MULTIDIMENSIONAL ENCRYPTION ALGORITHM FOR COMPUTER NETWORKS

MUSBAH J. AQEL, A . S. ABDUL-AHAD, R. S. QAHWAJI

Department of Electronic Image and Media Communication–
School of Informatics, Bradford University,
Richmond Road, Bradford BD7 1DP,U.K.
musbahaqel @yahoo.com, amir_st ephan@ yahoo.ac.uk
R.S.R.Qahwaji@Bradford.ac.uk

Abstract: The paper proposes a multidimensional encryption algorithm for security in computer networks. The work in this paper is intended to be quite different from the security algorithms used today, like WEP (Wireless Equivalent Privacy), 802.1X and so on. With Quality of Protection (QoP) as a major consideration, the same security effectiveness of former predecessor algorithms can be achieved. The algorithm can be used at different levels of security based on the degree of security required. This degree of security is divided into four levels, three of which are based on block cipher and the fourth is based on stream cipher approach. Since the algorithm is developed based on symmetric key approach, it could also be used for decryption with different and extra complexities.

Keywords: Multidimensional encryption, decryption, QoP, symmetric key

1. INTRODUCTION

In recent years, the fast progress in the fields of telecommunications, satellite, broadcasting, and mobile communication, have resulted in significant effect and explosive growth in related fields such as Internet, multimedia, and wireless residential networks (Yu et al, 2001). The data security of Internet aims at protecting the data from unauthorized intrusion, which is of paramount importance (Dittman et al., 2001; Forta and Lauver, 2000). Likewise, the security of multimedia data is essential for commerce protection
(Dittman et al, 2001; Salli et al, 1998; Lo and Chen, 1999).
Threat models normally pose negative ongoing effects due to their attacks
Diversity (Eavesdropper attack, Trojan horse attack, Man-in-the-middle attack…and so on). This is usually accentuated by the weakness and the vulnerability of some algorithms used today in security and their being easily breakable (Air defence, 2004; Peikari and Fogie, 2003).

Generally, network security services can be divided into four areas:

Confidentiality, authentication, data integration, and Non-repudiation. Confidentiality is a security service that provides resistance to the security attack whenever two parties like to communicate with each other and don't wish to reveal the contents of their messages to a third party. This communication process should not be revealed to an unauthorized party. Encryption of the message and the identities of the two communicating parties is the most common method used to provide confidentiality and provides a guarantee for the receiver of a message on an assurance of the sender identity (Stalling, 1998; Simmons, 1990).

There are mainly three categories of cryptographic methods for data encryption and decryption; Secret Key schemes that use the same key (shared key) for encryption and decryption (i.e. RSA algorithm), Public Key schemes that use different keys for encryption and decryption (i.e. DES algorithm), and Hash Function (one-way functions) that are used to protect the integrity and authenticity of messages (Brenton and Cameron, 2003; Shamir, 1997).

Accordingly, the objectives of this paper are to introduce a new security model in such a way that the attackers' threats (internal as well as external threats) be far from reaching their immediate objectives, and are handicapped in terms of time until the expiration of the importance and the privacy of the protected data are of no more significance.

In this paper, a multidimensional algorithm is proposed to encrypt and decrypt a plain text message with the same algorithm. The algorithm is based on four levels of security, where the first three levels are based on block cipher and the fourth level is based on stream cipher. According to the importance of the contents of the message, a proper level of security will be selected and used. Levels (1-3) of the encryption are intended as tactical security while using the fourth level is intended as strategic security.

2. MULTIDIMENSIONAL ENCRYPTION ALGORITHM

Any message (i.e. a text file) can be divided into a group of eight lines, each line into groups of eight words, and each word into groups of eight characters if possible (if not, the preceding word is appended with the next word and so forth), and each character is converted to encrypted 8-binary value that is different from its actual ASCII value. Of course, many choices can be made for the number of Lines, Words, Characters, and Binary. However, the choice of eight is time-effective (i.e. a good trade-off is a between time and speed of execution of the algorithm). According to the importance of the message or any parts thereof, a suitable security level will be selected. There are four levels for the selection of the degree of security required to encrypt the message:

1. Low level security
2. Moderate level security
3. High level security
4. Critically high level security

These levels of security represent the four dimensions of the algorithm (i.e. line, word, character, and binary (ASCII)) as follows:

1. Low level degree of security can be implemented by line encryption dimension alone.

2. Moderate level degree of security can be implemented by word encryption dimension alone.

3. High level of security can be implemented by character encryption dimension alone.

Levels 1, 2, and 3 are considered block cipher. However, the character encryption dimension may also be considered as a stream cipher (Anderson, 2001).

