Third Dimensional Determinants and its Application in Cryptography

ADITYA MITRA

Contents

Third Dimensional Determinants and its Application in Cryptography

Abstract

Determinant can be defined as a scalar value that is formed by applying certain linear transformations on a 'square' matrix. In other words, it is a function that maps a square matrix to a scalar value. This is the well-known definition of 'determinant'.

It was in the 1730s when Maclaurin wrote the 'Treatise of algebra,' (published much later, that is in 1748), contains the first published results on determinants proving Cramer's rule for 2x2 and 3x3 systems and indicating how the 4x4 case would work. Cramer gave the general rule for NxN systems in a paper 'Introduction to the analysis of algebraic curves' (1750). The rule appeared in an Appendix to the paper with no proof.

Since then, 'determinant' (though the term was coined by Gauss in 'Disquisitiones arthmeticae' in 1801) has been used for various purposes started from solving systems of equations to Cryptography in modern era.

In this, I would like to extend the concept of determinants to three dimensions and show its application in cryptography. Cryptography is more or less synonymous to encryption: the conversion of information from a readable state to apparent 'nonsense'. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.

By three dimensions, I would like to define determinants for cubic matrices.

Cubic Matrices

Cubic matrices are those that have equal number of rows, columns and depth elements.

Example of Cubic Matrices:

- A cubic matrix of order 2 can be written as

A=

For simplicity of typing, I would refer to this order 2 matrix as

a_{111}	a_{121}
a_{112}	a_{122}
a_{211}	a_{221}
a_{212}	a_{222}

- Similarly, a cubic matrix of order 3 can be written as

A=

For simplicity of typing, I would refer to this matrix as

a_{111}	a_{121}	a_{131}
a_{112}	a_{122}	a_{132}
a_{113}	a_{123}	a_{133}
a_{211}	a_{221}	a_{231}
a_{212}	a_{222}	a_{232}
a_{213}	a_{223}	a_{233}
a_{311}	a_{321}	a_{331}
a_{312}	a_{322}	a_{332}
a_{313}	a_{323}	a_{333}

henceforth. The 3D matrices will be represented in similar order.

Planes in a 3D Matrix

For the ease of computation and understanding, I would represent a 3D matrix in terms of 'Planes' representing a surface in the matrix. A plane of a 3D matrix can be represented at a 2D matrix. A 3D matrix can be represented in terms of 3 types of planes –

- Row plane
- Column plane
- Depth plane

I would be considering this matrix for this example:

$$
A = \begin{bmatrix}
\begin{matrix}
a_{111} & a_{121} & a_{131} \\
a_{112} & a_{122} & a_{132} \\
a_{113} & a_{123} & a_{133} \\
a_{211} & a_{221} & a_{231} \\
a_{212} & a_{222} & a_{232} \\
a_{213} & a_{223} & a_{233} \\
a_{311} & a_{321} & a_{331} \\
a_{312} & a_{322} & a_{332} \\
a_{313} & a_{323} & a_{333}
\end{matrix}
\end{bmatrix}
$$

Row Plane:

Row plane i of a 3D matrix of order n is defined as the plane containing the elements a_{xyi} where $x, y \in [1, n]$, i being constant.

For example, in the given 3D matrix,

- Row plane 1 =

$$
\begin{bmatrix}
a_{111} & a_{121} & a_{131} \\
a_{211} & a_{221} & a_{231} \\
a_{311} & a_{321} & a_{331}
\end{bmatrix}
$$

- Row plane 2=

$$\begin{bmatrix} a_{112} & a_{122} & a_{132} \\ a_{212} & a_{222} & a_{232} \\ a_{312} & a_{322} & a_{332} \end{bmatrix}$$

- Row plane 3=

$$\begin{bmatrix} a_{113} & a_{123} & a_{133} \\ a_{213} & a_{223} & a_{233} \\ a_{313} & a_{323} & a_{333} \end{bmatrix}$$

Hence, it can be seen that Row plane 1 of a 3D cubic matrix is the rear face of the matrix (as seen from the front) and row plane n is the front face (seen from front).

Column Plane:

Column plane i of a 3D matrix of order n is defined as the plane containing the elements a_{xiz} where $x, z \in [1, n]$, i being constant.

