A2 / ALA / DA-II /

Sharadindu Adhikari 19BCE2105

Q1. Use the Gram-Schmidt orthogonalization on the Euclidean space $\mathbb{R}^4$ to transform the basis $\{(0,1,1,0), (-1,1,0,0), (1,2,0,-1), (-1,0,0,-1)\}$ into an orthonormal basis.

Sol^n: Here we've to orthonormalize the following set of vectors:

$$\bar{v}_1 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \quad \bar{v}_2 = \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad \bar{v}_3 = \begin{bmatrix} 1 \\ 2 \\ 0 \\ -1 \end{bmatrix}, \quad \bar{v}_4 = \begin{bmatrix} -1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$$

Now, w.k.t., according to the Gram-Schmidt process,

$$\bar{u}_K = \bar{v}_K - \sum_{j=1}^{K-1} \text{proj}_{\bar{u}_j}(\bar{v}_K),$$

where $\text{Proj}_{\bar{u}_j}(\bar{v}_K) = \dfrac{\bar{u}_j \cdot \bar{v}_K}{|\bar{u}_j|} \cdot \bar{u}_j$ is a vector projection

The normalized vector is:

$$\bar{e}_K = \frac{\bar{u}_K}{|\bar{u}_K|}$$

- step 1:

$$\bar{u}_1 = \bar{v}_1 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\therefore\ \bar{e}_1 = \frac{\bar{u}_1}{|\bar{u}_1|} = \frac{(0,1,1,0)}{\sqrt{0^2+1^2+1^2+0^2}} = \frac{(0,1,1,0)}{\sqrt{2}} = \left(0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right)$$

$$\bar{e}_1 = \begin{bmatrix} 0 \\ 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{bmatrix}$$

- Step-2 :

$$\bar{u}_2 = \bar{v}_2 - \text{Proj}_{\bar{\mu}_1}(\bar{v}_2) = \bar{v}_2 - \langle \bar{v}_2, \bar{\mu}_1 \rangle \bar{u}_1$$

$$= (-1,1,0,0) - \left(0 + \frac{1}{\sqrt{2}} + 0 + 0\right)\left(0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right)$$

$$= (-1,1,0,0) - \left(0, \frac{1}{2}, \frac{1}{2}, 0\right)$$

$$= \left(-1, \frac{1}{2}, \frac{-1}{2}, 0\right)$$

$$\bar{e}_2 = \frac{\bar{u}_2}{|\bar{u}_2|} = \frac{(-1, 1/2, -1/2, 0)}{\sqrt{(-1)^2 + (1/2)^2 + (1/2)^2 + 0^2}} = \frac{(-1, 1/2, -1/2, 0)}{\sqrt{(3/2)}}$$

$$\bar{e}_2 = \left(-\sqrt{\frac{2}{3}}, \frac{1}{\sqrt{6}}, \frac{-1}{\sqrt{6}}, 0\right)$$

$$\therefore\ \bar{e}_2 = \begin{bmatrix} -\sqrt{2}/\sqrt{3} \\ 1/\sqrt{6} \\ -1/\sqrt{6} \\ 0 \end{bmatrix}$$

- <u>step-3</u> :

$$\bar{u}_3 = \bar{v}_3 - \text{proj}_{\bar{u}_1}(\bar{v}_3) - \text{proj}_{\bar{u}_2}(\bar{v}_3)$$

$$= \bar{v}_3 - \langle \bar{v}_3, \bar{u}_1 \rangle \bar{u}_1 - \langle \bar{v}_3, \bar{u}_2 \rangle \bar{u}_2$$

$$= (1, 2, 0, -1) - (0 + \sqrt{2} + 0 + 0)\left(0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right) -$$

$$\left(-\sqrt{\frac{2}{3}} + \sqrt{\frac{2}{3}} + 0 + 0\right)\bar{u}_2$$

$$= (1, 2, 0, -1) - (0, 1, 1, 0)$$

$$= (1, 1, -1, -1)$$

$$\bar{e}_3 = \frac{\bar{u}_3}{|\bar{u}_3|} = \frac{(1, 1, -1, -1)}{\sqrt{1^2 + 1^2 + (-1)^2 + (-1)^2}} = \frac{(1, 1, -1, -1)}{2} = \left(\frac{1}{2}, \frac{1}{2}, \frac{-1}{2}, \frac{-1}{2}\right)$$

$$\therefore \bar{e}_3 = \begin{bmatrix} 1/2 \\ 1/2 \\ -1/2 \\ -1/2 \end{bmatrix}$$

