CREATING A CIPHER FOR DATA SECURITY

Charles Ndung'u

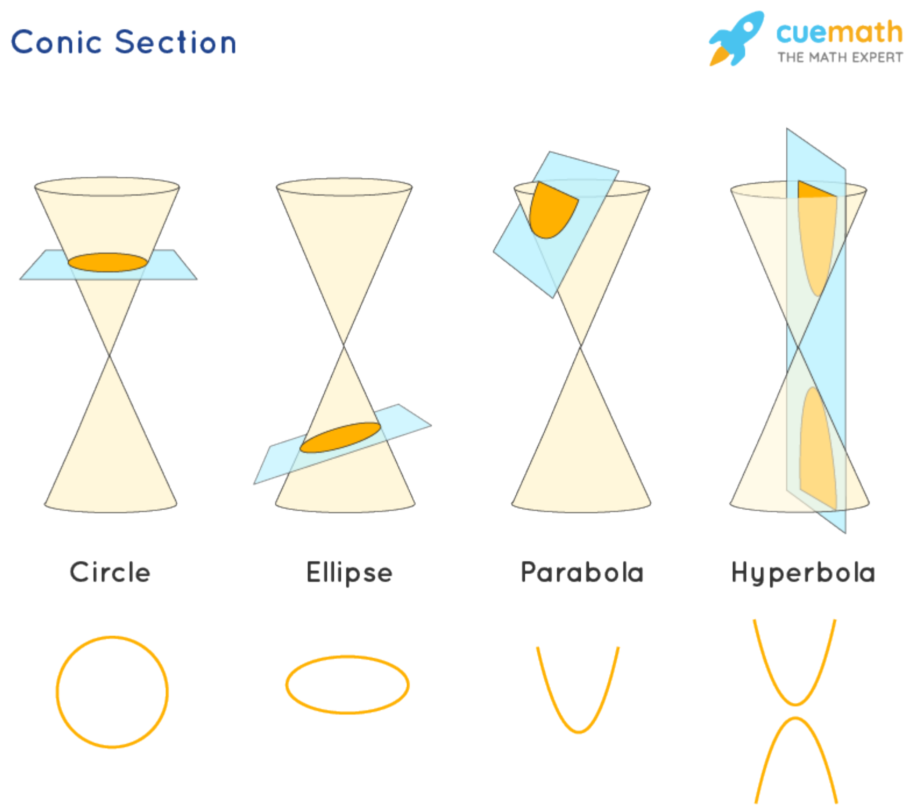
March 2023

1 BACKGROUND KNOWLEDGE FOR THE CIPHER DEVELOPMENT

1) Conic Section. 2) Laplace Transforms. 3) Linear Algebra. 4) Ordinary Differential Equations. 5) Partial Differential Equations.

2 Conic Sections Recarp.

We will develop a cryptographic cipher using the knowledge of Cones and planes. The cipher will be used to encrypt password in SQL databases. A conic section, conic or a quadratic curve is a curve obtained from a cone's surface intersecting a plane. The three types of conic section are the hyperbola, the parabola, and the ellipse; the circle is a special case of the ellipse, though it was sometimes called as a fourth type. Diagram 1.0



From the above diagram we shall beigin with getting the areas of the figures which will lead to cryptographic cipher development.

AREA OF A CIRCLE CIPHER DEVELOPMENT

$$X^2 + Y^2 = R^2(Equationofacirclewithcenterattheorin(0,0) \tag{1}$$

$$(X-a)^2+(Y-b)^2 = R^2(Equationofacircleatthecenter(a,b)noteaandbarepositive) \tag{2}$$

Example of each case: Given the center of a circle with radius 4 center (3,0) find the equation of the circle.

