

# Multidimensional Encryption Algorithm for Computer Networks

**Musbah J. Aqel**

[musbahaqel@yahoo.com](mailto:musbahaqel@yahoo.com),

**A . S. Abdul-Ahad**

[amir\\_st\\_ephan@yahoo.ac.uk](mailto:amir_st_ephan@yahoo.ac.uk)

**R. S. Qahwaji**

[R.S.R.Qahwaji@Bradford.ac.uk](mailto:R.S.R.Qahwaji@Bradford.ac.uk)

Department of electronic Image and Media Communication–  
School of Informatics, Bradford University,  
Richmond Road, Bradford BD&1DP,U.K.

## ABSTRACT

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 paper proposes a multidimensional encryption algorithm for security in computer networks. 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 can also be used for decryption with different and extra complexities. Categories and Subject Descriptors: C[computer system organization],C.2 [computer communication networks], C.2.0 [general] General Terms: security

**Key Words:** 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 [3]. The data security of Internet aims at protecting the data from unauthorized intrusion is of paramount importance [4] [13]. Likewise, the security of multimedia data is essential for commerce protection [4] [1] [2].

Threat models normally pose negative ongoing effects due to their attacks diversity (Eavesdropper attack, Trojan horse attack, Man-in-the-middle messages to a third party. This communication process should not

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 [5] [11].

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

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 [6] [9].

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 [10] [8].

Accordingly, the objectives of this paper is 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**

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

Any message (i.e. a text file) can be divided into a group of eight lines, and each line to groups of eight words, and each word to 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 of the number of Lines, Words, Characters, and Binary. However, the choice of eight is time-effective (i.e. an optimization 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 [12].

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. This will be considered later in sections 2.4, and 4.

### 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 Fig (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.

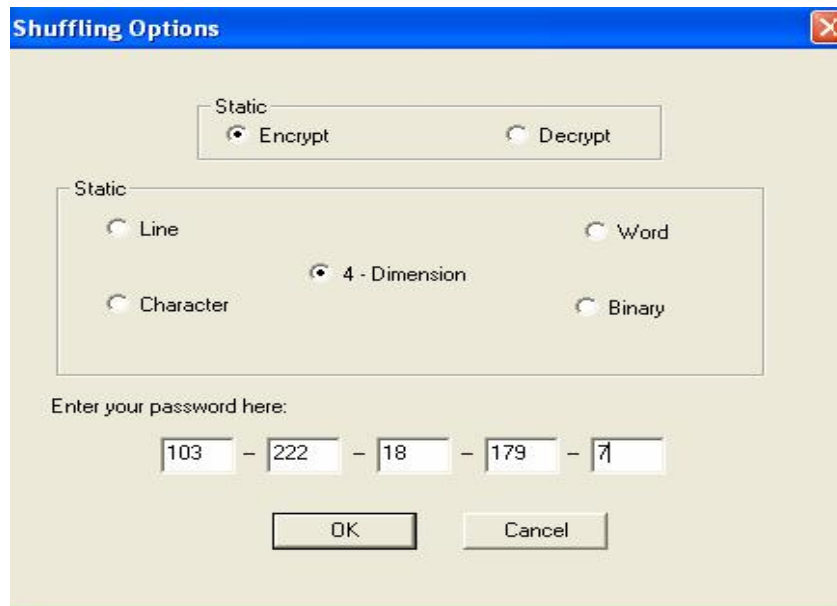


Fig (1): Selection of dimension and secret key management.

#### 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 Fig (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 Fig (3). This process is repeated until all 8-line groups of the text are encrypted in different and specific scramble code for each group.