- <u>step-4</u> :

$$\bar{u}_4 = \bar{v}_4 - \text{Proj}_{\bar{u}_1}(\bar{v}_4) - \text{Proj}_{\bar{u}_2}(\bar{v}_4) - \text{Proj}_{\bar{u}_3}(\bar{v}_4)$$

$$= \bar{v}_4 - \langle \bar{v}_4, \bar{u}_1 \rangle \bar{u}_1 - \langle \bar{v}_4, \bar{u}_2 \rangle \bar{u}_2 - \langle \bar{v}_4, \bar{u}_3 \rangle \bar{u}_3$$

$$= \bar{v}_4 - (0)\cdot\bar{u}_1 - \left(\sqrt{\frac{2}{3}}\right)\cdot\left(-\sqrt{\frac{2}{3}}, \frac{1}{\sqrt{6}}, \frac{-1}{\sqrt{6}}, 0\right) - (0)\cdot\bar{u}_3$$

$$= (-1, 0, 0, -1) - \left(-\frac{2}{3}, \frac{1}{3}, \frac{-1}{3}, 0\right)$$

$$= \left(-1/3, -1/3, 1/3, -1\right)$$

$$\bar{e}_4 = \frac{\bar{u}_4}{|\bar{u}_4|} = \frac{-1/3, -1/3, 1/3, -1}{\sqrt{\frac{1}{9}+\frac{1}{9}+\frac{1}{9}+1}}$$

$$= \left(-\sqrt{3}/6, -\sqrt{3}/6, \sqrt{3}/6, -\sqrt{3}/2\right)$$

$$\therefore \bar{e}_4 = \begin{bmatrix} -\sqrt{3}/6 \\ -\sqrt{3}/6 \\ \sqrt{3}/6 \\ -\sqrt{3}/2 \end{bmatrix}$$

Hence the reqd. set of orthonormal vectors is :

$$\left\{ \left(0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right), \left(-\sqrt{\frac{2}{3}}, \frac{1}{\sqrt{6}}, \frac{-1}{\sqrt{6}}, 0\right), \left(\frac{1}{2}, \frac{1}{2}, \frac{-1}{2}, \frac{-1}{2}\right), \right.$$

$$\left. \left(-\frac{\sqrt{3}}{6}, -\frac{\sqrt{3}}{6}, \frac{\sqrt{3}}{6}, -\frac{\sqrt{3}}{2}\right) \right\}$$

19BCE2105

Q2. Extend the set of vectors $\{(2,3,-1), (1,-2,-4)\}$ to an orthogonal basis of the Euclidean space $\mathbb{R}^3$ with the standard inner product and then find the associated orthonormal basis.

Sol^n

Let $\bar{v}_1 = (2,3,-1)$ and $\bar{v}_2 = (1,-2,-4)$.

We can see that they are orthogonal to each other, then $\langle \bar{v}_1, \bar{v}_2 \rangle$ should be zero.

Let's see: $\langle \bar{v}_1, \bar{v}_2 \rangle = 2\times 1 + 3\times(-2) + (-1)\cdot(-4)$

$= 2 - 6 + 4$

$= 0$, hence they're orthogonal to each other

Let the third vector, $\bar{v}_3 = (x, y, z)$ which should be orthogonal to these 2 vectors

So,

$\langle \bar{v}_1, \bar{v}_3 \rangle = 0$; $\langle \bar{v}_2, \bar{v}_3 \rangle = 0$

$\Rightarrow 2x + 3y - z = 0$ $\qquad \Rightarrow x - 2y - 4z = 0$

$\Rightarrow 2(2y + 4z) + 3y - z = 0$ $\qquad \Rightarrow x - 2y = 4z$

$\Rightarrow 4y + 8z + 3y - z = 0$ $\qquad \Rightarrow x = 4z + 2y$

$\Rightarrow 7y + 7z = 0$ $\qquad \Rightarrow \boxed{x = 2z}$

$\Rightarrow \boxed{y = -z}$

We've 2 eq^{ns} and 3 variables, then we've to take $z = 1$ as it is a free variable. Then we get the $\bar{v}_3$ vector

$\therefore \quad \bar{v}_3 = (x, y, z) = (2, -1, 1)$.

