International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2024 Scholar AI LLC.
https://ijpsat.org/

Vol. 48 No. 2 January 2025, pp. 158-167

# *The Use Of Functions $f: D_1 \times D_2 \times D_3 \to \mathbb{R}^3$ For Encrypting And Decrypting Data In Space*

Azir Jusufi[1] Blinera Zekaj[2] Gazmend Xhaferi[3] Altin Jusufi[4]

[1,3] University of Tetova, Tetovo, North Macedonia

[2]Nettxio, Prishtina, Kosovo

[4]MIG-Skopje, North Macedonia

[1]azir.jusufi@unite.edu.mk; [2]blinera.zekaaj@gmail.com

[3]gazmend.xhaferi@unite.edu.mk; [4]altinjusufi2@gmail.com

**Abstract– Cryptology, due to its ancient use, can be considered an old science; however, given the rapid development it has undergone recently, it can also be viewed as a contemporary science. The study of cryptosystems is highly important, and there is valuable scientific research on the subject. Modern encryption systems are based on complex mathematical algorithms and implement a combination of symmetric and asymmetric key encryption schemes to ensure secure communication. Using the function $\mathbf{f}: \mathbf{D_1} \times \mathbf{D_2} \times \mathbf{D_3} \to \mathbb{R}^3$ for encrypting objects provides an effective and secure method to protect the privacy, security, and confidentiality of sensitive data, such as artworks or various sculptures.**

**The use of $\mathbf{f}: \mathbf{D_1} \times \mathbf{D_2} \times \mathbf{D_3} \to \mathbb{R}^3$ operates in three-dimensional space, encrypting objects in a way that makes it difficult for unauthorized individuals to decrypt their shape and structure. The application of encryption functions for 3D objects or forms can be utilized in industries such as virtual reality, engineering, and many other fields.**

**Keywords – Encryption, Decryption, Functions, Commutative Composite Functions, Objects, 3D Shapes.**

## 1..Introduction

Cryptography (from the Greek *kriptos* - secret, and *graphos* - writing) is the science that aims to conceal a message and transmit the hidden message to an authorized recipient, who can then revert it to its original state.[1] The transformation of the message, known as plaintext, into a concealed format referred to as ciphertext (or cryptogram) is achieved through the so-called encryption function, which enables the authorized recipient to convert the ciphertext back into plaintext. [1],[14],[15]. The entirety of these elements forms what is known as a cryptographic structure (abbreviated as cryptostructure or cryptosystem)[1], It is understood that the encryption process is carried out using an encryption algorithm.

The key is known to the sender and the authorized recipient, but not to those from whom the plaintext is concealed. The key and the ciphertext must uniquely determine the plaintext. The reconstruction of the plaintext from a given ciphertext is referred to as decryption and is accomplished through the so-called decryption function, which is defined by a decryption algorithm and the key kkk. For a given key, the decryption function is the inverse of the encryption function. The concepts described above can be summarized as follows:

**Definition 1.1** A cryptosystem is called a quintuplet (*P, C, K, E, D*) , where

- *P*- is a finite family of all plaintexts;
- *C*- is a finite family of all ciphertexts;
- *K*- is a finite family of all possible keys;
- *E* and D are sets of mappings from *P* to *C* and from *C* to *P*, respectively, such that for every çdo *k*∈*K*, there exists an encryption function $e_k \in E$ and a decryption function $d_k \in D$
- that satisfies $\forall x \in P\ , d_k\big(e_k(x)\big) = x.$

The use of encryption and decryption is as old as communication itself. Before computers, the security of encryption was ensured by exchanging encryption keys between the sender and the recipient, a process that often posed risks.

The first encryption was achieved using the substitution method based on a set of substitution rules. More complex ciphers operate with the help of powerful computer algorithms that reconstruct the bits into digital signals. In order to retrieve the content of the encrypted signal, we need the correct decryption key.[3][4][5]

In cryptography, a key is a variable value or a string of characters applied to an algorithm on a block or string of plaintext or ciphertext.