For example, in the given 3D matrix,

- Column plane 1 =

$$\begin{bmatrix} a_{111} & a_{112} & a_{113} \\ a_{211} & a_{212} & a_{213} \\ a_{311} & a_{312} & a_{313} \end{bmatrix}$$

- Column plane 2=

$$\begin{bmatrix} a_{121} & a_{122} & a_{123} \\ a_{221} & a_{222} & a_{223} \\ a_{321} & a_{322} & a_{323} \end{bmatrix}$$

- Column plane 3=

$$\begin{bmatrix} a_{131} & a_{132} & a_{133} \\ a_{231} & a_{232} & a_{233} \\ a_{331} & a_{332} & a_{333} \end{bmatrix}$$

Hence, it can be seen that Column plane 1 of a 3D cubic matrix is the left face of the matrix (as seen from the left) and column plane n is the right face (seen from left).

Depth Plane:

Depth plane i of a 3D matrix of order n is defined as the plane containing the elements a_{iyz} where $x, z \in [1, n]$, i being constant.

For example, in the given 3D matrix,

- Depth plane 1 =

$$\begin{bmatrix} a_{111} & a_{121} & a_{131} \\ a_{112} & a_{122} & a_{132} \\ a_{113} & a_{123} & a_{133} \end{bmatrix}$$

- Depth plane 2=

$$\begin{bmatrix} a_{211} & a_{221} & a_{231} \\ a_{212} & a_{222} & a_{232} \\ a_{213} & a_{223} & a_{233} \end{bmatrix}$$
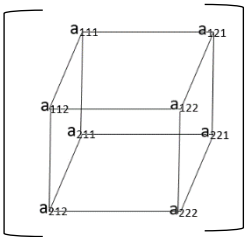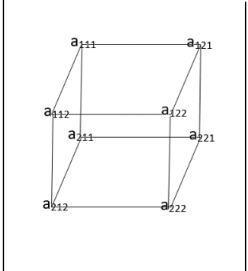
- Depth plane 3=

$$\begin{bmatrix} a_{311} & a_{321} & a_{331} \\ a_{312} & a_{322} & a_{332} \\ a_{313} & a_{323} & a_{333} \end{bmatrix}$$

Hence, it can be seen that Depth plane 1 of a 3D cubic matrix is the top face of the matrix (as seen from the top) and Depth plane n is the bottom face (seen from top).

Thus, a matrix of order n can be decomposed into 3n planes.

Determinant

To every cubic matrix A of order n and the elements $a_{ijk} \in R$, we can associate a real number to it, denoted by det A or $|A|$

If A= [cube diagram with vertices a_{111}, a_{121}, a_{112}, a_{122}, a_{211}, a_{221}, a_{212}, a_{222}]   then, det A = $|A|$ = [cube diagram with vertices a_{111}, a_{121}, a_{112}, a_{122}, a_{211}, a_{221}, a_{212}, a_{222}] $\in R$

Minors and Co-Factors of an Element

Minor of an a_{ijk} is represented as M_{ijk} and is defined as the value of the determinant of the remaining matrix after deleting
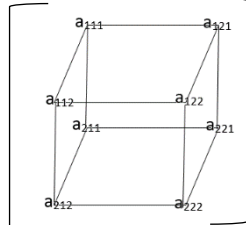
- Row plane k
- Column plane j
- Depth plane i

Co-factor of an element a_{ijk} is represented as A_{ijk} and is defined as

$A_{ijk} = (-1)^{i+j+k+1} * M_{ijk}$

Value of Determinant of a matrix A

- If the matrix is of Order 1, $|A|$ is the number itself.
- If the matrix is of Order 2, the determinant can be defined as:

Let A= [cube diagram with vertices a_{111}, a_{121}, a_{112}, a_{122}, a_{211}, a_{221}, a_{212}, a_{222}]

Det A = $|A|$ = $(a_{111} * a_{222}) + (a_{121} * a_{212}) - (a_{112} * a_{221}) - (a_{122} * a_{211})$

- If the matrix is of Order n, the determinant can be calculated by expanding it about a plane (Similar to Sarrus' scheme for 2D determinants).

Let A be a matrix of order n. Its determinant can be calculated by

Det A = $|A|$ = $\sum a_{ijk} * A_{ijk}$ where $a_{ijk} \in$ One plane.