$$(X-a)^2 + (Y-b)^2 = R^2 \tag{3}$$

$$(X-3)^2 + (Y-0)^2 = 16 \tag{4}$$

$$X^2 - 6X + 9 + Y^2 + 16 \tag{5}$$

$$AnswerX^2 + Y^2 - 6X - 7 = 0(andthusthisisourequationofthecircle) \tag{6}$$

Example 2
Given the following equation with center at the origin find the radius

$$X^2 + Y^2 = 16 \tag{7}$$

$$fromtheequationofacircleX^2 + Y^2 = R^2 \tag{8}$$

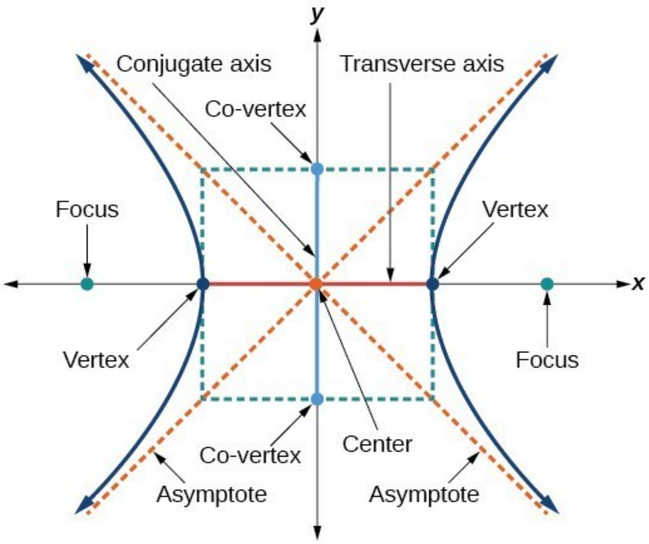
$$R^2 = 16 \tag{9}$$

$$R = \sqrt{16} \tag{10}$$

$$R = 4 \tag{11}$$

Which is the radius of our circle. EQUATION OF A HYPERBOLA

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1 \tag{12}$$



Here the diagram shows a hyperbola whose center is at the origin otherwise the equation of a parabola whose center is not on the origin is given by

$$\frac{(X-h)^2}{a^2} - \frac{(Y-K)^2}{b^2} = 1 \tag{13}$$

Example given the following equation get the Center, Focus, Asymptotes, Vertices.

$$\frac{(X-3)^2}{25} - \frac{Y-5}{16} = 1 \tag{14}$$

Center is (3,5)

$$C^2 = a^2 + b^2 \tag{15}$$

$$C^2 = \sqrt{41} \tag{16}$$

$$C = (+-)6.4031 \tag{17}$$

Our focus is (-6.4031,0) and (6.4031,0)
Our vertices are given by $\sqrt{25} = (+-)5, (3+-5,5)thus(-2,5)and(8,5)isourvertices$
$TheFociare(-3.4031,5)and(9.4031,5)$

3 The Laplace Recarp

Here we shall use the differential property of the laplace transform

$$\mathcal{L}\{f(t)\} = \int_{t=0}^{\infty} f(t)e^{-st}f(t)dt \tag{18}$$

In this case, we want to find the Laplace transform of X^2. Using the definition of the Laplace transform, we have:

$$F(s) = \mathcal{L}X^2 \quad = \int_0^{\infty} e^{-st}X^2 dt \tag{19}$$

$$\mathcal{L}X^2 = \mathcal{L}t^2 = \frac{2!}{s^{2+1}} = \frac{2}{s^3} \tag{20}$$

In LaTeX, you can typeset the Laplace transform of X^2 using the following code:

$$\mathcal{L}X^2 = \mathcal{L}t^2 = \frac{2!}{s^{2+1}} = \frac{2}{s^3} \tag{21}$$

