Using the Connected Components of Topological Spaces in Cryptography

Abedal-Hamza Mahdi Hamza [#1], Saba Nazar Faisel Al-khafaji [*2]

Department of Mathematics Faculty of Computer Science and Mathematics , University of Kufa, IRQ.

***Abstract*— In this paper, we gave a technique for cryptography. This technique depends on the connected components of a topological space.We chose a basis for a topology such that the elements of this basis are the components of that topological space.**

***Keywords*— topological space, connected components, basis, cryptography.**

I. INTRODUCTION

Cryptography is the study of methods for sending messages in secret (encrypted form) so that only the intended recipient can remove the encryption and read the message [4]. Cryptography comes from the Greek root words kryptos, meaning hidden, and graphikos, meaning to write. The word cryptic(hidden), appears in 1638, while crypto- as a prefix for concealed or secret makes its appearance in 1760. The term cryptogram appears much later, first occurring in 1880 [2].

The earliest documented use of ciphers was in the Roman army under Julius Caesar around 60 B.C.. This was a simple substitution cipher where each letter in plaintext is replaced by some other letter. The Caesar cipher is a special case of the Shift Cipher [4].

The original message is called the plaintext, and the decrypted message is called the ciphertext.. Both the plaintext and the ciphertext are written in terms of elements from a finite set A, called an alphabet of definition . The alphabet may consist of numbers, letters from an alphabet such as the English, Greek, or symbols such as !, @, *, or any other symbols .The alphabet of for the plaintext and ciphertext may differ, but the usual convention is to use the same [2].
To make cryptanalysis more difficult, we need a set of parameters K, called the keyspace, whose elements are called keys [4].

If the encryption and decryption keys are the same (or mathematically derivable from each other), then the algorithm is called symmetric**.**If the key used for encryption is different from the key used for decryption, then the algorithm is called asymmetric [2].

The modern scientific study of cryptography is sometimes referred to as cryptology [2].

II. FUNDAMENTAL CONCEPTS

2.1 Definition [1]

Let X be a topological space:

(i) X is called connected if there does not exist a pair of disjoint non-empty open sets whose union is X.

(ii) X is called disconnected if X is not connected.

(iii) If X is disconnected, then a pair of disjoint non-empty open sets whose union is X is called a separation of X.

2.2 Definition [3]

A set A contained in a topological space X is said to be connected in X if A is connected in the subspace topology. If A is not connected in X, we say it is disconnected.

2.3 Definition [3]

A component $\mathcal{F}$ of a topological space X is a maximal connected subset of X; that is $\mathcal{F}$ connected and $\mathcal{F}$ is not a proper subset of any other connected subset of X.

2.4 Example

Consider the following topology $\mathcal{T}$ on the set

$$X = \{a, b, c, d, e\}$$
$$\mathcal{T} = \{X, \emptyset, \{a\}, \{c, d\}, \{a, c, d\}, \{b, c, d, e\}\}.$$

The components of X are $\{a\}$ and $\{b, c, d, e\}$. Note that $\{c, d\}$ is connected but it is not a component for $\{c, d\} \subset \{b, c, d, e\}$.

2.5 Theorem [3]

A topological space $(X, \mathcal{T})$ is a connected space if, and only if, X has exactly one component.

2.6 Theorem [3]

The components of X are connected disjoint subspaces of X whose union is X, such that each non-empty connected subspace of X intersects only one of them.

III. APPLICATION(CRYPTOGRAPHY)

Let M be a message. Take a finite topological space X such that a number of elements depends on the number of character of a message that we need to encode. We can encrypt the entire message or deducting parts and encrypt them on alone and in both cases the number of elements of this set depends on the number of characters taken from the message.We choose X such that its components form a basis for its

topology.Each component has the same number which is the number of letters.

We choose a finite set A of different numbers. Then we assigned a number of A for each letter of the message M.We send this number to a fixed vector of a set of vectors Y. This fixed vector is sent to a component of X.