Principal Diagonals of a 3D Matrix

A 3D matrix of order n contains 2 principal diagonals. The body diagonals from depth plane 1, row plane 1 to depth plane n, row plane n are the principal diagonals.

Thus, in the given Matrix of order 3, the principal diagonals are:

$a_{111} - a_{222} - a_{333}$ and $a_{131} - a_{222} - a_{313}$

Properties of Determinants

i. If each element in a plane of a determinant is 0, the value of the determinant is 0.

ii. If any two adjacent parallel planes in a determinant are interchanged, the value of the determinant turns negative.

Corollary: If any plane of a determinant is passed over m parallel planes, the resulting determinant is $(-1)^m$ times the original value.

iii. If two parallel planes are identical, the value of the determinant is 0.

iv. If each element in a plane is multiplied by a constant k, the value of the new determinant is k times that of the original value.

Corollary: If it is seen that in two parallel planes, the corresponding elements are proportional, then the value of determinant is 0.

v. If each element in a plane of a determinant consists of sum of two or more terms, the determinant can be expressed as the sum of two or more elements whose other planes parallel to the given one is not altered.

vi. If to each element of a plane of a determinant be added the equimultiples of the corresponding elements of one or more parallel planes, the value of the determinant remains unchanged.

vii. The sum of the products of elements of any plane with the cofactors of the corresponding elements of a parallel plane is even if all elements are integers.

Note: The proof of all the properties have been shown with matrices of order 2 or 3. It is equally valid for matrices of higher orders.

Proof of Properties

i.   Let us consider the given determinant:

$a_{111}= 0$	$a_{121}= 0$	$a_{131}= 0$
$a_{112}= 0$	$a_{122}= 0$	$a_{132}= 0$
$a_{113}= 0$	$a_{123}= 0$	$a_{133}= 0$
a_{211}	a_{221}	a_{231}
a_{212}	a_{222}	a_{232}
a_{213}	a_{223}	a_{233}
a_{311}	a_{321}	a_{331}
a_{312}	a_{322}	a_{332}
a_{313}	a_{323}	a_{333}

Expanding about depth plane 1, the value comes out to

$0*A_{111} + 0*A_{121} + 0*A_{131} + 0*A_{112} + 0*A_{122} + 0*A_{132} + 0*A_{113} + 0*A_{123} + 0*A_{133} = 0$. Hence, proved.

ii.   Let us consider the given determinant

A=

a	b
c	d
e	f
g	h

A= ah + bg – de – cf.

Interchanging the depth planes:

B=

e	f
g	h
a	b
c	d

B= ed + cf -ah -bg

Hence, A=-B, proved.

iii.   Let us consider the following determinant:

A=

a	b	c
d	e	f
g	h	i
j	k	l
m	n	o
p	q	r
j	k	l
m	n	o
p	q	r

After interchanging depth planes 2 and 3, the determinant still remains the same (using property ii.)

Hence, A=-A ➔ A=0.

iv.   Let us consider the following determinant:

A=

a	b
c	d
w	x
y	z

A=az + by – cx – dw

Multiplying depth plane 2 by constant k:

B=

a	b
c	d
kw	kx
ky	kz

B= kaz + kby – kdw – kcx = kA

Thus, B=kA, proved.

v.   Let us consider the following determinants:

A=

a	B
c	D
e + w	f + x
g + y	h + z

A= a (h + z) +b (g + y)-c (f + x)-d (e + w)

B=

a	b
c	d
e	f
g	h

B= ah + bg – de – cf.

C=

a	b
c	d
w	x
y	z

C= az + by – cx – dw

B+C= ah + bg – de – cf + az + by – cx – dw = a (h + z) +b (g + y)-c (f + x)-d (e + w) = A proved.

vi.   Property vi is a corollary of properties iii, iv and v together.

vii.   Let us consider the following determinant:

a	b	c
d	e	f
g	h	i
j	k	l
m	n	o
p	q	r
s	t	u
v	w	x
y	z	α

Multiplying elements of depth plane 1 with cofactors of depth plane 2

-a (eα + fz -hx -iw) +b (dα +fy -gx -vi) -c (dz +ey -gw -vh) +d (bα +cz -hu -it) − e (aα +cy -vg -is) +f (az +by -hs -gt) -g (bx + cw -eu -ft) +h (ax +cv -du -fs) −i (aw +bv -dt -es)

= 2(-aeα+bdα-cdz-iaw-bvi-cey+faz+bfy-cgw-gbx+hax+cvh-dvh-dit+evy+eis-hfs-fgt)

Thus, the result is even if the terms of the determinant are all integers.