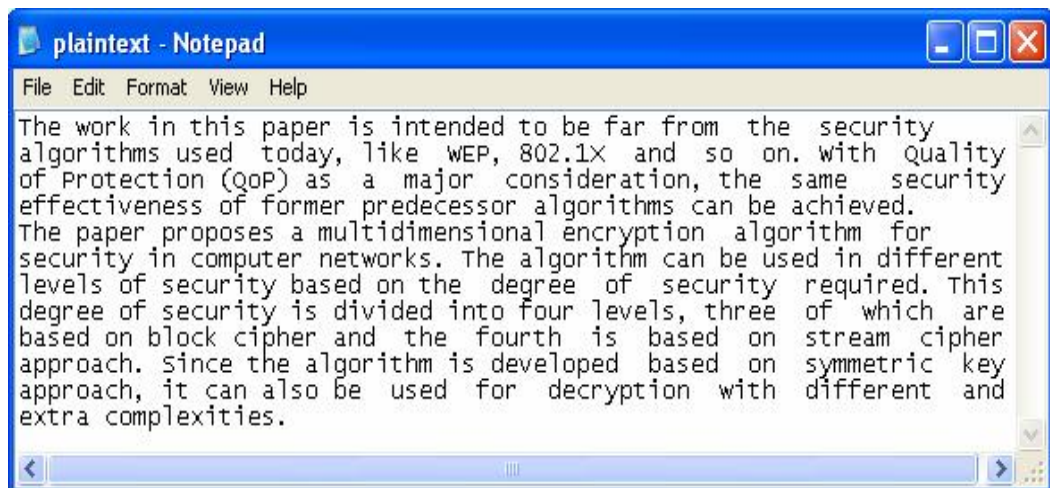


Fig (2): Plaintext.

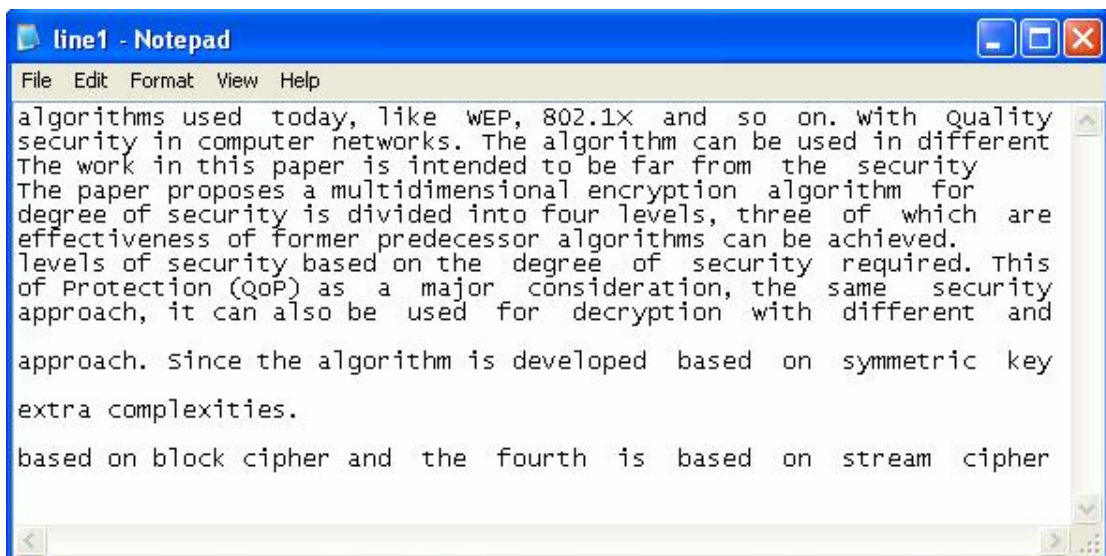


Fig (3): Applying Line encryption to the text of Fig(2).

### 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 Fig (4). Note that in this example the word dimension encryption is applied to the original plaintext file as shown in Fig (2).