4. Critically high level security can be implemented by binary (ASCII) encryption dimension alone. This part is considered as a stream cipher.

Even though, strictly speaking, non-consecutive selection of the levels of security is theoretically possible; however, such a selection provides no additional value and is of no practical significance, and hence, is neither recommended nor advocated.

3. THE PROPOSED ALGORITHM

The algorithm proceeds as follows:

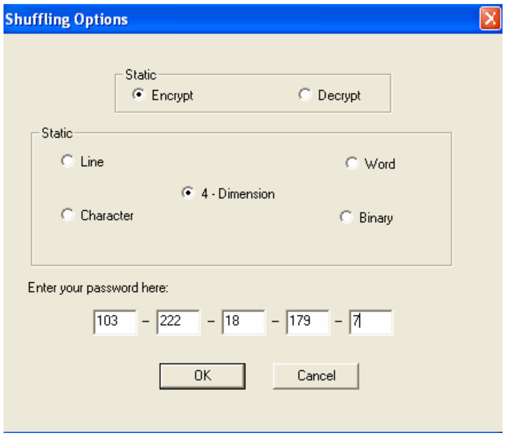
1. Key generation policy and tapping process (Maximum Length)

The secret key consists of five interactive GUI (Graphical User Interface) components of text fields as shown in figure 1, where the first four text fields are considered as sub keys for each dimension. Each sub key has 8-bit size, which is 0-255 decimal equivalent. The fifth text field represents the XORed tapping selection process of an 8-bit register. The sub key value of each one of the first four text fields represents the initial value for a relevant register. The sub key value of the fifth text field represents the selection of tapping model (0-15 allowed probabilities); with each of these sixteen models being designed to give a maximum length.

After selecting the dimension(s) (i.e., any single dimension, or any combination of dimensions, or all the dimensions) and completing the initialization of the text field(s) (i.e., any relevant single text field, or any relevant combination of text fields, or all the four text fields), where the fifth text field must always be set; each one of the four tapped registers generates its own maximum length depending on its initializations.

The maximum length values of each one of the four tapped registers (their tapping configurations are decided by the fifth text field) will be used to get the independent scramble codes for each of the relevant dimensions, therefore resulting in a complication in the process of attacking.

There are exactly 8! (40320) scramble codes, where the condition to accept any of these codes depends on the difference of minimum-2 between any two adjacent numerals (e.g. 47283615), this difference is a programmable issue.



Static
● Encrypt ○ Decrypt

Static
○ Line ○ Word
● 4 - Dimension
○ Character ○ Binary

Enter your password here:
103 – 222 – 18 – 179 – 7

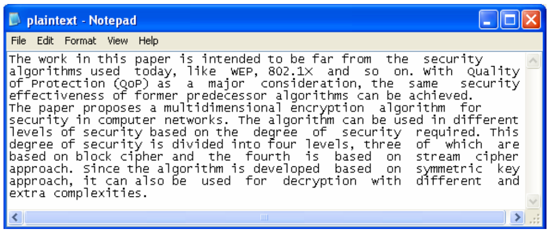
Figure 1: Selection of dimension and secret key management

2. Selection of encryption dimension

At this stage, the degree of security level should be decided so that the suitable dimension of encryption would be selected accordingly. There are four dimensions for encryption starting from level 1 to level 4. Level 1 represents the weakest dimension that is based on block cipher and level 4 is the strongest dimension that is based on stream cipher. Hence, according to the importance of the message at hand, the degree of security should be decided and hence the dimension will be selected. The dimension encryption process will be carried out as follows:

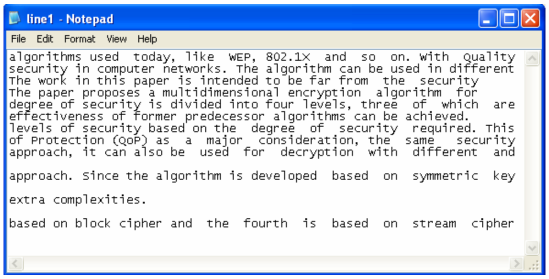
I. *Line Dimension Encryption*

Any text file consists of a collection of lines as shown in figure 2. The file subdivides into groups; each group consists of 8-lines. The first group of 8-lines will be selected and the positions of the lines will be scrambled and rearranged according to the scramble codes generated as shown in figure 3. This process is repeated until all 8-line groups of the text are encrypted in different and specific scramble code for each group.



```
The work in this paper is intended to be far from  the  security
algorithms used  today, like  WEP, 802.1X  and  so  on. With  Quality
of Protection (QoP) as  a  major  consideration, the  same   security
effectiveness of former predecessor algorithms can be achieved.
The paper proposes a multidimensional encryption  algorithm  for
security in computer networks. The algorithm can be used in different
levels of security based on the  degree  of  security  required. This
degree of security is divided into four levels, three  of  which  are
based on block cipher and  the  fourth  is  based  on  stream  cipher
approach. Since the algorithm is developed  based  on  symmetric  key
approach, it can also be  used  for  decryption  with  different  and
extra complexities.
```

Figure 2: Plaintext

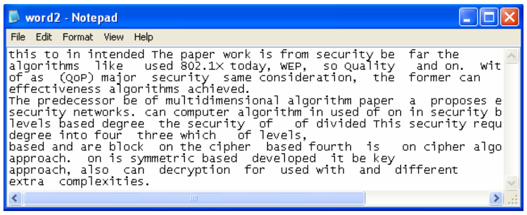


```
algorithms used  today, like  WEP, 802.1X  and  so  on. With  Quality
security in computer networks. The algorithm can be used in different
The work in this paper is intended to be far from  the  security
The paper proposes a multidimensional encryption  algorithm  for
degree of security is divided into four levels, three  of  which  are
effectiveness of former predecessor algorithms can be achieved.
levels of security based on the  degree  of  security  required. This
of Protection (QoP) as  a  major  consideration, the  same   security
approach, it can also be  used  for  decryption  with  different  and

approach. Since the algorithm is developed  based  on  symmetric  key

extra complexities.

based on block cipher and  the  fourth  is  based  on  stream  cipher
```

Figure 3: Applying Line encryption to the text of figure 2

II. Word Dimension Encryption

Any line of text consists of a collection of words; the lines are tokenized into 8-words groups. A second initialized text field is used to generate scramble codes to encrypt all the 8-word groups separately and uniquely as shown in figure 4. Note that in this example the word dimension encryption is applied to the original plaintext file as shown in figure 2.

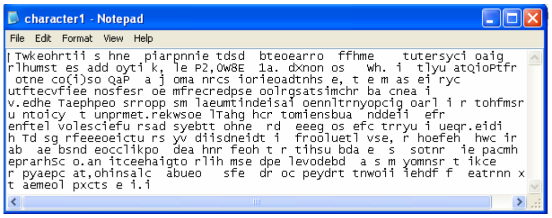


```
this to in intended The paper work is from security be  far the
algorithms  like   used 802.1X today, WEP,  so Quality   and on.  Wit
of as  (QoP) major  security  same consideration,  the  former can
effectiveness algorithms achieved.
The predecessor be of multidimensional algorithm paper  a  proposes e
security networks. can computer algorithm in used of on in security b
levels based degree  the security  of   of divided This security requ
degree into four  three which   of levels,
based and are block  on the cipher  based fourth  is   on cipher algo
approach.  on is symmetric based  developed  it be key
approach, also  can  decryption  for  used with  and  different
extra  complexities.
```

Figure 4: Applying Word encryption to the text of figure 2

III. Character Dimension Encryption

Continuing the process of encryption, the word in turn, consists of a collection of characters. The file is grouped in packets of 8-characters each. The third initialized text field is used to generate scramble codes to encrypt all the 8-character groups separately and uniquely as shown in figure 5. Note that the character encryption dimension is applied to the original Plaintext file as shown in figure 2.