Application in Cryptography

Using this algorithm, a nine-component data might be encrypted. A nine-component data is one which can be represented by nine or less real numbers. For example, a password with nine characters, the telephone numbers of nine friends and so on.

This algorithm involves the use of a public key, a private key (they both are 3x3 matrices), the nine-component data matrix (another 3x3 matrix) and generated a cipher matrix (3x3 again) and a real number one-time usable key. This One-time Key is dynamic and is purely based on the data to be encrypted. Thus, there is a different One-time key for different data.

The encryption algorithm

We would create a 3D matrix of order 3. The depth plane 1 is the public key matrix. The depth plane 2 is the cipher matrix and depth plane 3 is the private key matrix.

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9
x_1	x_2	x_3
x_4	x_5	x_6
x_7	x_8	x_9
b_1	b_2	b_3
b_4	b_5	b_6
b_7	b_8	b_9

In this generated matrix, the matrix containing the numbers a_1, a_2… a_9 is the public key matrix, the matrix containing the numbers b_1, b_2… b_9 is the private key matrix. The matrix containing the numbers x_1, x_2… x_9 is the matrix to be encrypted.

The cipher matrix, let it contain the elements k_1, k_2… k_9. It is generated by

- $k_1 = x_1/x_1$
- $k_2 = x_2/x_1$
- $k_3 = x_3/x_1$ and so on.

In short, each element of the matrix to be encrypted is divided by x_1 and written as corresponding elements in the cipher matrix.

The one-time key is generated by computing the determinant of this 3D matrix of order 3.

Hence, it is seen that the cipher matrix would contain the ratio of each number with x_1. Thus, it is quite obvious that k_1 would always be equal to 1. Thus, it is redundant to show that '1'. Hence, I decide to change the value of k_1 to $k_2 \oplus k_3 \oplus … \oplus k_8$. This would act as the parity checker and help to detect if there is an error in the transmission or if the data has been modified illicitly.
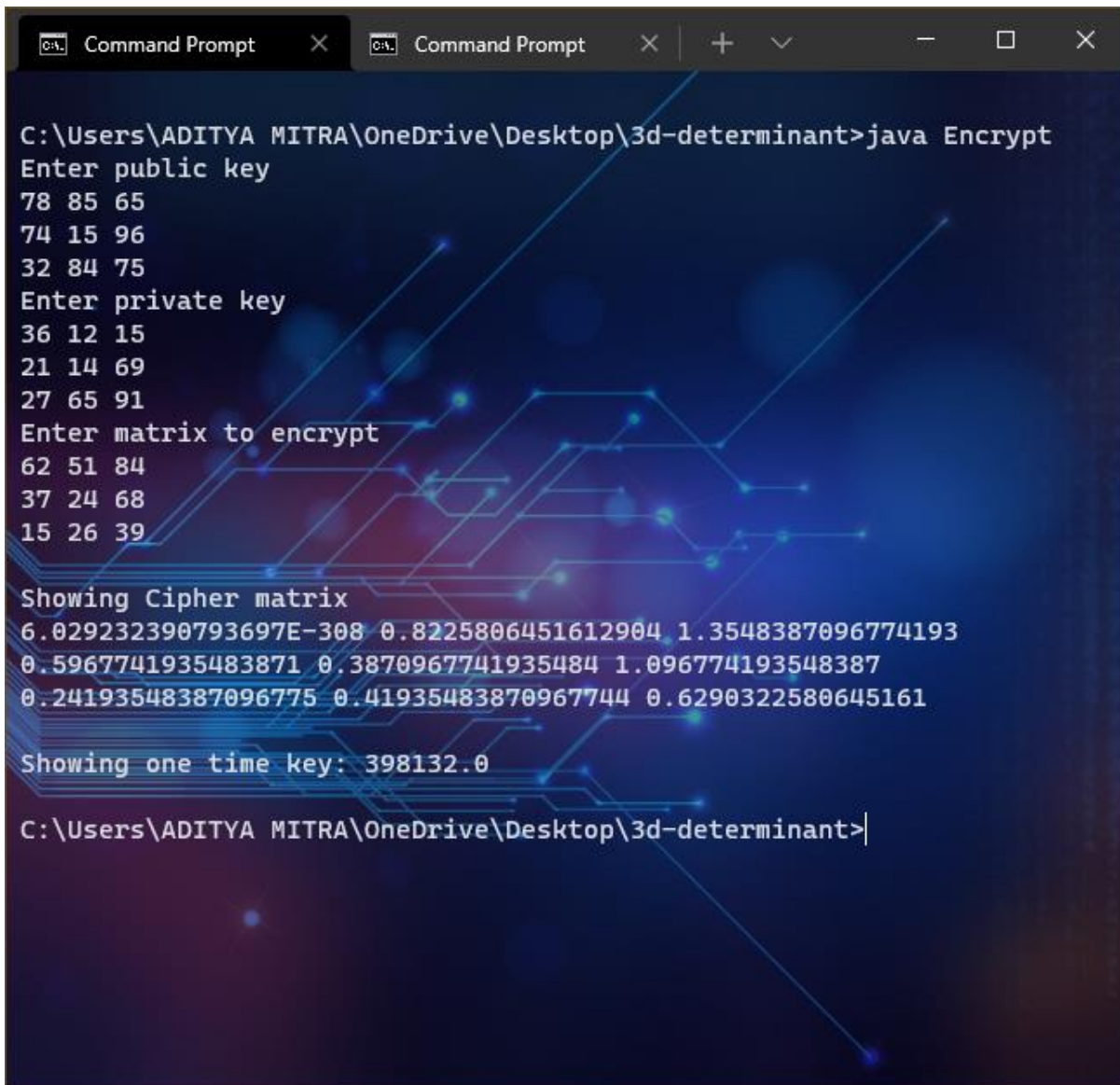
Even if an adversary gets to know the cipher matrix, he would only know the ratio between the numbers. And there is an infinitely long set of numbers having same ratio as in between them. Hence, it would be impossible for him to decrypt it.