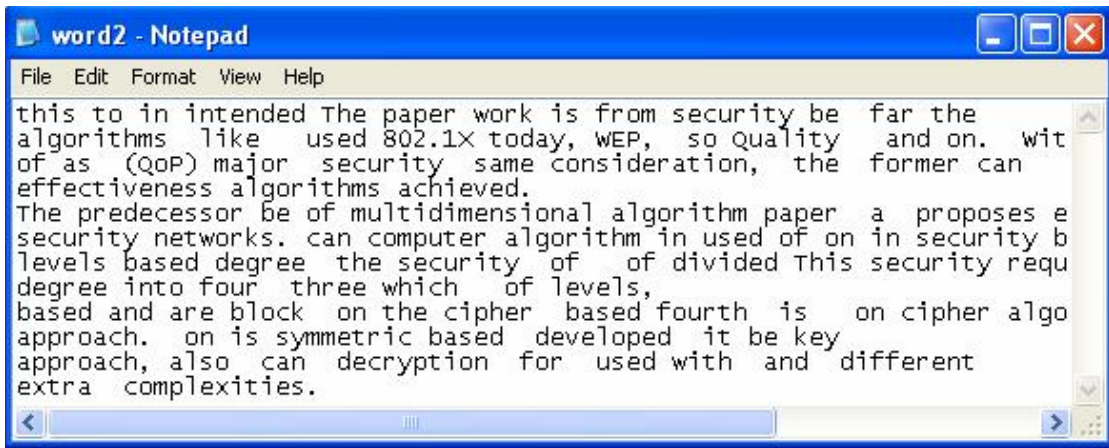


Fig (4): Applying Word encryption to the text of Fig(2).

### 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 Fig (5). Note that the character encryption dimension is applied to the original Plaintext file as shown in Fig(2).

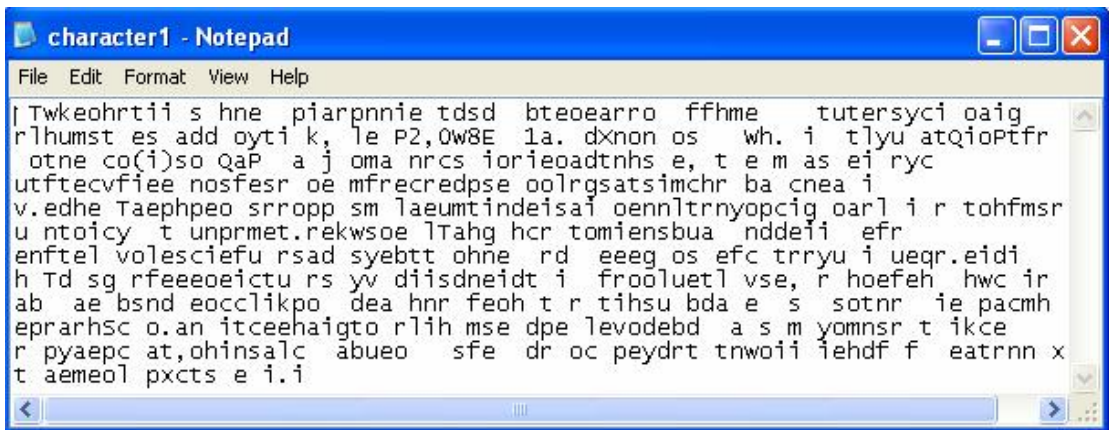


Fig (5): Applying Character encryption to the text of Fig(2).

### 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 Fig (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 Fig (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 Fig (7). This subject will be discussed in more detail in the next paragraph.

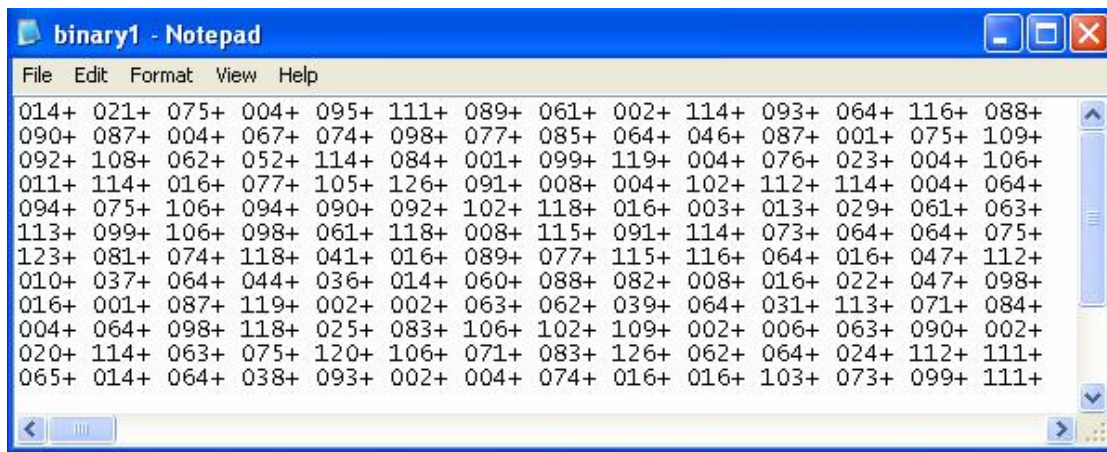


Fig (6): Applying Binary encryption to the text of Fig(2).