Now we'll do the normalization in order to get the orthonormal basis.

$$\bar{u}_1 = \bar{v}_1 = \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix} \quad . \quad \bar{e}_1 = \frac{\bar{u}_1}{|\bar{u}_1|} = \begin{bmatrix} 2/\sqrt{14} \\ 3/\sqrt{14} \\ -1/\sqrt{14} \end{bmatrix}$$

$$\bar{u}_2 = \bar{v}_2 = \begin{bmatrix} 1 \\ -2 \\ -4 \end{bmatrix} \quad . \quad \bar{e}_2 = \frac{\bar{u}_2}{|\bar{u}_2|} = \begin{bmatrix} 1/\sqrt{21} \\ -2/\sqrt{21} \\ -4/\sqrt{21} \end{bmatrix}$$

$$\bar{u}_3 = \bar{v}_3 = \begin{bmatrix} 2 \\ -1 \\ 1 \end{bmatrix} \quad . \quad \bar{e}_3 = \frac{\bar{u}_3}{|\bar{u}_3|} = \begin{bmatrix} 2/\sqrt{16} \\ -1/\sqrt{16} \\ 1/\sqrt{16} \end{bmatrix}$$

Hence the associated orthonormal basis is:

$$\left\{ \left(2/\sqrt{14}, 3/\sqrt{14}, -1/\sqrt{14}\right), \left(1/\sqrt{21}, -2/\sqrt{21}, -4/\sqrt{21}\right), \left(2/\sqrt{16}, -1/\sqrt{16}, 1/\sqrt{16}\right) \right\}$$

19BCE2105

Q3. Find an orthonormal basis of the row space of the matrix :

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 \\ 2 & 1 & 2 & 3 \end{bmatrix}$$

Sol : Basis of the row-space :

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 \\ 2 & 1 & 2 & 3 \end{bmatrix} \quad \begin{matrix} R_2 \leftarrow R_2 - R_1 \\ R_3 \leftarrow R_3 - 2R_1 \end{matrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & 0 & 1 \end{bmatrix} \quad \begin{matrix} R_3 \leftarrow R_3 + R_2 \checkmark \\ R_1 \leftarrow R_1 - R_2 \checkmark \end{matrix}$$

$$\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Clearly, as we can see the leading 1's in the row-echelon form, only rows R_1 and R_2 are linearly independent, thereby forming the basis of rowspace.

$\therefore$ Basis : $\{(1,0,1,2), (0,1,0,-1)\}$.

Now, let $\bar{v}_1 = (1,0,1,2)$, and $\bar{v}_2 = (0,1,0,-1)$.

According to the Gram- Schmidt process,

$$\bar{u}_K = \bar{V}_K - \sum_{J=1}^{K-1} \text{Proj}_{\bar{u}_J} (\bar{V}_K),$$

where, $\text{proj}_{\bar{u}_J}(\bar{V}_K) = \frac{\bar{u}_J \cdot \bar{V}_K}{|\bar{u}_J|} \cdot \bar{u}_J$ is a vector projection.

The normalized vector is :

$$\bar{e}_K = \frac{\bar{u}_K}{|\bar{u}_K|}$$

We've:

$$\bar{u}_1 = \bar{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 2 \end{bmatrix}$$

$$\bar{e}_1 = \frac{\bar{u}_1}{|\bar{u}_1|} = \frac{(1, 0, 1, 2)}{\sqrt{6}} = \left(\frac{1}{\sqrt{6}}, 0, \frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}\right)$$

$$\therefore \bar{e}_1 = \begin{bmatrix} 1/\sqrt{6} \\ 0 \\ 1/\sqrt{6} \\ 2/\sqrt{6} \end{bmatrix}$$

lly,

$$\bar{u}_2 = \bar{v}_2 - \text{Project}_{\bar{u}_1}(\bar{v}_2)$$

$$= (0, 1, 0, -1) - \langle \bar{v}_2, \bar{u}_1 \rangle \bar{u}_1$$

$$\bar{u}_2 = \bar{v}_2 - \text{Proj}_{\bar{u}_1}(\bar{v}_2)$$

$$= (0,1,0,-1) - \left(\frac{-2}{\sqrt{6}}\right)\cdot\left(\frac{1}{\sqrt{6}}, 0, \frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}\right)$$