The decryption algorithm

The decryption algorithm is nothing but reversing the encryption algorithm. The decryption algorithm would calculate the value of x_1 from the public key, the private key, the cipher matrix and the one-time key. Then, every element of the cipher matrix is multiplied with x_1 to get the clear matrix once again. The program will do this only after checking the parity element, k_1 of the cipher matrix.

Hence, it is seen that this cryptographic method is secure. There is nearly zero probability for any zero-knowledge attack on the cipher matrix to be successful. Even if the public key and the cipher matrix is known, there is nearly zero probability of generating the clear matrix without the private key and the one-time key both.
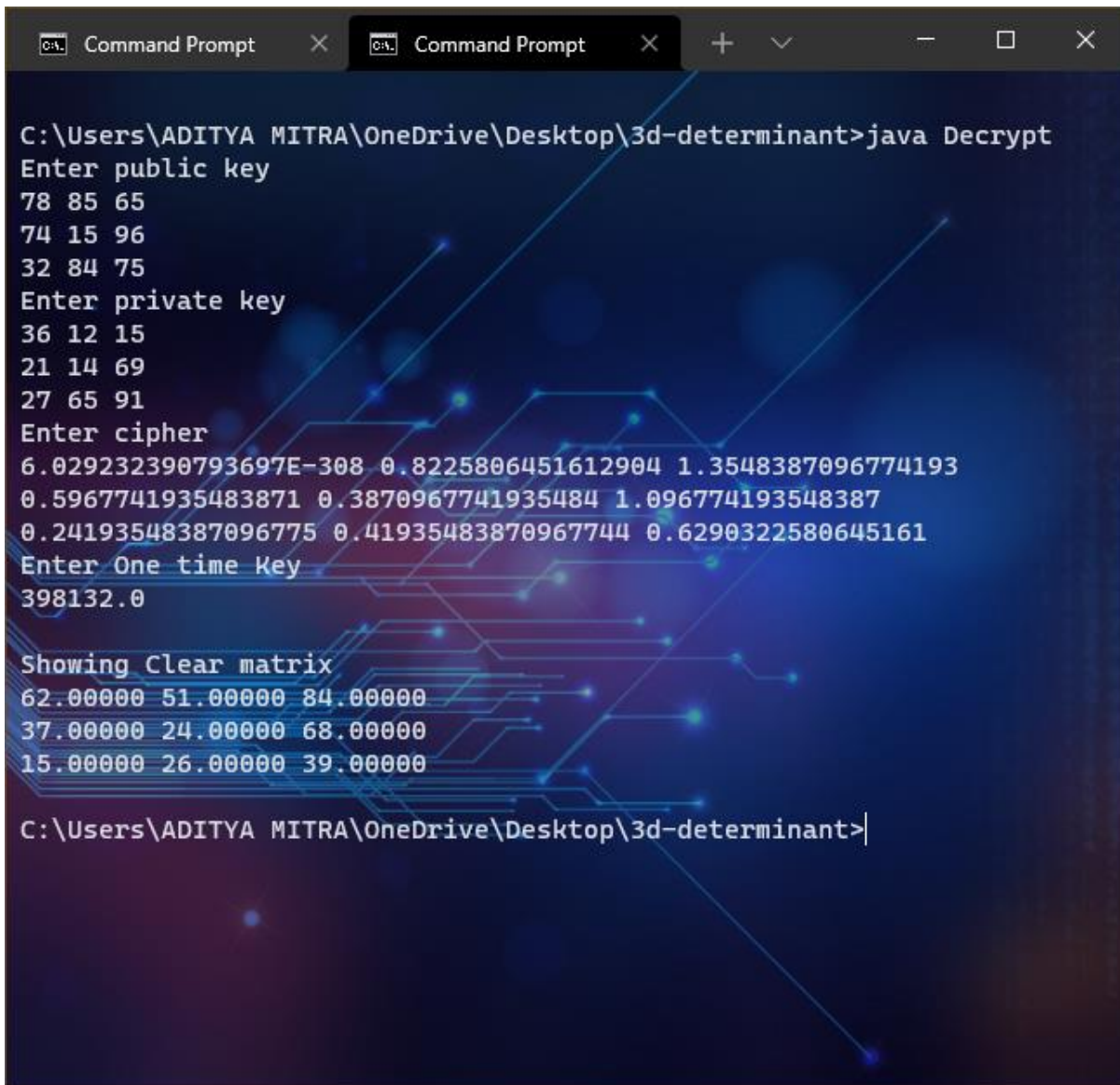
Screenshots showing Encryption


```
C:\Users\ADITYA MITRA\OneDrive\Desktop\3d-determinant>java Encrypt
Enter public key
78 85 65
74 15 96
32 84 75
Enter private key
36 12 15
21 14 69
27 65 91
Enter matrix to encrypt
62 51 84
37 24 68
15 26 39

Showing Cipher matrix
6.029232390793697E-308 0.8225806451612904 1.3548387096774193
0.5967741935483871 0.3870967741935484 1.096774193548387
0.24193548387096775 0.41935483870967744 0.6290322580645161

Showing one time key: 398132.0

C:\Users\ADITYA MITRA\OneDrive\Desktop\3d-determinant>
```

Screenshot showing Decryption


```