Cryptosystems are classified into two types: secret key cryptosystems and public key cryptosystems. The secret key cryptosystem is the oldest type of secret notation, where both the sender and the recipient share the same secret key.

In a public key cryptosystem, two keys are used: a public key known to everyone and a private or secret key known only to the recipient of the message. The public key and the secret key are related in such a way that the public key is used solely for encrypting messages, while the secret key is used exclusively for decrypting them. [1][6].

The purpose of this work is to explore and develop effective methods for using functions $f\colon D_1 \times D_2 \times D_3 \to \mathbb{R}^3$ for encrypting objects or 3D shapes in order to ensure the privacy, security, and confidentiality of sensitive data. The aim is to create secure and efficient algorithms that can be used in practical applications, improving the performance and results of the encryption of figures.

## 2.The use of functions $\boldsymbol{f\colon D_1 \times D_2 \times D_3 \to \mathbb{R}^3}$ for encrypting and decrypting data in space.

### 2.1 Knowledge about Functions

- Let A, B be two arbitrary sets. Every subset f of the Cartesian product A×B is called a *binary relation* from set A to set B. Thus, *f*⊆*AxB*.
- The relation $f$ from the non-empty set A to the non-empty set B is called a mapping or function from set A to set B if it has the property...

$$(\forall x \in A), (\exists!\, y \in B), \quad (x, y) \in f.$$

Functions are classified as follows:

- If *f* maps the set *A* to the set *B* and if $V_f$=*B*, then we say that *f* is a *surjective* function from the set *A* to the set *B*. The fact that $V_f$=*B* means, in other words, that the statement: $\forall y \in B, \exists x \in A, y = f(x)$ is true.
- For the function $f\colon A \to B$ we will say that it is an *injective* function if.

$$\forall x_1, x_2 \in A, \text{we have } f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

- The function *f*, which is both injective and surjective, is called a *bijective function* or bijection.
- ***Inverse function.*** Given a relation from *A* to *B*, for the function *f*, the inverse relation of it can be found

$$f^{-1} = \{(y, x) \in B \times A | y = f(x)\},$$

which may not be a function. If the inverse relation $f^{-1}$ is a function, it is called *the inverse function of f*. It is proven that the function $f$ has an inverse function $f^{-1}$ only when the function $f$ is bijective.

### 2.2 Knowledge about Linear Transformations

**Definition 2.2.1.** Let $L$ and $L'$ be vector spaces over the same field F with dimensions n and m, respectively. The function $f: L \to L'$ defined by $f(a_1, a_2, .., a_n)$=$(b_1, b_2, .., b_m)$, for any $(a_1, a_2, .., a_n) \in L$, is called a transformation of the space $L$ into the space $L'$

**Definition 2.2.2**. Let $L$ and $L'$ be vector spaces over the same field $F$. For the function

$f:L\to$L' we say it is linear or a linear transformation if:

a) $f(a + b) = f(a) + f(b)$ , for $\forall\ a,b\in L$ , and

b) $f(\lambda a) = \lambda f(a)$ , $\forall\ a\in L$ and $\forall\lambda \in F$.

Or, if we combine the conditions mentioned above, we obtain:

**Definition 2.2.3.** Let $L$ and $L'$ be vector spaces over the same field $F$. For the function

$f$: L→L' we say it is linear or a linear transformation if

$$f(\alpha a + \beta\, b) = \alpha f(a) + \beta f(b),\ \ \forall\ a,b\in L \text{ and } \forall\ \alpha,\beta \in F$$

**Statement 2.2.1.** Let $A$ be an arbitrary matrix of type $m$ x $n$ over the field $F$. The matrix $A$ defines a linear transformation $T: F^n \to F^m$, given by $\vec{v} \to A\vec{v}$, për $\forall\vec{v} \in F^n$.

