Journal of mathematics and computer science 11 (2014), 147-158

Contents list available at JMCS

Journal of Mathematics and Computer Science

Journal Homepage: www.tjmcs.com

An Application of the Crystography

Hacı AKTAŞ[1], Mehmet KALKAN[2]

[1]*Erciyes University, Kayseri*
[2]*Nevşehir Hacı Bektaş Veli University, Nevşehir.*

[1]***haktas@erciyes.edu.tr,*** [2]***mhmtklkn@yahoo.com***

Article history:
Received May 2014
Accepted June 2014
Available online June 2014

Abstract

A combination of cryptography and steganography is very important to information safety. Because together, they will not only hide but also encrypt the information at the same time. In the most crystographic studies, they hide the cipher text (encrypted) into the image, video or audio files to transfer. In this paper, we will give a simple and more convenient example for Crystography. We can also say that this method is applicable for most of the cryptographic algorithms to transfer them to the crystographic algorithm. As a simple example, it can be applicable for ATM card passwords etc. And then we have created and applied our method by using C# program language.

Keywords: Cryptography, Steganography, Pi, Crystography.
Categories: SD E.3, SD D 4.6, SD H. 2.5

1. Introduction

Cryptography is a collection of mathematical methods which transforms information from readable form to unreadable form. It is called encryption. A modern cryptographic systems are designed around computational hardness assumptions and must provide five main conditions; confidentiality, authentication, integrity, un deniability and access control. There are many appliction of cryptography [15,18, 20].

Steganography is a tool for communication that transfers confidential information over an open communication channel. It allows users to transfer information hidden in the plain text, pictures, audio or video files. To do this, it is not required any changes in the text to be hidden. Thus, the hidden data can be maintained and other people cannot be able to access the content. Steganography differs from cryptography in this aspect [2,5, 6, 7,9].

Both methods provide secure communication, but they use different algorithms and methods. By using the combination of these two methods it can be obtained a more confidential safer algorithm. M. H. Rajyagur has been identified the combination of cryptography and steganography as Crystography [14].

A combination of cryptography and steganography is very important to information safety. Because together, they will not only hide but also encrypt the information at the same time. In the most crystographic studies, they hide the cipher text (encrypted) into the image, video or audio files to transfer.

Cryptography is a set of mathematical methods which used to transform an information that cannot be read by unwanted people. Keyless, secret key and public key cryptography algorithms are three main groups. However, along with the design of quantum computers we must also be mentioned about quantum cryptography. But as it requires a very high cost the usage area is very limited [17,19].

In this paper, we will give a simple and more convenient example for Crystography. We can also say that this method is applicable for most of the cryptographic algorithms to transfer them to the crystographic algorithm. As a simple example, it can be applicable for ATM card passwords etc. And then we have created and applied our method by using C# program language.

Definition 1.1: Let; P is a finite set of plain text,

C, is a finite set of chipper text,

K, the key space, a finite set of possible keys,

E, is a finite set of Off function,

D, On a finite set of functions

If, for $\forall k \in K$ there is an encryption function, $e_{k} \in E$ and the corresponding decryption function $d_{k} \in D$ is; such that, $e_{k}: P \rightarrow C$ and $d_{k}: C \rightarrow P$ f.

If it provides $\forall x \in P\ d_{k}(e_{k}(x)) = x$, then (P, C, K, E, D) is called a crypto system.

The most common cryptography system are;

Keyless Cryptography (MD5, SHA-1, RIPEMD-160)

The changes in inputs causes the butterfly effect,

The system is protected by a very secret security system.

Secret Key (or symmetric) Cryptography (Caesar, Vigenere, DES, 3DES,RC5, Blowfish, IDEA, SAFER, AES)

Key size is small,

Can do faster encryption,

Key generation rate is high, but the key change is a serious problem,

Safety of the system is connected to the key.

Public Key (asymmetric) Cryptography (Diffie-Hellman, RSA, ElGamal, is Paille, Blum - Goldwasser, Goldwasser-mical, the Okamoto-Uchiyama,)

Key pair of sender and receiver are separate,

Each user is just enough to keep his own secret key,

Key exchange, even over insecure channels can be safely,

Uses the one-way function,

Will send a separate key for each recipient must produce,
The system is slow [18].

Also there are hybrid systems that use a combination of keys advantageous aspect of secret key and public key cryptography systems. Hybrid systems use symmetric keys for encryption, to transport these keys between the two sides, they use the asymmetric methods [11,13].