Finally, we used a linear transformation

$h: \mathbb{R}^n \longrightarrow \mathbb{R}^n$,

$h(u) = Bu$

where B is a nonsingular matrix whose columns are the components of X.

M	m_1	m_2		m_n
A	1	2	....	n
	↕	↕		↕
Y	y_1	y_2		y_n
	↕	↕		↕
V	$v(1)$	$v(2)$	....	$v(n)$
	↕	↕		↕
C	c_1	c_2	....	c_n

Fig.1 Encryption and decryption processes

IV. SOME NOTATIONS

(1) Message space : a set of strings (plain text messages) over some alphabet that needs to be encrypted.

(2) A : set of different numbers. We assigned a number for each letter of the message where
$|M| = |A| = |Y| = |V| = |C| = n$
$|X| = n^2$.

(3) X : Topological space with a basis $\mathcal{T}_{\mathcal{B}}$.

(4) Y : transform the message to the vector of firm number.

(5) V : this vector transform to the component of X.

(6) C : denotes a vector called the cipher vector.

V. THE ENECRYPTION PROCESS(ALGORITHM)

$\mathbb{R} \xrightarrow{g} \mathbb{R}^n \xrightarrow{f} \mathbb{R}^n \xrightarrow{h} \mathbb{R}^n$

$(A \longmapsto Y \longmapsto V \longmapsto C)$

$(h\ o\ f\ o\ g): \mathbb{R} \longrightarrow \mathbb{R}^n$

$(h\ o\ f\ o\ g)$ is one-to-one transformation from A onto C.

$(h\ o\ f\ o\ g)(x_i) = h\left(f(g(x_i))\right)$

$= h(f(y_i))$

$= h(v(i))$

$= B\ v(i) = c_i$

VI. THE DECRYPTION PROCESS(ALGORITHM)

$(h\ o\ f o\ g)^{-1}: \mathbb{R}^n \longrightarrow \mathbb{R}$

$(C \longmapsto V \longmapsto Y \longmapsto A)$

$(h\ o\ f o\ g)^{-1}$ is one-to-one transformation from C onto A.

$(h\ o\ f o\ g)^{-1}(c_i) = (g^{-1} o f^{-1} h^{-1})(c_i)$

$= g^{-1}(f^{-1}(h^{-1}(c_i)))$

$= g^{-1}(f^{-1}(B^{-1}(c_i)))$

$= g^{-1}(f^{-1}(v(i)))$

$= g^{-1}(y_i)$

$= x_i$

VII. EXAMPLE

The encryption of the message "come":

Let $X = \{1, 2, 3, 4, 5, 6, 7, -8, 9, 10, 11, -12, 13, 14, 15, -16\}$.

$|X| = n^2$, $n = 4$.

$\mathcal{T}_{\mathcal{B}} =$

$\{\{1, 5, 6, 7\}, \{2, -8, 9, 10\}, \{3, 11, -12, 13\}, \{4, 14, 15, -16\}\}$.

M : m_i C o m e

A : a_i 1 2 3 4

Y : y_i $\begin{bmatrix}1\\1\\1\\1\end{bmatrix}\begin{bmatrix}2\\2\\2\\2\end{bmatrix}\begin{bmatrix}3\\3\\3\\3\end{bmatrix}\begin{bmatrix}4\\4\\4\\4\end{bmatrix}$

V : v_i $\begin{bmatrix}1\\5\\6\\7\end{bmatrix}\quad\begin{bmatrix}2\\-8\\9\\10\end{bmatrix}\quad\begin{bmatrix}3\\11\\-12\\13\end{bmatrix}\quad\begin{bmatrix}4\\14\\15\\-16\end{bmatrix}$,

$h: \mathbb{R}^4 \longrightarrow \mathbb{R}^4$

h is a one-to-one transformation from V onto C.