$$For\ real, \forall\vec{v}, \vec{w} \in F^n,\ T(\vec{v} + \vec{w}) = A(\vec{v} + \vec{w}) = A\vec{v} + A\vec{w} = T(\vec{v}) + T(\vec{w})$$

$$\forall\vec{v} \in F^n,\ \forall k \in F,\quad T(k\vec{v}) = A(k\vec{v}) = kA\vec{v} = kT(\vec{v}).$$

**Example 2.2.1 .** Using a linear transformation $\mathbb{R}^3 \to \mathbb{R}^3$, given by the matrix T, the irregular pyramid ABCD with base vertices A(0,1,2), B(2,3,4), C(2,0,3) and apex D(3,4,6) should be encrypted.

$$T = \begin{bmatrix} 2 & -1 & 3 \\ -5 & 3 & 1 \\ -3 & 2 & 3 \end{bmatrix}.$$

**Solution**: Let the irregular pyramid ABCD be given , where A(0,1,2), B(2,3,4), C(2,0,3) and D (3,4,6)

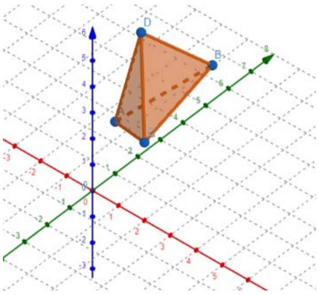


*Figure 1. The unencrypted pyramid ABCD*

From $TX_1 = X_2 \Rightarrow \begin{bmatrix} 2 & -1 & 3 \\ -5 & 3 & 1 \\ -3 & 2 & 3 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2x - y + 3z \\ -5x + 3y + z \\ -3x + 2y + 3z \end{bmatrix}$, we take:

- For the point A(0,1,2), we have $\begin{bmatrix} 2 & -1 & 3 \\ -5 & 3 & 1 \\ -3 & 2 & 3 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 5 \\ 8 \end{bmatrix}$, thus A'(5,5,8);
- For the point B(2,3,4), we have $\begin{bmatrix} 2 & -1 & 3 \\ -5 & 3 & 1 \\ -3 & 2 & 3 \end{bmatrix}\begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 13 \\ 3 \\ 12 \end{bmatrix}$, thus B'(13,3,12);
- For the point C(2,0,3), we have $\begin{bmatrix} 2 & -1 & 3 \\ -5 & 3 & 1 \\ -3 & 2 & 3 \end{bmatrix}\begin{bmatrix} 2 \\ 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 13 \\ -7 \\ 3 \end{bmatrix}$, thus C'(13,-7,3);
- For the point D(1,1,6), we have $\begin{bmatrix} 2 & -1 & 3 \\ -5 & 3 & 1 \\ -3 & 2 & 3 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 6 \end{bmatrix} = \begin{bmatrix} 19 \\ 4 \\ 17 \end{bmatrix}$, thus D'(19,4,17).

We obtain the encrypted body A'B'C'D':

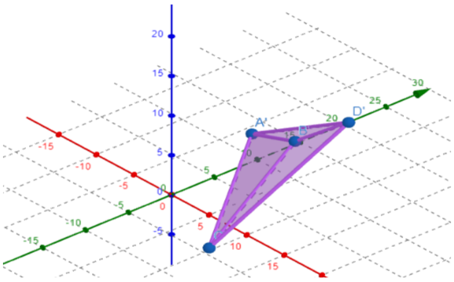


*Figure 2. The encrypted pyramid A'B'C'D'*

**Note**: In fact, in example 2.2.1, we have a linear transformation of bodies, which in most cases does not change the type or shape.

- Next, we will examine a special type of mapping functions $F: D_f \times D_g \times D_h \to \mathbb{R}^3$ given by $F(x, y, z) = (f(x), g(y), h(z))$,for all $\forall(x, y, z) \in D_f \times D_g \times D_h$, where $D_f, D_g, D_h \subseteq \mathbb{R}$. The functions $f: D_f \to \mathbb{R}$ , $g: D_g \to \mathbb{R}$ and $h: D_h \to \mathbb{R}$ re bijective functions, hence there exist corresponding inverse functions $f^{-1}(x)$, $g^{-1}(y)$ and $h^{-1}(z)$ Thus, we can form the inverse of F(x,y,z), which is given by $F^{-1}(x, y, z) = (f^{-1}(x), g^{-1}(y), h^{-1}(z))$.