THE DIFFERENTIABILITY PROPERTY OF THE LAPLACE TRANSFORMS

$$\mathcal{L}f^n(t) = S^nF\bar(s) - S^{n-1}f(0) - S^{n-2}f'(0) - S^{n-3}f''(0) - \tag{22}$$

$$\mathcal{L}e^-2t \tag{23}$$

Solving using the differential laplace property we have

$$\mathcal{L}e^-2t = s^2\mathcal{L}F\bar(s) - S^{n-1}f(0) - S^{n-2}f'(0) \tag{24}$$

$$\mathcal{L}e^-2t = S^2\mathcal{L}e^-2t - s(1) + 2 \tag{25}$$

$$\mathcal{L}4e^-2t = S^2\mathcal{L}e^-2t - S + 2 \tag{26}$$

$$\mathcal{L}e^-2t(4 - S^2) = -s + 2 \tag{27}$$

$$\mathcal{L}e^-2t = \frac{S-2}{S^2-4} \tag{28}$$

$$S^2 - 4 = (S-2)(S+2) \tag{29}$$

$$\mathcal{L}e^-2t = \frac{1}{S+2} \tag{30}$$

4 Ordinary Differential Equations Recarp

Here we shall look at solving ODE's using the D-Operator and getting the general solutions, this will help us in making of the cipher.
Example: solve the following using the D-Operator

$$D^2(sin5x) = -25sin5x \tag{31}$$

example 2:

$$D(X^3 - 5X) = 3X^2 - 5 \tag{32}$$

example 3:

$$D(e^2x) = 2e^2x \tag{33}$$

Now let us solve an ODE just to get familiar with it using the D-Operator;
Example 4:

$$\frac{d^{2y}p}{dx^2} + \frac{2yp}{dx} + 26yp = 5cos2x \tag{34}$$

$$(D^2 + 2D + 26)yp = 5cos2x \tag{35}$$

$$yp = \frac{1}{D^2 + 2D + 26}(5cos2x) \tag{36}$$

$$yp = \frac{1}{-4 + 2D + 26}(5cos2x) \tag{37}$$

$$yp = \frac{1}{2(D + 11)}(5cos2x) \tag{38}$$

$$yp = \frac{5}{2}(\frac{1}{D + 11})cos2x \tag{39}$$

$$yp = \frac{5}{2}(\frac{D - 11}{D^2 - 121})cos2x \tag{40}$$

$$yp = \frac{-1}{50}(Dcos2x - 11cos2x) \tag{41}$$

$$yp = \frac{-1}{50}(-2sin2x - 11cos2x) \tag{42}$$

$$yp = \frac{2}{50}(sin2x) + \frac{11}{50}(cos2x) \tag{43}$$

Example 5:

$$\frac{1}{D}(e^{4x}Sin2x) \tag{44}$$

$$e^{4x}(\frac{1}{D + 4})sin2x \tag{45}$$

$$e^{4x}(\frac{1}{D + 4})(\frac{-D + 4}{-D + 4})sin2x \tag{46}$$

$$e^{4x}(\frac{-D+4}{-D^2+16})sin2x \tag{47}$$

$$e^{4x}(\frac{-D+4}{4+16})sin2x \tag{48}$$

$$\frac{1}{20}e^{4x}(-Dsin2x+4sin2x) \tag{49}$$

$$\frac{-1}{20}e^{4x}(2cos2x-4sin2x)+c \tag{50}$$

Example 6:

$$D(e^{2x}cos3x)=e^{2x}(D+2)cos3x \tag{51}$$

$$e^{2x}[D(cos3x)+2cos3x] \tag{52}$$

Answer :

$$e^{2x}[-3sin3x+2cos3x] \tag{53}$$

5 Partial Differential Eqautions recarp

Here we shall look at the famous Monge's Notation which is vital in solving PDE's which is knowledge required in creating our cryptographic cipher, thus we shall begin by writting down the monges notation:

$$p=\frac{\partial z}{\partial x},q=\frac{\partial z}{\partial y},r=\frac{\partial^2 z}{\partial^2 x},t=\frac{\partial^2 z}{\partial^2 y},s=\frac{\partial^2 z}{\partial x\partial y} \tag{54}$$

We shall solve a few examples just to create muscle memory using Monge's notation,
Example 7: eliminate the arbitrary constants from the equation.

$$z=ax+by+ab \tag{55}$$

Thus here we will apply the Monge's notation to perform the operation.