C:\Users\ADITYA MITRA\OneDrive\Desktop\3d-determinant>java Decrypt
Enter public key
78 85 65
74 15 96
32 84 75
Enter private key
36 12 15
21 14 69
27 65 91
Enter cipher
6.029232390793697E-308 0.8225806451612904 1.3548387096774193
0.5967741935483871 0.3870967741935484 1.096774193548387
0.24193548387096775 0.41935483870967744 0.6290322580645161
Enter One time Key
398132.0

Showing Clear matrix
62.00000 51.00000 84.00000
37.00000 24.00000 68.00000
15.00000 26.00000 39.00000

C:\Users\ADITYA MITRA\OneDrive\Desktop\3d-determinant>
```

Conclusion

A 3D determinant can be useful in various situations, especially in situations involving complicated calculations. Here, I have described an application of 3D determinant, that is in Cryptography. It is possible to encrypt 9 element matrices in this method and theoretically, it is very secure. In future, it might be possible to develop newer concepts in the fields of Mathematics, Data structures and Data computations based on 3D determinants.

References

- The program to demonstrate the encryption algorithm can be cloned from the GitHub repository: https://github.com/AdityaMitra5102/3d-determinant.git

Citations

The following resources have been used:

- https://mathshistory.st-andrews.ac.uk/HistTopics/Matrices_and_determinants/
- https://en.wikipedia.org/wiki/Determinant
- https://en.wikipedia.org/wiki/Cryptography