Definition 1.2: Steganography is a tool that allows the communication of confidential information over an open communication channel.

Steganography allows users to transmit hidden information in the plain text, pictures, audio or video files. The hidden data does not need any changes on it. Thus, the hidden data can be protected without content from unwanted people. So, in this aspect Steganography differs from cryptography systems [8, 12].
Steganography is mathematically defined as follows:

Definition 1.3: A steganographic system is a mechanism that to hide *c* secret message inside the body cover *m* by using the key k. As a result, the stego object *m* is obtained that carrying hidden message *c*.
Let F be an embedding function while G be an extraction function then (F, G) pair is called stegosystem. Therefore; $s = F(° C, m, k)$ and $m = G(s, k)$.
If M is the set of all possible messages, then embedding capacity of stegosystem will be $\log 2^{M}$.

Too many different file format techniques can be used as a carrier, but digital images are the most popular for steganography**.** There are 4 techniques for it [14]:

1) Text Techniques:
• Line Shift Coding Protocol,
• Word Shift Coding Protocol,
• Feature Coding Protocol,
• White Space Manipulation,
• Text Content.

2) Image Techniques:
• Simple Watermarking,
• LSB - Least Significant Bit Hiding,
• Direct Cosine Transformation,
• Wavelet Transformation.

3) Audio Steganography:
There are four main steps for audio Steganography which are:
Alteration,
Modification,
Verification,

Reconstruction.

4) Video Steganography:
This technique is used for mixing of sound and image (video files) and sends it together over the transmission medium.

Both methods provide secure communication, but they use different algorithms and methods. By using a combination of these two methods we can be obtain concealable safer algorithms. There are some of the work done on the combination of steganography and cryptography;

F. Borges et al., define combination of these two methods as steganocryptography. They show the steganocryptography model for a case where extreme security is needed. In the model they use Diffie-Hellman, RSA and cryptography with irrational numbers. They use also steganography in the Discrete Cosine Transform coefficients to send a message through the frames [3].

M. H. Rajyaguru, says "For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points". They are trying to solve the problem about the technique, they compose a very feast exchangeable key to that massage and trying to secure the massage by that key. They showed the improvement of the image Steganography system using LSB approach to ensure a means of secure communication [14].

A.J. Raphael and Dr. V Sundaram focus on the strength of combining cryptography and steganography methods to enhance the security of communication over an open channel. Their method shown in the Figure1 as [16];

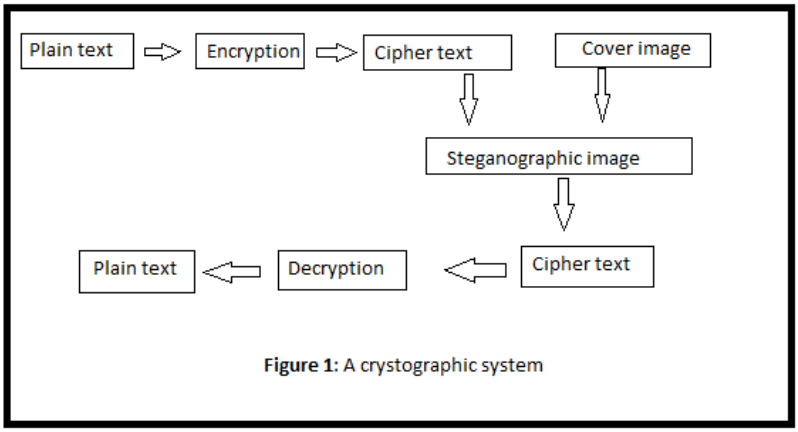

Figure 1: A crystographic system

A.M.A. Brifcani, describe the cryptography and steganography algorithms as stego-based-crypto. For encrypting the secret message, the system uses Rivest-Shamir-Adleman (RSA) cryptographic algorithm technique and to increase the security of the system were a key of 14 digits has been used, algorithm to cover this message it uses and Integer Wavelet Transform (IWT) based lifting scheme as a steganography. In here, to increase the capacity of the secret message payload and robustness, these

data are embedded in the IWT coefficients in 3 frequency sub-bands which are low, middle and high. This technique is tested by using 20 gray-scale standard images of size 512*512 with three formats (BMP, GIF and JPEG) [4].

A.R. Aparajita, look at hiding the text in text and then hiding the secret information in an image file by using various steganography methods. And then describe the main difference between cryptography and steganography[1].

