Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals of DAAAM International

DATABASE ENCRYPTION ALGORITHM: NEW SCYTALE

BOICEA, A[lexandru]; GRIGORE, E[lena] M[ihaela]; GHITA, V[lad]; BENTU, S[tefan] A[lexandru]; TRIFAN, I[onut] & POPA, G[eorge] D[an]

Abstract:*Databases are a major interest point for many business domains. Large amount of information must be carefully kept and managed. An attribute to maintain that "carefully" characteristic is to secure the information. Data encryption has at the moment many solutions. This paper comes with a new symmetric encryption algorithm which uses an old idea, the Scytale technique encountered at the ancient Greeks, and transforms it using IT and mathematical methods.*
Keywords: *database, encryption, Scytale, algorithm*

1. INTRODUCTION

The Scytale method was used by the ancient Greeks to communicate in their military campaigns. They were wrapping a strip of leather around a cylinder and form the encrypt message by reading it on horizontal. The recipient used a rod of the same diameter on which he wraps the paper to read the message. It has the advantage of being fast and not prone to mistakes (Sanger L., Wales J., 2001). A simple search on Google of the word "Scytale" will point you to the next picture (Fig. 1).

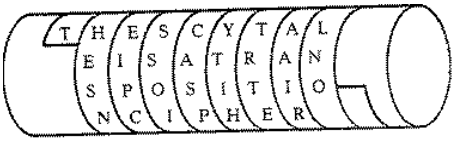

Fig. 1. Ancient Greeks Scytale (Brown L., 2001)

Which in today words is like you will wrap, for example, the abstract of this paper on a cylinder (Fig.2).

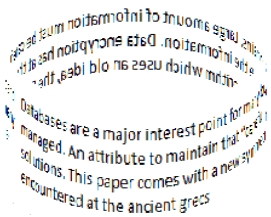

Fig. 2. Translation of what Scytale method could be today

For the New Scytale algorithm we propose to use the above idea but to generate a different geometric shape for each message that will be encrypted.

2. NEW SCYTALE ENCRYPTION METHOD

To describe how the algorithm work we will start from this text "databases are a major interest point for many business domains".

The NS method is formed from 4 steps:

At *first* it will be applied an algorithm to find out the 3D coordinates for the points which will be used to form the geometric figure. For that each 3 characters of the message will represent a point in space. To obtain the numerical values of the coordinates their ASCII values will be returned (Tab.1).

	x	y	z	
point 1	100	97	116	dat
point 2	97	98	97	aba
point 3	115	101	115	ses
point 4	32	97	114	ar
point 5	101	32	97	e a
point x	...	...	...	
point21	110	115	115	ns

Tab. 1. Space points coordinates

In case, that for the last point, remains one or two characters the ASCII code for that one will be replicated for each remained coordinate. The first intention was to fill it with zeros but, as in the above case, a point that will have one or more coordinates equal to zero will lead to an inconsistent geometric figure because all the other coordinates are greater than 32.

The second step is based on the Delaunay triangulation and will have as input data the coordinates obtained above and as output data a tessellation of tetrahedrons (de Berg M., 2008).

For the 21 points that we have obtained the figure will be like the one from Fig. 3.

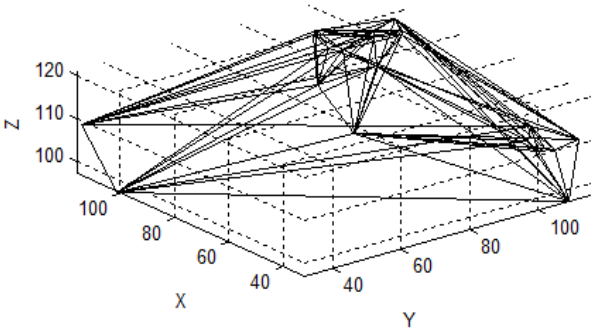

Fig. 3. The space figure obtained

As is it is easily to see the figure complicates along with the size of the message increases. That is a disadvantage of the algorithm because the delay will be significantly higher if it is a very long message. This is a part that is seen as a future request: the complexity of the figure must be in inverse proportion with the length of the message.

The third step is to convert the message into an image and wrap it on the Fig.4. For this type of conversion any already existing method can be used. The figure is expanded and the edges of the form are bolded so they can be observed.

Fig. 4. Wrapping the message on the figure obtained

At last *the fourth step* is to read the encrypted message(Fig.5).

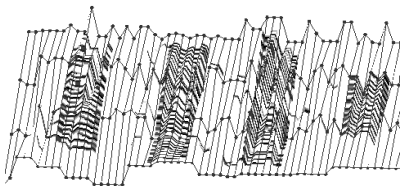

Fig. 5. Reading the encrypted message

The encrypted message will be sent in bits with the key formed from:

- *Geometric form dimensions*
- *Type of image:* format (.png, .jpg, .gif etc.), sizes, font color and size, background color, vertical alignment and other characteristics that were used when the conversion to image was done.