We will use the transformation function $F(x, y, z) = (f(x), g(y), h(z))$, as the encryption key for bodies in space, while the decryption key will be the inverse function $F^{-1}(x, y, z) = (f^{-1}(x), g^{-1}(y), h^{-1}(z))$, of the transformation function $F(x, y, z) = (f(x), g(y), h(z))$.

**Encryption Procedure:**

1. We place the body that we want to encrypt in a coordinate system Oxyz.
2. We identify several characteristic points $P_i(x_i, y_{i,} z_i)$, i=1,2,…,n, in the object.
3. As an encryption key, we use a mapping function )$F(x, y, z) = (f(x), g(y), h(z))$, where

   $(x_i, y_i, z_i)$, - represent the points of the unencrypted body *T*, while the values $(f(x_i), g(y_{i)}, h(z_i))$, represent the points of the encrypted body *T*k.

**Example 2.2.2** Encrypt the irregular pyramid with verticesA(1,2,3), B(6,4,1), C(3,6,2), D(5;1;0,1), E(5,2,5) with the help of the key function $F(x,y,z) = (\frac{2x-1}{4}, 2^y, 2\ logz)$.

**Solution**. Let the irregular pyramid be given with base ABCD and vertex E, with coordinates A(1,2,3), B(6,4,1), C(3,6,2), D(5;1;0,1), E(5,2,5).

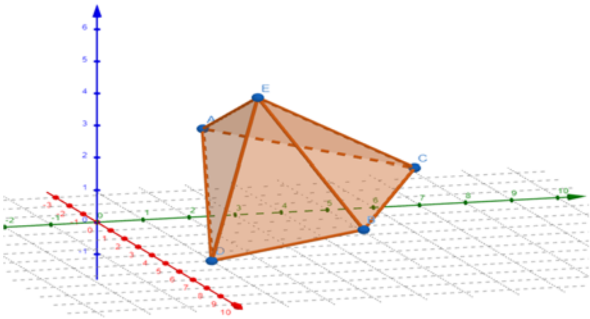


*Figure 3. The irregular pyramid ABCDE - unencrypted*

With the help of the key function $F(x,y,z) = (\frac{2x-1}{4}, 2^y, 2\ logz)$ we encrypt the vertices and obtain:

- For $A(1,2,3)$ we have $F(1,2,3) = (\frac{2\cdot1-1}{4}, 2^2, 2log3)$=$\left(\frac{1}{4}; 4; 0{,}954\right)$, thus $A^`\left(\frac{1}{4}; 4; 0{,}954\right)$;
- For $B(6,4,1)$ we have $F(6,4,1) = (\frac{2\cdot6-1}{4}, 2^4, 2log1)$=$\left(\frac{11}{4}; 16; 0\right)$, thus $B^`\left(\frac{11}{4}; 16; 0\right)$;
- For $C(3,6,2)$ we have $F(3,6,2) = (\frac{2\cdot3-1}{4}, 2^6, 2log2)$=$\left(\frac{5}{4}; 64; 0{,}6\right)$, thus $C^`\left(\frac{5}{4}; 64; 0{,}6\right)$;
- For $D(5;1;0,1)$ we have $F(5;1;0{,}1) = (\frac{2\cdot5-1}{4}, 2^1, 2log0{,}1)$=$\left(\frac{9}{4}; 2; -2\right)$, thus $D^`\left(\frac{9}{4}; 2; -2\right)$;
- For $E(5;2;5)$ we have $F(5;2;5) = (\frac{2\cdot5-1}{4}, 2^2, 2log5)$=$\left(\frac{9}{4}; 4; 1{,}4\right)$, thus $E^`\left(\frac{9}{4}; 4; 1{,}4\right)$.