$$\frac{\partial z}{\partial x}=a,\frac{\partial z}{\partial y}=b \tag{56}$$

thus replacing a and b with the partial derivatives from Monge's notation we obtain

$$z=px+qy+pq \tag{57}$$

where p=q
find the general solution to the PDE

$$2p+3q=1 \tag{58}$$

solution :

$$\frac{dx}{2}=\frac{dy}{3}=\frac{dz}{1} \tag{59}$$

$$C1 = \frac{x}{2} - \frac{y}{3} \tag{60}$$

and also

$$\frac{dy}{3} = \frac{dz}{1} \tag{61}$$

$$C2 = \frac{y}{3} - \frac{z}{1} \tag{62}$$

solving C1 and C2 we have

$$\frac{3x - 2y}{6} = 0 \tag{63}$$

and

$$\frac{y - 3z}{3} = 0 \tag{64}$$

the final solution is

$$(3x - 2y), (y - 3z) \tag{65}$$

Example 8:
Wrapping up all the skills we shall find the characteristics of the given hyperbolic equation

$$x\frac{\partial^2 u}{\partial^2 x} - y\frac{\partial^2 u}{\partial x} + \frac{\partial u}{\partial x} \tag{66}$$

solution :

$$x(y')^2 + y'y = o \tag{67}$$

$$y'(xy' + y) = 0 \tag{68}$$

This implies that y=C1 and now our C2 will be given by

$$x(\frac{dy}{dx} + y) = 0 \tag{69}$$

on solving(By separation of variables) we have:

$$ln|y| + ln|x| = ln|C2| \tag{70}$$

$$ln|xy| = ln|C2| \tag{71}$$

thus we can see that our r=y and s=xy
we now solve our PDE :

$$\frac{\partial u}{\partial x} = (\frac{\partial u}{\partial r}\frac{\partial r}{\partial x}) + (\frac{\partial u}{\partial s}\frac{\partial s}{\partial x}) = y(\frac{\partial u}{\partial s}) \tag{72}$$

solving the second derivative of U W.R.T x

$$\frac{\partial^2 u}{\partial x^2} = y[\frac{\partial^2 u}{\partial r}\frac{\partial r}{\partial y} + \frac{\partial^2 u}{\partial s^2}\frac{\partial s}{\partial y}] = y^2\frac{\partial^2 u}{\partial s^2} \tag{73}$$

$$\frac{\partial^2 u}{\partial x \partial y} = \frac{\partial u}{\partial s} + y[\frac{\partial^2 u}{\partial r \partial s}\frac{\partial r}{\partial y} + \frac{\partial^2 u}{\partial s^2}\frac{\partial s}{\partial y}] = \frac{\partial y}{\partial s} + y\frac{\partial^2 u}{\partial r \partial s} + xy\frac{\partial^2 u}{\partial s^2} \tag{74}$$

substituting back we get

$$-y^2\frac{\partial^2 u}{\partial r \partial s} = 0 \tag{75}$$

6 Advanced Linear Algebra 1 And 2

Let's start by getting the characteristic equation for the following matrices
$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$
To get the characteristic equation, recall

$$A - \lambda I = 0 \tag{76}$$

using this we can know the characteristic equation to be:

$$x2 - xTr(M) + detM = 0 \tag{77}$$

this is for a 2*2 matrix
let us see for a 3*3 matrix

$$x^3 - tr(A)x^2 + (A_{11} + A_{22} + A_{33})x - det(A) = 0 \tag{78}$$

Back to our question the characteristic equation is given by;

$$x^2 - (4)x + 3 = 0 \tag{79}$$

$$sum = -4, product = 3 \tag{80}$$

$$(-3, -1) \tag{81}$$

are our Eigen values, to get the Eigen vectors we write;
$\begin{pmatrix} 2-\lambda & 1 \\ 1 & 2-\lambda \end{pmatrix}$ where $\lambda is = (3, 1)$

$\det(A - \lambda I) = \begin{vmatrix} 2-\lambda & 1 1 & 2-\lambda \end{vmatrix} \quad = (2-\lambda)^2 - 1 \; = \lambda^2 - 4\lambda + 3 \quad = (\lambda - 1)(\lambda - 3).$

Thus, the eigenvalues of A are $\lambda_1 = 1$ and $\lambda_2 = 3$.

