryptography.

The basic problem of the coding theory is that, messages are transmitted over a communication

channel which is subject to noise. Noise can distort messages.

In coding theory, a **linear code** is an error-correcting code for which any linear combination of codewords is also a codeword. Examples of Linear block codes are→

II. THEORY:

HAMMING CODE(7,4) :

In telecom, **Hamming codes** are a family of linear error correcting codes that generalize the Hamming (7,4) and were invented by Richard Hamming in 1950. For each integer $r \geq 2$ there is a code with block length $n = 2^r - 1$ and message length $k = 2^r - r - 1$. The parity-check matrix of a Hamming code is constructed by listing all columns of length r that are non-zero.

CYCLIC CODE:

In coding theory, a **cyclic code** is a block code, where the circular shifts of each codeword gives another word that belongs to the code. Let C be a linear code of block length 'n'. Then C is a cyclic code if, for every codeword C'= (C_1,…..,C_n) from C the word obtained by a cyclic shift of components is again a codeword.

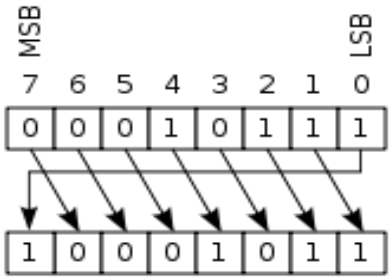

Fig.1

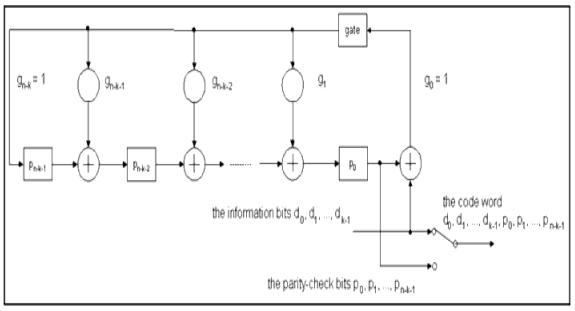

Fig.2 Cyclic Code Encoder Block :-

III. MATHEMATICAL ANALYSIS:

The Generator Matrix for (7,4)

Hamming Block is given by :-

$$G = \begin{pmatrix} 1\,0\,0\,0 & 1\,0\,1 \\ 0\,1\,0\,0 & 1\,1\,1 \\ 0\,0\,1\,0 & 1\,1\,0 \\ 0\,0\,0\,1 & 0\,1\,1 \end{pmatrix}$$

For any message word of 4 bits, say, I = (0001), the required encoded word can be determined by multiplying the information bits with the generator matrix. Here, C = I * G, will give the coded word (0001011), which belongs to the (7,4) Hamming Block.

One bit cyclic rotation will result to another codeword belonging to the same block code. Hence this Linear Code can be termed as Cyclic Code.

Codeword & its one bit ---- 0 0 0 1 0 1 1

rotated version ------- 1 0 0 0 1 0 1

Polynomial Representation Of Cyclic Code:

A code word can be expressed in terms of polynomial equations as given :

$p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \ldots\ldots\ldots\ldots\ldots + a_0x^0$, where, the coefficients will be either 0 or 1.

Suppose, we have a codeword = 0 1 1 0 0 1 0

The equivalent polynomial will be $= 0*x^{7-1} + 1*x^{7-2} + 1*x^{7-3} + 0*x^{7-4} + 0*x^{7-5} + 1*x^{7-6} + 0*x^{7-7}$

$= x^5 + x^4 + x$

For summation of two polynomials, Modulo 2 operation is preferred.

Generator Polynomial : For a block code, first non-zero codeword is a Generator for all the code words, & the corresponding polynomial is denoted as the Generator polynomial. For (7,4) Hamming code, it is $= x^3 + x + 1$

IV. PROCESS:

Non Systematic Cyclic Code generation:

Let the message in bits be = 1 1 0 0

Corresponding message polynomial = $x^3 + x^2$

Multiplying with the generator polynomial will give the encoded polynomial as

$= x^6 + x^5 + x^4 + x^2$. The final coded word in bits is 1 1 1 0 1 0 0, where 1st four bits are not 1100. Hence it is Non- Systematic Cyclic Code.

Systematic Cyclic Code generation:

The systematic form is implemented, where the message bits will be present in the 1st four bits of coded sequence. This is done by the following steps:-

-

a). $i(x) * x^{n-k}$ [i(x)= information polynomial, n= total block length, k=no. of msg bits]

b). $R_{g(x)}[i(x) * x^{n-k}] = r(x)$ [r(x) = remainder of the division]

c). $i(x) * x^{n-k} + r(x) = c(x)$ => Systematic coded polynomial.