We obtained the encrypted body A` B` C` D` E` this way

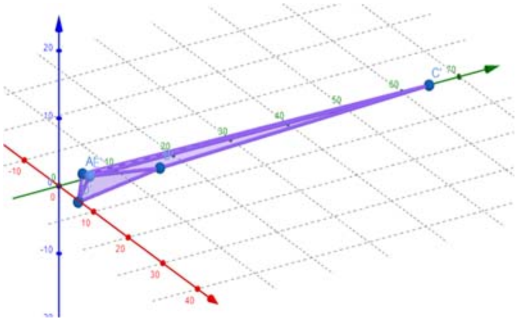


*Figure 4. The encrypted body A' B' C' D' E'*

**Decryption Procedure:**

1. We take the characteristic points $P_i(x_i, y_i, z_i)$, i=1,2,…,n, of the encrypted body

2. As the decryption key, we use the inverse function of the transformation function $F(x,y,z)=(f(x),g(y),h(z))$, namely $F^{-1}(x,y,z)=(f^{-1}(x),g^{-1}(y),h^{-1}(z))$, where $(x_i,y_i,z_i)$, - represent the encrypted points of the body *T*$_k$, while the triples $(f^{-1}(x_i),g^{-1}(y_{i),}h^{-1}(z_i))$, represent the points of the decrypted body *T*.

3.

**Example 2.2.3.** Decrypt the body A' B' C' D' E' given the encrypted vertices $A'\left(\frac{1}{4};4;0{,}954\right)$; $B'\left(\frac{11}{4};16;0\right)$;$C'\left(\frac{5}{4};64;0{,}6\right)$; $D'\left(\frac{9}{4};2;-2\right)$; $E'\left(\frac{9}{4};4;1{,}4\right)$ , as well as the key function for transformation $F(x,y,z)=\left(\frac{2x-1}{4},2^y,2\,logz\right)$.

**Solution.** Let the encrypted body A' B' C' D' E' be given with the encrypted vertices $A'\left(\frac{1}{4};4;0{,}954\right)$; $B'\left(\frac{11}{4};16;0\right)$;$C'\left(\frac{5}{4};64;0{,}6\right)$; $D'\left(\frac{9}{4};2;-2\right)$; $E'\left(\frac{9}{4};4;1{,}4\right)$, so:

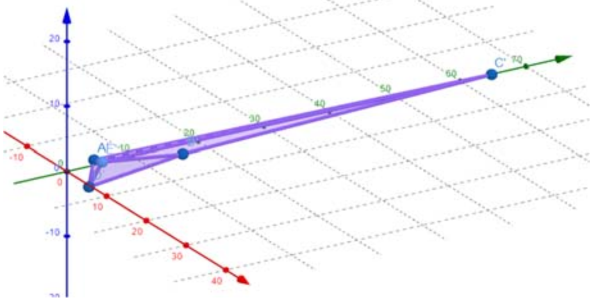


*Figure 5. The Encrypted Body A' B' C' D' E'*

- First, we find the inverse function$F^{-1}(x,y,z)$, which is the decryption key given by:

From $F(x,y,z)=(f(x),g(y),h(z))=\left(\frac{2x-1}{4},2^y,2\,logz\right)$ we obtain that:

$$f(x)=\frac{2x-1}{4}\Rightarrow f^{-1}(x)=\frac{4x+1}{2}$$

$$g(y)=2^y\Rightarrow g^{-1}(y)=log_2y$$

$$h(z)=2logz\Rightarrow h^{-1}(z)=10^{\frac{z}{2}}$$

Therefore, the inverse function $F^{-1}(x,y,z)$ is given by $F^{-1}(x,y,z)=(\frac{4x+1}{2},log_2y,10^{\frac{z}{2}})$.