$$= (0,1,0,-1) + \left(\frac{2}{6}, 0, \frac{2}{6}, \frac{4}{6}\right)$$

$$= \left(\frac{1}{3}, 1, \frac{1}{3}, \frac{-1}{3}\right)$$

$$\bar{e}_2 = \frac{\bar{u}_2}{|\bar{u}_2|} = \frac{1/3, 1, 1/3, -1/3}{\sqrt{\frac{1}{9}+1+\frac{1}{9}+\frac{1}{9}}} = \left(\frac{\sqrt{3}}{6}, \frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{6}, -\frac{\sqrt{3}}{6}\right)$$

$$\therefore \bar{e}_2 = \begin{bmatrix} \sqrt{3}/6 \\ \sqrt{3}/2 \\ \sqrt{3}/6 \\ -\sqrt{3}/6 \end{bmatrix}$$

$\therefore$ The reqd. set of orthonormal vectors is:

$$\left\{\left(\frac{1}{\sqrt{6}}, 0, \frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}\right), \left(\frac{\sqrt{3}}{6}, \frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{6}, -\frac{\sqrt{3}}{6}\right)\right\}$$

19BCE2105

Q4. In $\mathbb{R}^3$, let $\alpha = (a_1, a_2, a_3)$, $\beta = (b_1, b_2, b_3)$.
Determine whether $\langle , \rangle$ is a real inner product for $\mathbb{R}^3$, if $\langle , \rangle$ be defined by:

(i) $\langle \alpha, \beta \rangle = |a_1 b_1 + a_2 b_2 + a_3 b_3|$;

(ii) $\langle \alpha, \beta \rangle = (a_1 + a_2 + a_3) \cdot (b_1 + b_2 + b_3)$;

(iii) $\langle \alpha, \beta \rangle = a_1 b_1 + (a_2 + a_3) \cdot (b_2 + b_3)$;

(iv) $\langle \alpha, \beta \rangle = a_1 b_1 + (a_2 + a_3) \cdot (b_2 + b_3) + a_3 b_3$.

Sol^n:

(i) a) $\langle \alpha, \beta \rangle = |a_1 b_1 + a_2 b_2 + a_3 b_3|$

$= |b_1 a_1 + b_2 a_2 + b_3 a_3|$

$= \langle \beta, \alpha \rangle$

$\therefore$

b) $\langle \alpha + \beta, \gamma \rangle = \langle \alpha, \gamma \rangle + \langle \beta, \gamma \rangle$. Let $\gamma = (c_1, c_2, c_3)$

$\langle \alpha + \beta, \gamma \rangle = |(a_1 + b_1) c_1 + (a_2 + b_2) c_2 + (a_3 + b_3) c_3|$

$= |a_1 c_1 + b_1 c_1 + a_2 c_2 + b_2 c_2 + a_3 c_3 + b_3 c_3|$

$= |\langle \alpha, \gamma \rangle + \langle \beta, \gamma \rangle|$

Now, we know that, $|a| + |b| \geqslant |a+b|$.

So the above equality is not possible even if we take individual modulus. So, this is NOT inner product space.

(ii) a) $\langle \alpha, \alpha \rangle \geqslant 0$ and $\langle \alpha, \alpha \rangle = 0$ only for $\alpha = (0,0,0)$.

$$\langle \alpha, \beta \rangle = (a_1 + a_2 + a_3) \cdot (b_1 + b_2 + b_3)$$

$$\langle \alpha, \alpha \rangle = (a_1 + a_2 + a_3)^2.$$

But here if we pull $\alpha = (-1, 0, 1)$, then $\langle \alpha, \alpha \rangle = 0$.

But it should be 0 only for $\alpha = (0,0,0)$.

So, it as well is NOT inner product space.

(iii) a) $\langle \alpha, \alpha \rangle \geqslant 0$ and $\langle \alpha, \alpha \rangle = 0$ iff $\alpha = (0,0,0)$.

$$\langle \alpha, \alpha \rangle = a_1^2 + (a_2 + a_3)^2$$

Here also if we take $\alpha = (0, 1, -1)$, then $\langle \alpha, \alpha \rangle = 0$;

but it should be 0 only for $\alpha = (0,0,0)$.