#### 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 (  $16 * \text{Math.pow}(256,4) * \text{Math.pow}(8!,4) = 1.8 * 10^{29}$ ).

-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 underlied 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 Fig (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 strength of the algorithm does not depend solely on the length of the key, but also on

encryption including both block and stream ciphering. Finally, as a consequence to these aspects, the dimension(s) used in the encryption process.

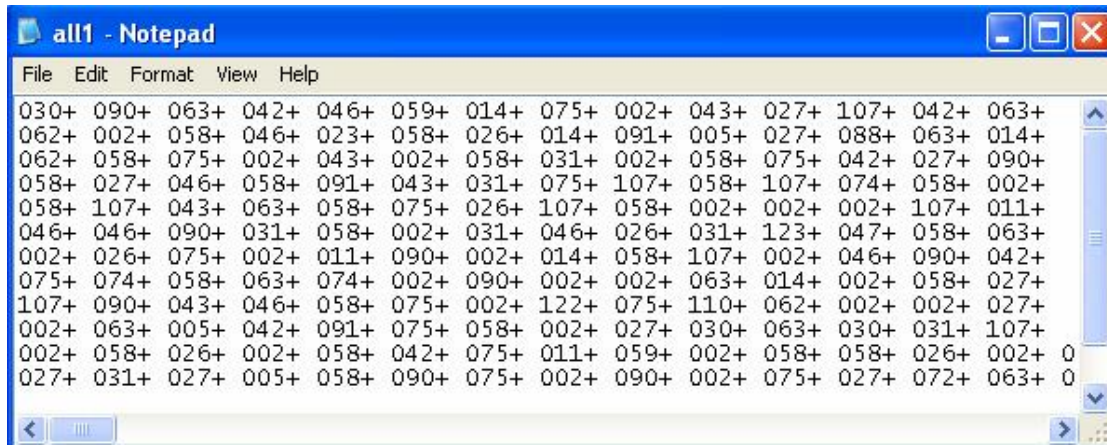


Fig (7): Four dimensions encryption of Line, Word, Character, and Binary in combination of the original Plaintext.

## 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

1. SALLI, K. T., HAMALAINEN, T., AND KNUUTILA J., AND SAARINEN,

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.  
 2. LO, C.C., AND CHEN, Y. J., 1999. Secure Communication Mechanisms for GSM Networks. IEEE Trans. Consumer Electronics, vol. 45, pp. 1074-1080.  
 3. YU, H. H., KUNDUR, D., AND LIN C. Y., 2001. Spies, thieves, and the battle for multimedia in the digital era", IEEE multimedia, vol. 8, no. 3, pp. 8-12, July-Sept. 2001.  
 4. DITTMAN, J., WOHLMACHER, P., AND NAHRSTEDT, K., 2001. Using Cryptographic and Watermarking Algorithms, IEEE Multimedia, vol. 8, no. 3, pp. 54-65, July-Sept. 2001.  
 5. "Wireless LAN Security: What Hackers Know That You Don't", AirDefence, Inc. 2004.

- 6.** STALLINGS, W.,1998 , Cryptography and Network Security", Prentice-Hall, 1998.
- 7.** "Securing Enterprise Data: Extensible Protection for Data, Applications and Hosts", VORMETRIC, Inc. 2004.
- 8.** SHAMIR, A.,1997. How to Share a Secret, Communications of ACM, vol. 22, no. 11, pp. 612-613,.
- 11.** PEIKARI, C., AND FOGIE, S., 2003. Maximum Wireless Security, SAMS Publishing.
- 12.** ANDERSON, R. J., 2001. Security Engineering: A Guide to Building Dependable
- 9.** SIMMONS,G. J., 1990.How to (really) Share a Secret, Advances in Cryptology-Crypto '88 Proceedings, Springer-Verlag, p. 390-448.
- 10.** BRENTON, C., AND CAMERON, H.,2003.Networking Security, Sybex Distributed Systems, John Wiley & Sons, Inc.
- 13.** FORTA, B., AND LAUVER, K.,ET.AL., 2000.WAP Development with WML and WMLScript, by SAMS Publishing.