The first two steps were implemented in Matlab version 7.7.0.471 (R2008B). For shape generation function *delaunay3* was used as follows:

$$Tes = delaunay3(x, y, z, \{'Qt', 'Qbb', 'Qc', 'Qz'\}) \quad (1)$$

Parameters Qt, Qbb, Qc, Qz were used to triangulate all non-simplicial facets before generating results, to scale the last coordinate to [0,m] for Delaunay, to keep coplanar points with nearest facet and to add a point above the paraboloid of lifted sites for a Delaunay triangulation (Barber C, 2002). To plot the output of the *delaunay3* function we used *tetramesh* function which displays the tetrahedrons defined in Tes as mesh. A row of Tes contains indices into XY of the vertices of a tetrahedron (The MathWorks Inc., 2010). *Tetramesh* uses the default transparency parameter value 'FaceAlpha' = 0.9 but we changed the value to 1 so that the edges from inside the shape could not be seen because they do not make the object of this demonstration:

$$tetramesh(Tes, XY, 'FaceAlpha', 1, 'CData', NaN); \quad (2)$$

XY concatenates the arrays that keeps the coordinates.

To wrap the image on the shape we had to expande it, this means that the *surface* function was used on the Tes parameter:

$$I = imread('E:\research.png'); \quad (3)$$

$$warp(Tes, I) \quad (4)$$

3. THE DELAUNAY TRIANGULATION

The Delaunay triangulation of a set of points in the plane divides the plane into a number of triangles, plus one open figure. The set of triangles is the "best" in the sense that: one couldn't add another triangle without going out of the plane and the triangles maximize their smallest angle; that is, the triangles avoid being long and skinny.

The Delaunay triangulation leaves an open figure, which is the inverse of the convex hull. That is, the outermost edges of the triangles form the convex hull of the points.

The Delaunay triangulation is also the dual of the Voronoi diagram of these points. An edge of the triangulation maps to an edge of the diagram; a triangle maps to a Voronoi vertex; a vertex of the triangulation maps to a Voronoi cell.

The incremental algorithm begins by surrounding the point set by one huge triangle. One by one (aribtrarily), a point is connected to the triangle which surrounds it. Once all points have been connected, the lines which connect the points to the original huge triangle are removed; the figure that remains is the Delaunay triangulation (Franklin&Marshall College, 2010).

A Voronoi diagram is sometimes also known as a Dirichlet tessellation. The cells are called Dirichlet regions, Thiessen polytopes, or Voronoi polygons.

Voronoi diagrams were considered as early at 1644 by René Descartes and were used by Dirichlet (1850) in the investigation of positive quadratic forms. They were also studied by Voronoi (1907), who extended the investigation of Voronoi diagrams to higher dimensions. They find widespread applications in areas such as computer graphics, epidemiology, geophysics, and meteorology. A particularly notable use of a Voronoi diagram was the analysis of the 1854 cholera epidemic in London, in which physician John Snow determined a strong correlation of deaths with proximity to a particular (and infected) water pump on Broad Street (Weisstein E., 2010).

4. CONCLUSION

The New Scytale (NS) algorithm borrows the main idea from the ancient Scytale and the Delaunay Triangulation to make the shape based on the input message but it brings a method to return a set of 3D points and unite all this elements to form a new symmetric algorithm.

The key transmitted is composed on multiple elements that were used on encryption steps. A decrypting method makes the object of the next paper because there are some points that needs improvements so that the encrypting part to be complete.

The project is in research phase and we need to find a way to implement the reading bit by bit from the shape and to form a new image with the string of bits that we obtain.

The problem of the delays must also be solved. A solution to this is to introduce an alternative to the tetrahedrons: the curved forms and to simplify the shape when the message size is very large.

5. REFERENCES

Barber, C. B. (2002). The Geometry Center, *Available from:* http://www.qhull.org/html/qh-optq.htm#Qc *Accessed:* 2010-05-29

Brown, L. (2001). Classical Transposition Ciphers, *Available from*: http://www.cs.ubbcluj.ro/~florin/Si/Security/ccs3/lectures/less05.html *Accessed:* 2010-05-30

de Berg, M.et al (2008). *Computational Geometry: Algorithms and Applications*, Publisher, ISBN, Springer-Verlag

Franklin&Marshall College (2010). Delaunay Triangulation: incremental algorithm, Available from: http://www.fandm.edu/x5087 Accessed: 2010-05-29

Sanger, L. & Wales, J. (2001). Wikipedia, *Available from:* http://en.wikipedia.org/wiki/Scytale *Accessed:* 2010-05-29

Weisstein, E. (2010). Voronoi Diagram, *Available from:* http://mathworld.wolfram.com/VoronoiDiagram.html *Accessed:* 2010-05-29

*** The MathWorks, Inc. (2010) *Available from:* http://www.mathworks.com/access/helpdesk/help/techdoc/ref/tetramesh.html *Accessed*: 2010-05-02