So, it is NOT inner product space as well.

(iv) a)
$$\langle \alpha, \beta \rangle = a_1 b_1 + (a_2 + a_3) \cdot (b_2 + b_3) + a_3 b_3$$
$$= b_1 a_1 + (b_2 + b_3) \cdot (a_2 + a_3) + b_3 \cdot a_3$$
$$= \langle \beta, \alpha \rangle$$

b) $\langle K\alpha, \beta \rangle = K \cdot a_1 \cdot b_1 + (K \cdot a_2 + K \cdot a_3) \cdot (b_2 + b_3) + K \cdot a_3 \cdot b_3$

$= K \cdot a_1 b_1 + K(a_2 + a_3) \cdot (b_2 + b_3) + K \cdot a_3 \cdot b_3$

$= K \cdot (a_1 b_1 + (a_2 + a_3) \cdot (b_2 + b_3) + a_3 \cdot b_3)$

$= K \cdot \langle \alpha, \beta \rangle$

c) $\langle \alpha + \beta, \gamma \rangle = \langle \alpha, \gamma \rangle + \langle \beta, \gamma \rangle$; let $\gamma = (c_1, c_2, c_3)$

$\langle \alpha + \beta, \gamma \rangle = (a_1 + b_1) c_1 + (a_2 + b_2 + a_3 + b_3) \cdot (c_2 + c_3) +$
$(a_3 + b_3) \cdot c_3$

$= a_1 c_1 + b_1 c_1 + (a_2 + a_3) \cdot (c_2 + c_3) + (b_2 + b_3) \cdot (c_2 + c_3)$
$+ a_3 c_3 + b_3 c_3$

$= a_1 c_1 + (a_2 + a_3) \cdot (c_2 + c_3) + a_3 c_3 +$
$b_1 c_1 + (b_2 + b_3) \cdot (c_2 + c_3) + b_3 c_3$

$= \langle \alpha, \gamma \rangle + \langle \beta, \gamma \rangle$

d) $\langle \alpha, \alpha \rangle \geq 0$ and $\langle \alpha, \alpha \rangle = 0$ iff $\alpha = (0, 0, 0)$

$\langle \alpha, \alpha \rangle = a_1^2 + (a_2 + a_3)^2 + a_3^2$

Here, it will always be positive (+ve), because even if $a_2 + a_3$ is 0 for anything other than $a_2 = 0$, $a_3 = 0$, there will always some value left for a_3^2 or a_1^2.

Let $\alpha = (0,0,0)$.

Then, $\langle \alpha, \alpha \rangle = 0+0+0 = 0$

So it satisfies all the 4 conditions, Hence THIS IS an inner product space.

— 19BCE2105 —

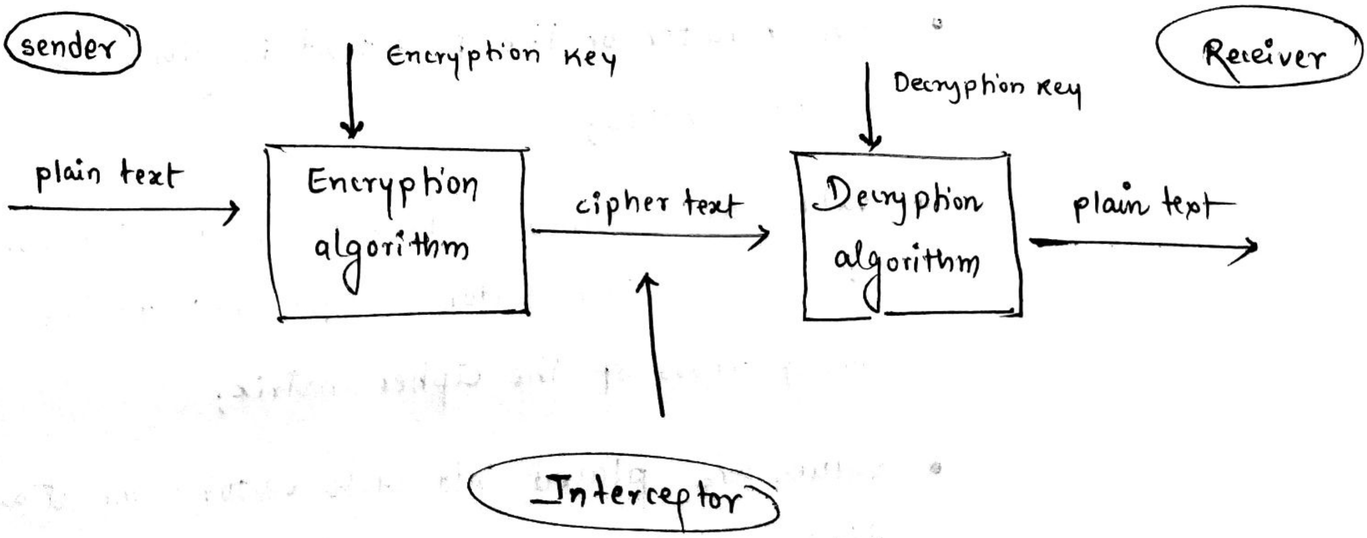
Q5. Write notes on the following subjects:

1: classical cryptosystems — Plain text, Cipher Text, Encryption, Decryption.

Sol^n:

classical cryptosystems :

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.



Components of cryptosystem :

a) **Plain text** : It means unencrypted information, pending input into cryptographic algorithms, usually encryption algorithms. This usually refers to data that is transmitted or stored unencrypted.

b) **Cipher text** : It is the scrambled version of the plain text produced by the encryption algorithm using a speific encryption key. It flows on public channel.

c) **Encryption algo.** : It is a mathematical proces that produces a cipher text for any given plaintext and encryption key. Details :

- each character of the plaintext is given a numerical value;
- values are separated into vectors, such that no. of rows of each vector is equivalent to the no. of rows of the cipher matrix;
- values are placed into each vector: one at a time, going down a row for each value. Once a vector is filled, the next vector is created;

- the vectors are then augmented to form a matrix that contains the plain text ;
- the plain text matrix is then multiplied with the cipher matrix to create the cipher text.

d) **Decryption algo :** It is a mathematical algorithm that produces a unique plaintext for any given ciphertext and decryption key. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it. Details :

- To decrypt a ciphertext message (matrix), the original cipher matrix must be used. The cipher matrix must be inverted in order to decrypt the cipher text.
- This inverted cipher matrix is then multiplied with the cipher matrix.
- The product produces the original plain text matrix.
- The plaintext can be found again by taking this product and splitting it back up into its separate vectors, and then converting the numbers back into their latter forms.

e) **Encryption Key :** It is a value that is known to the Sender.

f) **Decryption key :** It is a value that is known to the receiver

- 19BCE2105 -

2. Introduction to wavelets (only approx. of wavelet from Raw data.)

Sol^n:

The fundamental idea behind wavelets is to analyze according to scale. Indeed, some researchers feel that a whole new mindset or perspective is refreshing in processing data.

Wavelets are functions that satisfy certain mathematical requirements, and are used in representing data or other functions.

Approximations using superposition of functions has existed since the early 1800s. The wavelet analyses the scale that we use to look at data plays a special role. Wavelet algorithm process data at different scales of resolutions.

The wavelet analysis procedure is to adopt a wavelet prototype function, called an analyzing wavelet or mother wavelet.

THE DISCRETE WAVELET TRANSFORM :

Dilations and translations of the "mother function" of "analyzing wavelet" $\phi(x)$, defined on orthogonal basis, our wavelet basis :

$$\phi_{(s,l)}(x) = 2^{-s/2} \cdot \phi\left(2^{-s} x - l\right).$$

The variables s and l are integers that scale and dilate the mother function ϕ to generate wavelets.

To span our data domain at different resolutions, the analyzing wavelet is used in a scaling equation:

$$W(x) = \sum_{K=-1}^{N-2} (-1)^K \cdot C_{K+1} \cdot \phi(2x + K)$$

$W(x)$ is the scaling function for the mother function ϕ, and C_K are the wavelet coefficients. The wavelet coefficients must satisfy linear and quadratic constraints of the form:

$$\sum_{K=0}^{N-1} C_K = 2, \quad \sum_{K=0}^{N-1} C_K \cdot C_{K+2l} = 2\,\delta_{l,0}$$

where δ is the delta function and l is the location index

[please turn over]

Applications of Wavelets :

i) Computer and human vision

ii) FBI fingerprint compression

iii) Denoising noisy data

iv) Detecting self-similar behaviour in a time-series

v) Musical note.