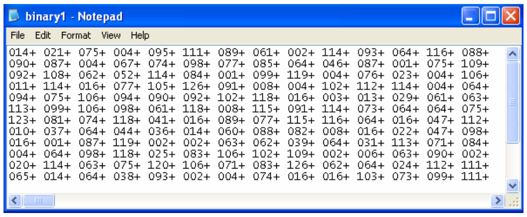


```
Twkeohrtii s hne  piarpnnie tdsd  bteoearro  ffhme    tutersyci oaig
rlhumst es add oyti k, le P2,0W8E  1a. dXnon os   wh. i  tlyu atQioPtfr
 otne co(i)so QaP  a j oma nrcs iorieoadtnhs e, t e m as ei ryc
utftecvfiee nosfesr oe mfrecredpse oolrgsatsimchr ba cnea i
v.edhe Taephpeo srropp sm laeumtindeisai oennltrnyopcig oarl i r tohfmsr
u ntoicy  t unprmet.rekwsoe lTahg hcr tomiensbua  nddeii  efr
enftel volesciefu rsad syebtt ohne  rd  eeeg os efc trryu i ueqr.eidi
h Td sg rfeeeoeictu rs yv diisdneidt i  frooluetl vse, r hoefeh  hwc ir
ab  ae bsnd eocclikpo  dea hnr feoh t r tihsu bda e  s  sotnr  ie pacmh
eprarhSc o.an itceehaigto rlih mse dpe levodebd  a s m yomnsr t ikce
r pyaepc at,ohinsalc  abueo   sfe  dr oc peydrt tnwoii iehdf f  eatrnn x
t aemeol pxcts e i.i
```

Figure 5: Applying Character encryption to the text of figure 2

IV. Binary (ASCII) Dimension Encryption

The final process of this algorithm is to operate on the binary bits of each character. At this stage the whole text is in the form of groups, each consisting of 8-binary bits. The fourth initialized text field is introduced and applied to generate the scramble codes to encrypt these groups, bit by bit, (stream ciphered) as shown in figure 6. This is in contrast to levels 1, 2, and 3 where the encryption is block ciphered. Note again that the binary (ASCII) encryption dimension is applied to the original Plaintext file as shown in figure 2. So far, each of the four levels of the encryption algorithm has been applied to the original plaintext file. However, these four levels of the encryption algorithm can be applied in combination, i.e. consecutively in a cascading order. The output of each level is used as input to the next level. The final output of such a combined procedure is shown in figure 7. This subject will be discussed in more detail in the next paragraph.



```
014+ 021+ 075+ 004+ 095+ 111+ 089+ 061+ 002+ 114+ 093+ 064+ 116+ 088+
090+ 087+ 004+ 067+ 074+ 098+ 077+ 085+ 064+ 046+ 087+ 001+ 075+ 109+
092+ 108+ 062+ 052+ 114+ 084+ 001+ 099+ 119+ 004+ 076+ 023+ 004+ 106+
011+ 114+ 016+ 077+ 105+ 126+ 091+ 008+ 004+ 102+ 112+ 114+ 004+ 064+
094+ 075+ 106+ 094+ 090+ 092+ 102+ 118+ 016+ 003+ 013+ 029+ 061+ 063+
113+ 099+ 106+ 098+ 061+ 118+ 008+ 115+ 091+ 114+ 073+ 064+ 064+ 075+
123+ 081+ 074+ 118+ 041+ 016+ 089+ 077+ 115+ 116+ 064+ 016+ 047+ 112+
010+ 037+ 064+ 044+ 036+ 014+ 060+ 088+ 082+ 008+ 016+ 022+ 047+ 098+
016+ 001+ 087+ 119+ 002+ 002+ 063+ 062+ 039+ 064+ 031+ 113+ 071+ 084+
004+ 064+ 098+ 118+ 025+ 083+ 106+ 102+ 109+ 002+ 006+ 063+ 090+ 002+
020+ 114+ 063+ 075+ 120+ 106+ 071+ 083+ 126+ 062+ 064+ 024+ 112+ 111+
065+ 014+ 064+ 038+ 093+ 002+ 004+ 074+ 016+ 016+ 103+ 073+ 099+ 111+
```

Figure 6: Applying Binary encryption to the text of figure 2

4. MULTIDIMENSIONAL ALGORITHM IMPLEMENTATION

The main theme, which is considered in designing the algorithm, is the expiration of the file itself. This is mainly dependent on the importance of the data in the file. The expiration of the importance of the data (i.e. files) is a relative parameter. Some files have short expiration of importance after which the data in the file becomes meaningless and hence any attacking of these files becomes useless and time wasting. So, tactically the selection of one or any combination of the first three dimensions would suffice and serve the desired purpose.