For instance, if the message bits are 0 1 1 1, then the systematic version of it will be, 0 1 1 1 0 1 0.

Algorithms utilized in coding process :

For generation of Systematic Cyclic Code :-

a) Assign n(total no. of bits) & k(message bits) to 7 & 4 respectively.

b) Perform the operation :

p<=(k,(n-k)) #parity matrix. And i<= (k,k) #identity matrix

c)Concatenate 'p' & 'I' & assign the result to a variable g<= concatenate(p & i).

d)Ask for the input message from user & store it into a variable 'd'.

e)Multiply the user input & the concatenated result (matrix multiplication).

f)Perform modulo 2 operation & store the result in a variable of choice.

g)Display that variable.

For Non-Systematic Cyclic Code :-

a)For (7,4) Block code, the generator polynomial will be = $x^3 + x + 1$

b)Any message word is to be given by the user in bits.

c)The word is converted into its corresponding polynomial form.

d)The coded polynomial is to be obtained by multiplying the message and generator polynomial & performing modulo 2 operation.

e)The resulting polynomial is re- converted to bits & displayed.

For Decoding Cyclic Codes :

a) Let i := 0. Compute the syndrome s for a received vector r.

b) If s is in the syndrome look-up table, goto Step 6.

c) Let i := i + 1. Enter a 0 into the SR input, computing s_i.

d) If s_i is not in the syndrome look-up table, goto Step 3.

e) Let e_i be the error pattern corresponding to the syndrome s_i. Determine e by cyclically shifting

e_i i times to the left.

f) Let c := r − e. Output c.

Syndrome Decoding for Cyclic Codes :-

Let s(x) be the syndrome polynomial corresponding to a received polynomial r(x).

Let $r_i(x)$ be the polynomial obtained by cyclically shifting the coefficients of r(x) i steps to the right.

Then the remainder obtained when dividing xs(x) by g(x) is the syndrome $s_1(x)$ corresponding to $r_1(x)$.

Having computed the syndrome s with an SR division circuit, we get $s_i(x)$ after the input of i 0s into the circuit.

We then need only store one syndrome s for an error pattern e and all cyclic shifts of e.

The syndrome S can be calculated for matrix form by= $S = r * H^T$

Where r = received word, H= parity check matrix.

V. OUTPUT AND DATA ANALYSIS:

Outputs of the matlab codes of the corresponding algorithms

****

cyclic74_encoder.m

I/P :: The msg word : [1 1 0 1]

O/P ::

Generator Matrix:

1 1 0 1 0 0 0

0 1 1 0 1 0 0

1 1 1 0 0 1 0

1 0 1 0 0 0 1

Message Word:

1 1 0 1

Generator Polynomial:

x^3 + x^2 + 1

The codeword is:

0 0 0 1 1 0 1

****

****

cyc74_decoding.m

1.

Input Code word To be Decoded : [0 0 0 1 1 0 1]

O/P ::

Received word of 7 bit:

0 0 0 1 1 0 1

Syndrome :

0 0 0

The received code is CoRRecT.

0 0 0 1 1 0 1

2.

Input Code word To be Decoded : [0 1 0 1 1 0 1]

received word of 7 bit:

0 1 0 1 1 0 1

Syndrome :

0 1 0

The received code is INCoRRecT.

Correct codeword is:

0 0 0 1 1 0 1

****

****

poly_encoding.m

Enter msg in bit : [0 1 0 1]

Codeword is:

0 1 0 0 1 1 1

VI. CONCLUSION:

The data encryption and decryption technique nowadays are taken to a far advanced stage with the evolution of Cyclic code and quasi cyclic code. This paper is showing that the Encoding and Decoding process of Cyclic code using MatLab programming become a promising technique in error detection and correction process in secure data transmission and reception.

VII. REFERENCES:

[1] Blahut, Richard E. (2003), Algebraic Codes for Data Transmission (2nd ed.), Cambridge University Press .

[2] Hill, Raymond (1988), A First Course In Coding Theory, Oxford University Press .

[3] MacWilliams, F. J.; Sloane, N. J. A. (1977), The Theory of Error-Correcting Codes, New York: North-Holland Publishing.

[4] Van Lint, J. H. (1998), Introduction to Coding Theory, Graduate Texts in Mathematics **86** (3rd ed.), Springer Verlag .

[5] Shu Lin, Daniel J. Costello $J_{R.}$ (1983), Error Control Coding : Fundamentals & Applications.