S. A.Laskar and K. Hemachandra, to have for secret data communication they propose a method of combining cryptography and steganography. They suggest a high-performance JPEG steganography along with a substitution encryption method.
the method consists of three steps;

1. Compress the hidden message,
2. Encrypt this hidden message,
3. Embed obtained hiding data in the cover image

Their technique uses the discrete cosine DCT which used in the frequency domain for hiding encrypted data inside of an image. Their results show that the visual and the statistical values of the stegoimage with encrypted data before the insertion are similar to the values after the insertion. So it reduces the chance of the confidential message which being detected and enables secret communication. The effectiveness of this method has been estimated by computing MSE and PSNR[10].

A. B. Mansoor et al, used both systems for improved data security and defined this system as a hybrid CRYPTO-STEGANO technique. In this technique they use AES and DES cryptology algorithms for encryption and then hidden in JPEG images using F5 and model based steganography techniques [11].

2. Application of Crystography:

In this part, the simple application of the crystographic system will be given.

Definition 2.1: Fet is the value that obtained from the number sequence generated from cover text. It determine the placement range and the how many digits shifted is the number of bits.

This value is dependent on the bits number. For 4 bits system $0 < fet < 4$, for 16 bits $0<fet<16$ and so on. But smaller values are more effective for the system.

In this study, the most mysterious irrational number π as the cover, ten digits decimal system and Turkish alphabet letters will be used.

First of all, create Table1 by corresponding each letter with a number.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	

15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Table1

Decimal portion of the number π selected in desired size;

π=3,14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706798 21

Each number of plain text letters is determined from Table1. Determined numerals are placed between the digits of the series of numbers obtained from the π as;

Delete digits after the comma up to the fet value,

Put the first number just after the first digit,

Other numbers are placed one by one by passing digit up about the fet value respectively,

Get the new covered series of number,

Create a new table (Table2) that composed of 4 bits for each digit from 0 to 9,

0	1	2	3	4
0000	0001	0010	0011	0100
5	6	7	8	9
0101	0110	0111	1000	1001

Table2

Determine corresponding of each digits from Table2,

Get new series which consists of 0 and 1,

Separate each 3 digits of this series,

Sort the odd row triplets as the firs column, then the even row triplets respectively,

Get the new series which consists of 0 and 1,

Identify a key that composed of 4 bits in binary (Table3),

0000	0001	0010	0011
N	E	V	Ş
0100	0101	0110	0111
H	İ	R	Ü
1000	1001	1010	1011
S	T	F	B

1100	1101	1110	1111
L	M	O	G

Table3

Identify a character for each 4 bits of the new series from Table3 respectively,

Get the covered and encrypted text.

Example 2.1:

Plain text : NEVŞEHİR

Stego cover: Pi

Key : NEVŞHİRÜSTFBLMOG

Fet : 3

Apply this example on the above method program it by using the C# codes.

Solution 2.1: Each number of plain text letters is determined from Table1,

N	E	V	Ş	E	H	İ	R
16	5	26	22	5	9	11	20

Define pi;

π=3,14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706 79 821

Delete 3 digits after the comma,

592653589793238462643383279502884197169399375105820974944592307816406286208998628034825342117067 9 821

Put the first number just after the first digit,

5169265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706 79 821

Other numbers are placed one by one by passing 3 digits up respectively,

5169265535268972293253849626114332 0

Get the new covered series of number,

Create a new table (Table2) that composed of 4 bits for each digit from 0 to 9,

0	1	2	3	4
0000	0001	0010	0011	0100

5	6	7	8	9
0101	0110	0111	1000	1001

Table2

Determine corresponding of each digits from Table2,

Get new series which consists of 0 and 1, and get;

0101000101101001001001100101010100110101001001101000100101110010001010010011001001
0100111000010010010110001001100001000101000011001100100000

Separate each 3 digits of this series,

010 100 010 110 100 100 100 110 010 101 010 011 010 100 100 110 100 010 010 111 001 000 101
001 001 100 100 101 001 110 000 100 100 101 100 010 011 000 010 001 010 000 110 011 001 000
00

Sort the odd row triplets as the firs column, then the even row triplets respectively,

Get the new series which consists of 0 and 1,

0100101001000100100101001000100011010011000010001001000110100101100010010011010011
0101011100110010111000001100101110100101010000001000011000

Identify a key that composed of 4 bits in binary (Table3),

0000	0001	0010	0011
N	E	V	Ş
0100	0101	0110	0111
H	İ	R	Ü
1000	1001	1010	1011
S	T	F	B
1100	1101	1110	1111
L	M	O	G

Table3

Identify a character for each 4 bits of the new series from Table3 respectively,

Get the covered and encrypted text.