As a result and on the light of what is explained above, the algorithm is designed to gain the advantages of both block and stream ciphering techniques simultaneously. As such it will sustain and strengthen the algorithm strategically against the attackers by posing different phases, especially when using all four dimensions for encryption where the secret key is long (i.e. 36 bits) enough thereby complicating any trial to break the encrypted file.

Mathematically and practically, the strength of the multidimensional algorithm is calculated and measured as follows:

-Each one of the first four text fields and the fifth text field give 256 and 16 combinational probabilities, respectively.

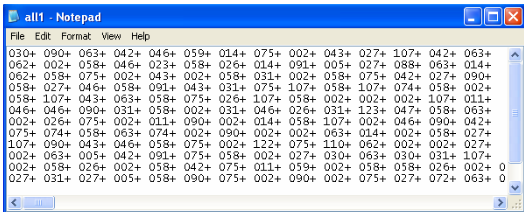
-The combinational probability of each one of the first four text fields selects one of the permutations 8! (40320) randomly and independently. So, the total complexity of the algorithm will be (16*Math.pow (256, 4)*Math.pow (8!, 4) =1.8*10^29).

-Assuming that if the speed of the processing is (10^-12 sec), the attackers need (5.8*10^9 years) to break the encrypted file.

-The algorithm performance has been tested and evaluated by data visualization technique. An encrypted file has been subjected to visualization process where an excellent distribution has been obtained which indicates that the algorithm is quite strong and difficult to break.

Tactically, the selection of any combination of the first three of block ciphering dimensions will not have the same strength of the secret key compared to the full selection. Additionally, the contents of the encrypted file can be recognized easily when the first two dimensions are selected (line and word dimensions). Thus, the first two dimensions are introduced only to elongate and complicate the secret key when implementing the third or fourth dimensions (character or binary (ASCII) dimensions) as shown in figure 7. Moreover, this will cause hackers to suspect greatly, how the key management and selection have been accomplished.

After initialization, the key in the algorithm is entirely and totally a varied feature, exclusively for each dimension independently. This means that different and distinct list of scramble codes are generated for each dimension, thereby eliminating absolutely, any relationship between these dimensions. Accordingly, from a strategic point of view the algorithm has two important aspects; the long secret key and the multidimensional encryption including both block and stream ciphering. Finally, as a consequence to these aspects, the strength of the algorithm does not depend solely on the length of the key, but also on the dimension(s) used in the encryption process.



```
030+ 090+ 063+ 042+ 046+ 059+ 014+ 075+ 002+ 043+ 027+ 107+ 042+ 063+
062+ 002+ 058+ 046+ 023+ 058+ 026+ 014+ 091+ 005+ 027+ 088+ 063+ 014+
062+ 058+ 075+ 002+ 043+ 002+ 058+ 031+ 002+ 058+ 075+ 042+ 027+ 090+
058+ 027+ 046+ 058+ 091+ 043+ 031+ 075+ 107+ 058+ 107+ 074+ 058+ 002+
058+ 107+ 043+ 063+ 058+ 075+ 026+ 107+ 058+ 002+ 002+ 002+ 107+ 011+
046+ 046+ 090+ 031+ 058+ 002+ 031+ 046+ 026+ 031+ 123+ 047+ 058+ 063+
002+ 026+ 075+ 002+ 011+ 090+ 002+ 014+ 058+ 107+ 002+ 046+ 090+ 042+
075+ 074+ 058+ 063+ 074+ 002+ 090+ 002+ 002+ 063+ 014+ 002+ 058+ 027+
107+ 090+ 043+ 046+ 058+ 075+ 002+ 122+ 075+ 110+ 062+ 002+ 002+ 027+
002+ 063+ 005+ 042+ 091+ 075+ 058+ 002+ 027+ 030+ 063+ 030+ 031+ 107+
002+ 058+ 026+ 002+ 058+ 042+ 075+ 011+ 059+ 002+ 058+ 058+ 026+ 002+ 0
027+ 031+ 027+ 005+ 058+ 090+ 075+ 002+ 090+ 002+ 075+ 027+ 072+ 063+ 0
```