To find the corresponding eigenvectors, we solve the system of equations $(A - \lambda_i I)\mathbf{v_i} = \mathbf{0}$, where $\mathbf{v_i}$ is the eigenvector corresponding to λ_i.

For $\lambda_1 = 1$, we have

$$(A - \lambda_1 I)\mathbf{v_1} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad = \begin{bmatrix} x+y \\ x+y \end{bmatrix} = \begin{bmatrix} x+y=0 \\ x+y=0 \end{bmatrix} = \begin{bmatrix} x = x \\ x = -y \end{bmatrix}.$$

This implies that x=1 and y=-1 Thus, we need to find x and y such that $x + y = 0$, which gives $\mathbf{v_1} = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$.
Similarly, for $\lambda_2 = 3$, we have

$$(A - \lambda_2 I)\mathbf{v_2} = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -x+y \\ x-y \end{bmatrix} = \begin{bmatrix} -x = -x \\ x = y \end{bmatrix} = \begin{bmatrix} x = 1 \\ 1 = y \end{bmatrix}.$$

Thus, we need to find x and y such that $-y + x = 0$ and $x - y = 0$, which gives $\mathbf{v_2} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

Therefore, the eigenvectors corresponding to λ_1 and λ_2 are $\mathbf{v_1} = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$ and $\mathbf{v_2} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, respectively. You can also use Gauss Jordan Elimination Reduced Row Echelon Form First, we can add the first equation to the second equation to obtain

$$\begin{aligned} -x + y &= 0 \\ 0 &= 0. \end{aligned}$$

This tells us that $y = x$

7 Cipher Creation

One way to create a cipher using the equation of a hyperbola is to use the hyperbola's parametric equation. The parametric equation of a hyperbola is given by:
The equation of a circle with center (a, b) and radius r can be expressed in terms of tan and sin as follows:

$(x - a)^2 + (y - b)^2 = r^2$

Dividing both sides by r^2 and making the substitution $u = \frac{x-a}{r}$ and $v = \frac{y-b}{r}$, we get:

$u^2 + v^2 = 1$

Now, we can express u and v in terms of tan and sin using the following identities:

$\tan^2\theta + 1 = \sec^2\theta$

$\sin^2\theta + \cos^2\theta = 1$

Let θ be the angle between the positive x-axis and the line joining (a, b) to (x, y). Then we have:

$u = \frac{x-a}{r} = \frac{r\cos\theta}{r} = \cos\theta$

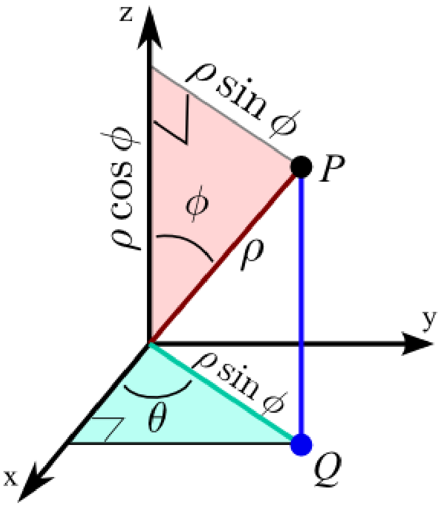
$v = \frac{y-b}{r} = \frac{r\sin\theta}{r} = \sin\theta$

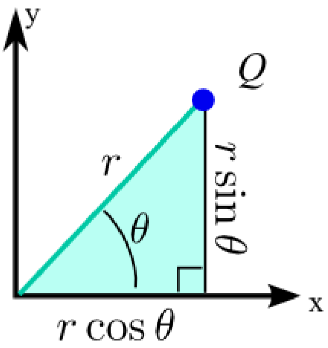
Substituting these expressions for u and v into the equation $u^2 + v^2 = 1$, we obtain:

$\cos^2\theta + \sin^2\theta = 1$

Therefore, the equation of a circle with center (a, b) and radius r can be expressed in terms of tan and sin as:

$(\frac{x-a}{r})^2 + (\frac{y-b}{r})^2 = \sin^2\theta + \cos^2\theta = 1$





The equation of a unit circle centered at the origin is given by

$$sin^2\theta + cos^2\theta = 1 \tag{82}$$

Where 1 is the radius using this knowledge we now form our cipher as below: Suppose we want to encrypt the message ”SECRET” using the equation of a circle. We can do this by mapping each letter to a point on a circle and then using the coordinates of the point as the encrypted message.

To map the letters to points on the circle, we can assign each letter a number based on its position in the alphabet (A = 1, B = 2, etc.). Then, we can use these numbers as the angle (in radians) to find the corresponding point on the unit circle using the equation:

$$x = cos(\theta) \tag{83}$$

$$y = sin(\theta) \tag{84}$$

For example, the letter ”S” has a numerical value of 19, so we can map it to the point:

$$x = cos(19) \tag{85}$$

$$y = sin(19) \tag{86}$$

Similarly, we can map the other letters to points on the circle:
E: $(x, y) = (\cos(5), \sin(5))$
C: $(x, y) = (\cos(3), \sin(3))$
R: $(x, y) = (\cos(18), \sin(18))$
E: $(x, y) = (\cos(5), \sin(5))$
T: $(x, y) = (\cos(20), \sin(20))$
The encrypted message is then the coordinates of these points in order:
Encrypted message:
(0.940,0.342),(0.959,0.283),(0.995,0.105),(0.982,0.190),(0.959,0.283),(0.939,0.345)
To decrypt the message, the recipient can use the reverse process by finding the

angles corresponding to the given points on the circle and mapping them back to their corresponding letters.
To decrypt the message, the recipient needs to find the angles corresponding to the given points on the circle and then map these angles back to their corresponding letters using the alphabet.

To find the angles, the recipient can use the inverse functions of sine and cosine:

$$\theta = arctan(\frac{y}{x}) \tag{87}$$

Note that the inverse of Tangent is represented by arctan or tan inverse. The trigonometric functions/ratios are: Sine/Cosine

$$tan = \frac{sin}{cos} \tag{88}$$

For example, to decrypt the first point (0.9455, 0.3256), the recipient can find the angle using:

$$\theta = arctan(\frac{0.3255}{0.9455}) \tag{89}$$

which gives 19.0021 approximately 19 when rounded off to the nearest tenths. or the first point, the decrypted letter is:

Decrypted letter: S (19) Decrypted letter: S(19)

Similarly, we can decrypt the other points on the circle to obtain the original message:
(-0.959, 0.283): E (5)
(-0.995, -0.105): C (3)
(0.982, -0.190): R (18)
(-0.959, 0.283): E (5)
(0.939, 0.345): T (20)
The decrypted message is "SECRET".

8 Implementations Of The Cipher

The primary use of this cipher is to provide a secure way of transmitting sensitive information between two parties. By encrypting the message using a cipher algorithm, the message becomes unreadable to anyone who does not have the key or knowledge of the algorithm. The intended recipient can then decrypt the message using the same key or algorithm to read the original plaintext message.
Some common uses of this cipher include:
Military and national security: Ciphers are often used by military and government agencies to communicate classified information and keep sensitive data secure from adversaries.
Business and finance: Companies may use ciphers to protect confidential information such as financial data, trade secrets, and client information from competitors and hackers.
Personal communication: Individuals can use ciphers to send private messages

and keep their personal information secure from unauthorized access.
Note this cipher uses the circle equation as the secrete key and thus you should note share the equation with the message you are encrypting.
we can make this encryption algorithim more complex by not using a unit circle centered at the origin like we have done, we can also use the hyperbolic functions in PDE to make it more complex.

Thank you!