HFHHTHSSMVNSTEFİSTŞHMİLLBSŞVOTİNVES

The program of this example by using the C# codes is;

```
kriptom.Form1                                                    richTextBox1_KeyP
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Collections;namespace kriptom
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }

        private void richTextBox1_KeyPress(object sender, KeyPressEventArgs e)
        {

            if (char.IsDigit(e.KeyChar))
            {
                e.Handled = true;
            }
            if(char.IsWhiteSpace(e.KeyChar))
            {
                e.Handled = true;
            }
            if(char.IsSymbol(e.KeyChar))
            {
                e.Handled = true;
            }
            if (char.IsPunctuation(e.KeyChar))
            {
                e.Handled = true;
            }


        }
        private void button1_Click(object sender, EventArgs e)
        {
            string girilenMetin = richTextBox1.Text;
            richTextBox2.Clear();

            if (girilenMetin.Length == 0)
            {
                MessageBox.Show("Giriş Yapın");
            }

            else
            {

                string[] metinDizisi = girilenMetin.Select(c => c.ToString()).ToArray();
```

```
metinDizisi = metinDizisi.Select(s => s.Replace("a", "0")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("b", "1")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("c", "2")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("ç", "3")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("d", "4")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("e", "5")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("f", "6")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("g", "7")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("ğ", "8")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("h", "9")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("ı", "10")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("i", "11")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("j", "12")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("k", "13")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("l", "14")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("m", "15")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("n", "16")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("o", "17")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("ö", "18")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("p", "19")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("r", "20")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("s", "21")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("ş", "22")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("t", "23")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("u", "24")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("ü", "25")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("v", "26")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("y", "27")).ToArray();
metinDizisi = metinDizisi.Select(s => s.Replace("z", "28")).ToArray();


//double pi = Math.PI;
//string piSayisi = pi.ToString();

Random rnd = new Random();
int fetDegeri = rnd.Next(2,10);


string piSayisi = "3.14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706798214808651328230664709384460955058223172535940812848111745028410270193852110555964462294895493038196442881097566593344612847564823378678316527120190914564856692346034861045432664821339360726024914127372458700660631558817488152092096282925409171536436789259036001133053054882046652138414695194151160943305727036575959195309218611738193261179310511854807446237996274956735188575272489122793818301194912983367336244065664308602139494639522473719070217986094370277053921717629317675238467481846766940513200056812714526356082778577134275778960917363717872146844090122495343014654958537105079227968925892354201995611212902196086403441815981362977477130996051870721134999999837297804995105973173281609631859502445945534690830264252230825334468503526193118817101000313783875288658753320838142061717669147303598253490428755468731159562863882353787593751957781857785321712268066130019278766111959092164201989380952572010654858632788659361533818279682303019520353018529689957736225994138912497217752834791315155748572424541506959508295331168617278558890750983817546374649393192550604009277016711390098488240128583616035637076601047101819429555596198946767837449448255379774726847104047534646208046684259069491293313677028989152104752162056960240580381501935112533824300355876402474964732639141992726042699227967823547816360093417216412199245863150302861829745557067498385054945885869269956909272107975093029553211653449872027559602364806654991198818347977535663698074265425278625518184175746728909777727938000816470600161452491921732172147723501414419735685481613611573525521334757418494684385233239073941433345477624168625189835694855620992192221842725502542568876717904946016534668049886272327917860857843838279679766814541009538837863609506800642251252051173929848960841284886269456042419652850222106611863067442786220391949450471237137869609563643719172874677
```

```
string islemeGirecekPiSayisi = piSayisi.Substring(2 + fetDegeri, (fetDegeri * girilenMetin.Length) - 1);

string[] piSayıDizisi = islemeGirecekPiSayisi.Select(c => c.ToString()).ToArray();

ArrayList piSayıDizisiList = new ArrayList();
piSayıDizisiList.AddRange(piSayıDizisi);

for (int k = 1, i = 0; i < metinDizisi.Length; i++, k += fetDegeri+1)
{
    piSayıDizisiList.Insert(k, metinDizisi[i]);

}
piSayıDizisiList.Insert(0, fetDegeri.ToString());

string[] piSayıDizisi2 = (string[])piSayıDizisiList.ToArray(typeof(string));
```

```
                for (int i = 0; i < piSayıDizisi2.Length; ++i)
                {
                    richTextBox2.Text += piSayıDizisi2[i].ToString();
                    //if (i < piSayıDizisi2.Length)
                    //    richTextBox2.Text += "";
                }
            }
        }
    }
}
```

3. Conclusion

Nearly all of the studies on the combination of cryptography and steganography (crystography) concerned about sending encrypted messages in a digital file like text, image, audio or video files. But we have presented a new approach of crystography. Our stego method could combine with DES, AES or RSA algorithms. The unique feature about our method is, it can be implemented to ATM card, cellphone .. etc. password security programs to improve their secure level. And also, any series of number can used as a stego cover.