Figure 7: Four dimensions encryption of line, word, character, and binary in combination of the original plaintext

5. CONCLUSION

A multidimensional algorithm with four dimensions has been developed for plain text data security. Each of the four dimensions represents an additional level to the degree of security. Since not all messages require the same degree of importance and security, the algorithm takes into account this idea and can provide different levels of security according to the importance and the privacy of the message. The first three levels are based on block cipher; they can be broken with increasing time and complexity from level 1 to level 3. The fourth level is based on stream cipher which is considered a rather very strong level, and very difficult to break. It is believed that this adds substantially to the mechanism of security.

REFERENCES

Air Defence, Inc., 2004, "Wireless LAN Security What Hackers Know That You Don't",

Anderson R. J., 2001, " Security Engineering: A Guide to Building Dependable
Distributed Systems". John Wiley & Sons, Inc.

Brenton C. and Cameron H. 2003, "Networking Security", Sybex.

Dittman J., Wohlmacher P.,and Nahrstedt K., 2001." Using Cryptographic and Watermarking Algorithms". IEEE Multimedia, vol. 8, no. 3, Pp. 54-65.

Forta B., and Lauver K., 2000, "WAP Development with WML and WMLScript", SAMS Publishing.

Lo, C.C., and ChenY. J., 1999, " Secure Communication Mechanisms for GSM Networks". IEEE Trans. Consumer Electronics, vol. 45, Pp. 1074-1080.

Peikari C., and Fogie S., 2003, " Maximum Wireless Security", SAMS Publishing.

Salli K.T., Hamalainen T., Knuutila J., and Saarienen J.,1998, " Security design for new wireless local area network TUTWLAN". IEEE International Symposium on Personal Indoor and Mobile Radio Communications, PIMR, vol. 3, Pp. 1540-1544.

Shamir A.,1997," How to Share a Secret", Communications of ACM, vol. 22, no. 11, Pp. 612-613.

Simmons G. J., 1990.How to (really) Share a Secret, Advances in Cryptology- Crypto '88 Proceedings, Springer-Verlag, Pp. 390-448.

Stallings W.,*1998* ," Cryptography and Network Security", Prentice-Hall.

Yu, H. H., Kundur, D., and Lin N. C. Y, 2001. “Spies, thieves, and the battle for multimedia in the digital era", IEEE multimedia, vol. 8, no. 3, Pp. 8-12.

AUTHORS’ BIOGRAPHIES

Dr. Musbah J. Aqel obtained his M.Sc. in Computer Engineering from Aligarh Muslim University – India and his PhD from I.T, Banaras Hindu University- India in Computer Engineering. He is currently associated professor of computer engineer, and chairman of Electrical and Computer Engineering Dept, Applied science university-Jordan. He joined Electronic Imaging and media communication department at the university of Bradford as a post doctoral. He is an editor in International journal of soft computing and applications. His research interest includes knowledge-base system design, image processing, computer networks, and simulation techniques.

Amir A. Stephan obtained his M.Sc in computer Engineering from Baghdad university. He joined school of informatics, university of Bradford as a PH.D. student. He worked as a lecturer at Applied Science university – Jordan.. His research of interest is computer network security, pattern recognition, and computer control.

Dr. R. S. Qahwaji received his PH.D from school of informatics, university of Bradford and he is currently a lecturer at the Electronic Imaging and media communications department at the University of Bradford. He is a member of the Higher Education academy (HEA), The Institution of Electrical Engineer (IEE), International Society for Computers and Their Applications (ISCA) and the American Geophysical Union (AGU). His research expertise include: image processing, pattern recognition and machine learning and the design of machine vision systems. He has publications in the fields of solar imaging, medical imaging, biometrics and face recognition, morphological transforms, statistical classifiers and neural networks, security and watermarking.