With the help of the decryption key function $F^{-1}(x,y,z)=(\frac{4x+1}{2},log_2y,10^{\frac{z}{2}})$ we decrypt the vertices A', B,' C', D', E'and obtain:

- For $A'\left(\frac{1}{4};4;0{,}954\right)$ we have $F^{-1}\left(\frac{1}{4};4;0{,}954\right)=\left(\frac{4\cdot\frac{1}{4}+1}{2},log_24,10^{\frac{0{,}954}{2}}\right)=(1{,}2{,}3)$ , thus A(1,2,3);
- For $B'\left(\frac{11}{4};16;0\right)$ we have $F^{-1}\left(\frac{11}{4};16;0\right)=\left(\frac{4\cdot\frac{11}{4}+1}{2},log_216,10^{\frac{0}{2}}\right)=(6{,}4{,}1)$, thus B(1,2,3);
- For $C'\left(\frac{5}{4};64;0{,}6\right)$ we have $F^{-1}\left(\frac{5}{4};64;0{,}6\right)=\left(\frac{4\cdot\frac{5}{4}+1}{2},log_264,10^{\frac{0{,}6}{2}}\right)=(3{,}6{,}2)$, thus C(3,6,2);

- For $D^{'}\left(\frac{9}{4}; 2; -2\right)$ we have $F^{-1}\left(\frac{9}{4}; 2; -2\right) = \left(\frac{4\cdot\frac{9}{4}+1}{2}, log_2 2, 10^{\frac{-2}{2}}\right) = (5; 1; 0{,}1)$, thus D$(5; 1; 0{,}1)$;

- For $E^{'}\left(\frac{9}{4}; 4; 1{,}4\right)$, we have $F^{-1}\left(\frac{9}{4}; 4; 1{,}4\right) = \left(\frac{4\cdot\frac{9}{4}+1}{2}, log_2 4, 10^{\frac{1{,}4}{2}}\right) = (5; 2; 5)$, thus E$(5; 2; 5)$.

We obtain the decrypted body ABCDE.