4. References:

[1] A.R. Aparajita, " STEGNOGRAPHY---"The Art of Hiding Information" A Comparison from Cryptography ", International Journal of Innovative Research in Science, Engineering and Technology, Copyright to IJIRSET www.ijirset.com, 1308, Vol. 2, Issue 5, May 2013.

[2]D. Bhattacharyya,Poulami Das,Samir Kumar Bandyopadhyay, and Tai-hoon Kim,Text Steganography: A Novel Approach, International Journal of Advanced Science and Technology, Vol. 3, February, (2009).

[3] Borges, F., Portugal, R., & Oliveira, J. Steganography with Public-Key Cryptography for Video conference, National Laboratory of Scientific Computing - LNCC, 25651-075, Petr´opolis, RJ

[4] A.M.A. Brifcani,"Stego-Based-Crypto Technique for High Security Applications ", International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 1793-8201, (2010).

[5] [Challita, 11] : K. Challita and H. Farhat, Combining Steganography and Cryptography: New Directions, IJNCAA, 1(1): (2011)199-208, SDIWC, (ISSN 2220-9085).

[6]S. Channalli, A. Jadhav, Steganography An Art of Hiding Data, International Journal on Computer Science and Engineering Vol.1(3),(2009) 137-141.

[7] N.N. El-Emam. (2007). "Hiding a large amount of data with high security using steganography algorithm." Journal of Computer Science 3 (4), (2007) 223-232.
[8] S. Gorla, Combination of cryptography and teganography for secure communication in video file, Master Thesis, California State University, Sacremento, (2009).
[9]N. Hamid et al, Image Steganography Techniques: An Overview, IJCSS, Volume (6) : Issue (3), (2012).
[10] S. A. Laskar and K. Hemachandran, "Secure Data Transmission Using Steganography and Encryption Technique" International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.
[11] A.B. Mansoor, Z. Khan, S.A. Khan, CRYPTO-STEG: A Hybrid Cryptology - Steganography Approach for Improved Data Security, Mehran University Research Journal of Engineering & Technology, Volume 31, No. 2, April, (2012).
[12] Maria Akhtar Mufti, Aihab Khan, Malik Sikandar Hayat Khiyal and Asim Munir, Transmitting Cryptographic data through Steganography, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, (2012), ISSN (Online): 1694-0814
[13] Ochin, Evgeny, Larisa Dobryakova, Zbigniew Pietrzykowski,Piotr Borkowsk. "The application of cryptography and steganography in the integration of seaport security subsystems Zastosowanie kryptografii i steganografii w integracji podsystemów bezpieczeństwa informacyjnego portów morskich." Zeszyty Naukowe Akademia Morska w Szczecinie, 26(98) pp.(2011),80-87.
[14]M. H. Rajyaguru, CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys,IJETAE, Volume 2, Issue 10, (2012).
[15] Amir Ehsani, “An Application of Co-Medial Algebras with Quasigroup Operations on Cryptology”, TJMCS Vol.10(2014), No.2, 113-118.[16] A.J. Raphael, Dr.V Sundaram, "Cryptography and Steganography -- A Survey",ISSN:2229-6093, IA.Joseph Raphael,Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.
[17] N. Saran, Kriptografideki Güncel Çalışmalar, 2. Mühendislik ve Teknoloji Sempozyumu, Çankaya Üniversitesi / Ankara,30 Nisan - 1 Mayıs 2009.
[18]http://tr.wikipedia.org, (2013).
[19]H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, G. Ribordy**,** “Quantum cryptography” Appl. Phys. B 67,(1998) 743–748.
[20]S. H. Kamali, M. Hedayati, R. Shakerian, S. Ghasempour, “Using Identity-Based Secret Public Keys Cryptography for Heuristic Security Analyses in Grid Computing” TJMCS Vol.3 No.4, (2011), 357 – 375.