$h(u) = Bu$

$$B = \begin{bmatrix}1 & 2 & 3 & 4\\5 & -8 & 11 & 14\\6 & 9 & -12 & 15\\7 & 10 & 13 & -16\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3 & 4\\5 & -8 & 11 & 14\\6 & 9 & -12 & 15\\7 & 10 & 13 & -16\end{bmatrix}\begin{bmatrix}1\\5\\6\\7\end{bmatrix} = \begin{bmatrix}57\\129\\84\\23\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3 & 4\\5 & -8 & 11 & 14\\6 & 9 & -12 & 15\\7 & 10 & 13 & -16\end{bmatrix}\begin{bmatrix}2\\-8\\9\\10\end{bmatrix} = \begin{bmatrix}53\\313\\-18\\-109\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3 & 4\\5 & -8 & 11 & 14\\6 & 9 & -12 & 15\\7 & 10 & 13 & -16\end{bmatrix}\begin{bmatrix}3\\11\\-12\\13\end{bmatrix} = \begin{bmatrix}41\\-23\\456\\-233\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3 & 4\\5 & -8 & 11 & 14\\6 & 9 & -12 & 15\\7 & 10 & 13 & -16\end{bmatrix}\begin{bmatrix}4\\14\\15\\-16\end{bmatrix} = \begin{bmatrix}13\\-151\\-270\\619\end{bmatrix}$$

Now can we sent the vectors the encrypted:

$\begin{bmatrix}57\\129\\84\\23\end{bmatrix}, \begin{bmatrix}53\\313\\-18\\-109\end{bmatrix}, \begin{bmatrix}41\\-23\\456\\-233\end{bmatrix}, and \begin{bmatrix}13\\-151\\-270\\619\end{bmatrix}.$

Suppose now that we receives the massage from reporter

$c_i = \begin{bmatrix}57\\129\\84\\23\end{bmatrix}, \begin{bmatrix}53\\313\\-18\\-109\end{bmatrix}, \begin{bmatrix}41\\-23\\456\\-233\end{bmatrix} and \begin{bmatrix}13\\-151\\-270\\619\end{bmatrix}$ where

$i = 1,2,3,4$

By decryption process solves the equation

$(h\ o\ fo\ g)^{-1}: \mathbb{R}^4 \longrightarrow \mathbb{R}$ (it is a one-to-one transformation from C onto A).

$(C \mapsto V \mapsto Y \mapsto A)$

$(h\ o\ fo\ g)^{-1}(c_i) = (g^{-1}of^{-1}h^{-1})(c_1)$

$= g^{-1}(f^{-1}(h^{-1}(c_1))) = g^{-1}(f^{-1}(B^{-1}(c_1)))$

$=$

$$g^{-1}(f^{-1}(\begin{bmatrix}-0.3058 & 0.0848 & 0.0714 & 0.0647\\0.2076 & -0.0580 & 0.0060 & 0.0067\\0.1451 & 0.0045 & -0.0357 & 0.0067\\0.1138 & 0.0045 & 0.0060 & -0.0246\end{bmatrix}\begin{bmatrix}57\\129\\84\\23\end{bmatrix})$$

$$= g^{-1}(f^{-1}\left(\begin{bmatrix}1\\5\\6\\7\end{bmatrix}\right))$$

$$g^{-1}\left(\begin{bmatrix}1\\1\\1\\1\end{bmatrix}\right) = C$$

Similarly

We has received the following message:

Come

VIII. CONCLUSION

We used a basis for a topological space and a linear transformation to encrypt a message. This method for cryptography was a new proposed method.

REFERENCES

[1] Adams C., and Franzosa R., *Introduction to Topology Pure and Applied*, Person Printice Hall, 2008.

[2] Hoffstein J., Pipher J.,& Silverman J.H., *An Introduction to mathematical Cryptography*, Springer, 2008.

[3] Munkres J. R., *Topology*, 2nd ed., New Delhi-110001, PHI,2009.

[4] Rosen K. H., *An Introduction to Cryptography*, 2nd ed., by Taylor & Francis Group, LLC, 2008.