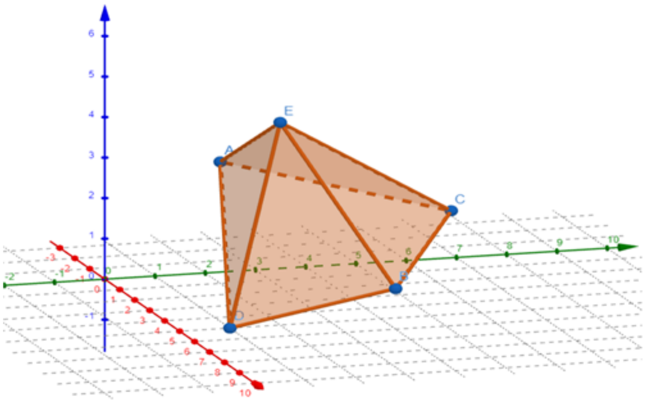


*Figure 6. The decrypted body ABCDE*

## 3. Program Implementation and Results

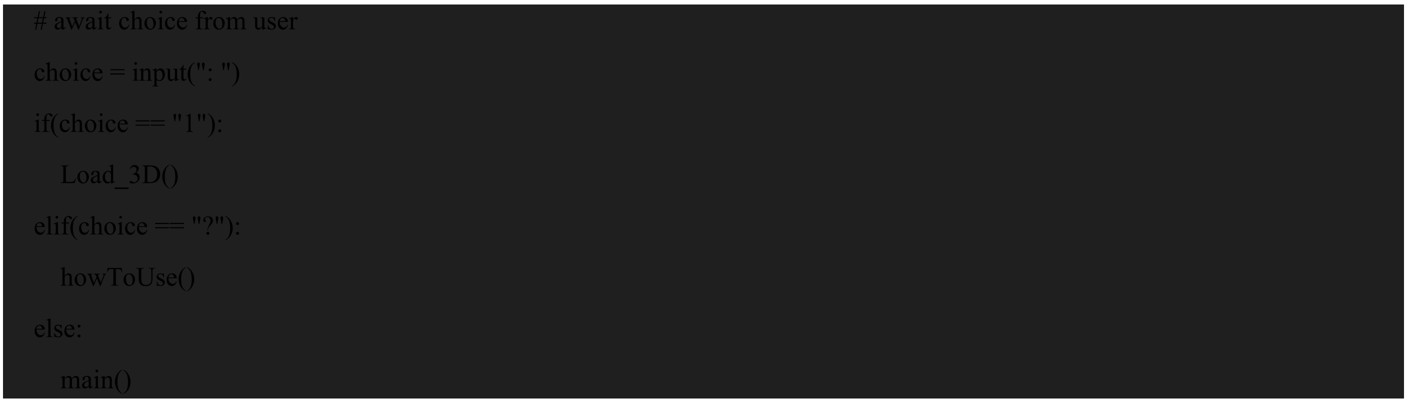
### 3.1. Implementation

This program, created in Python, utilizes various libraries to develop an interface for encrypting and decrypting 3D coordinates. The program is structured into several functions that allow the user to input options and view different visualizations of the encrypted and decrypted shapes.

To use this program, you can follow these steps:

- After the program is executed, you will see the 3D option. Press 1 for 3D.

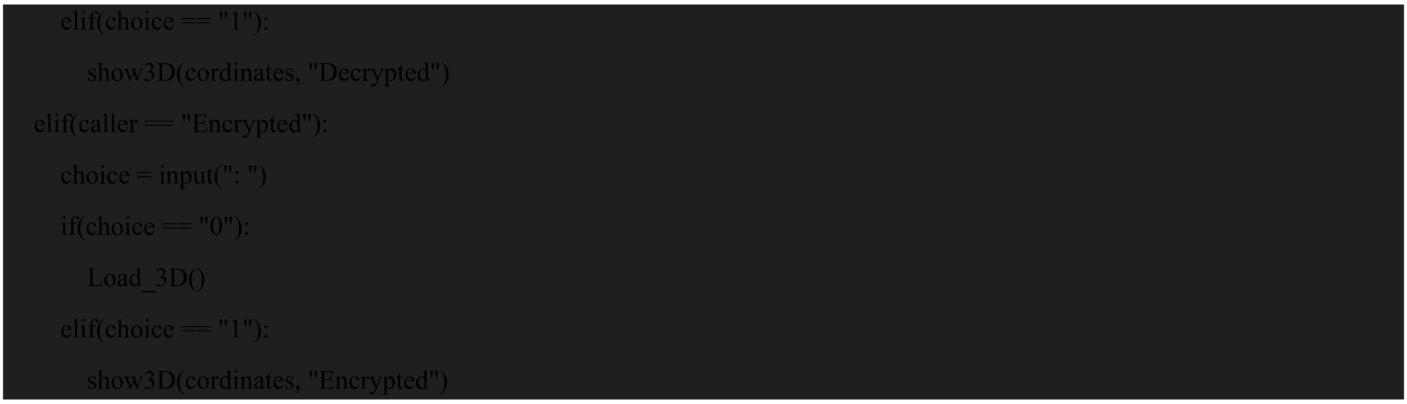
You can also use the option **"?"** to read how to use the program and how to enter the necessary data for the coordinates and functions



```
# await choice from user
choice = input(": ")
if(choice == "1"):
    Load_3D()
elif(choice == "?"):
    howToUse()
else:
    main()
```

*Figure 7. Selection of the Option for Executing the Program*

```
def show3D(cordinates, caller = ""):
    # all possible combinations of the cordinates that create an edge
    edges = list(combinations(cordinates, 2))
    fig = plt.figure()
    ax = fig.add_subplot(111, projection='3d')
    # connect every possible edge
    for edge in edges:
        x = [edge[0][0], edge[1][0]]
        y = [edge[0][1], edge[1][1]]
        z = [edge[0][2], edge[1][2]]
        # connect the vertexes
        ax.plot(x, y, z, c='#3f97d1')
        # place the vertexes on the 3D Plane
        ax.scatter(x, y, z, c='b', marker='o')
    # show the cordinates (x, y, z) of every vertex with text
    for i, vertex in enumerate(cordinates):
        ax.text(vertex[0], vertex[1], vertex[2], f'({vertex[0]}, {vertex[1]}, {vertex[2]})', fontsize=8)
    # text that will be on the axis
    ax.set_xlabel('X')
    ax.set_ylabel('Y')
    ax.set_zlabel('Z')
    # see which funciton called this function / either "Decrypted Shape" or "Encrypted Shape"
    plt.title(f"{caller} Shape")
    # adjust the top parameter so the 3D view looks bigger on screen
    plt.subplots_adjust(top=1.0)
    # show the plot
    plt.show()
    # see from which function this function was called and act accordingly
    if(caller == "Decrypted"):
        choice = input(": ")
        if(choice == "0"):
            Load_3D()
```



```
        elif(choice == "1"):
            show3D(cordinates, "Decrypted")
    elif(caller == "Encrypted"):
        choice = input(": ")
        if(choice == "0"):
            Load_3D()
        elif(choice == "1"):
            show3D(cordinates, "Encrypted")
```

*Figure 8. Function for Visualizing 3D Figures*

- **Encryption and Decryption:**

After selecting the dimension, the program will ask you to choose between encryption and decryption. If you select encryption, you will be prompted to provide the coordinates and functions for each dimension. If you decide on decryption, you will be asked to give each dimension's encrypted coordinates and functions.

## 4.Conclusions

In this paper, we aimed to present a new and interesting application of functions $F: D_f \times D_g \times D_h \to \mathbb{R}^3$. This cryptosystem is easy to use. After a theoretical treatment of the problem, we also attempted to concretize it with examples. Additionally, we have implemented this cryptosystem programmatically. In the aforementioned examples, we used simple key functions to ensure the work is easily understandable. As the complexity of the key functions increases, breaking this cryptosystem also becomes more difficult.

## REFERENCES

[1] Azir Jusufi Kristaq Filipi, Matematikë Diskrete dhe Aplikime, Prishtine, 2022

[2] https://tresorit.com/blog/the-history-of-encryption-the-roots-of-modern-day-cyber-security/

[3] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In23rd Annual ACM Symposium on Theory of Computing,1991.

[4] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography, 1998.

[5] C. Dwork, M. Naor. Method for message authentication from non-malleable cryptosystems, 1996.

[6] I. Damgard. Towards practical public key cryptosystems secure againstchosen ciphertext attacks. In Advances in Cryptology.

[7] K. Filipi, A. Jusufi, Xh. Beqiri, Matematika për ekonomistë, Tetovë, 2012

[8] Discrete Math, Mohamed Jamaloodeen, Kathy Pinzon, Daniel Pragel, Joshua Roberts, Sebastien Siva

[9] Mathematical Foundations and Aspects of Discrete Mathematics, Jean Gallier and Jocelyn Quaintance, March 2022

[10] Discrete Mathematics an Open Introduction, Oscar Levin, July 2021

[11] Discrete Maths in Computer Science, Gary Haggard, John Schlipf, Sue Whitesides

[12] A. Jusufi, D, Berisha, M, Reqica, P;rmbledhje detyrash nga matematika diskrete, Prishtine, 2022

[13] F. Kabashi, A. Jusufi, USE OF COMPOSITE COMMUTATION FUNCTIONS IN DETERMINING THE DIFFIE-HELLMAN KEYS, PROCEEDINGS OF THE 7TH ANNUAL INTERNATIONAL CONF-UBT, 2018

[14] B. Zekaj, A. Jusufi, B. Imeri-Jusufi, Using incomplete polynomial functions of the odd degree n and their inverses for data encryption and decryption, IFAC-PapersOnLine, Volume 55, Issue 39, 2022, Pages 241-246

[15] Mirlinda Reqica, Diellza Berisha, Azir Jusufi, Meriton Reqica, Exploitation of exponential and logarithmic functions for data encryption and decryption, IFAC-PapersOnLine, Volume 55, Issue 39, 2022, Pages 286-291