Generation of Random Key Stream using Word Grid Puzzle for the Applications of Cryptography

T.SIVAKUMAR[1], S.VEERAMANI[1], T.ANUSHA[2]

[1]Department of Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology
Pollachi, Coimbatore, Tamilnadu-642003, INDIA

[2]Department of Computer Science and Engineering
PSG College of Technology, Coimbatore, Tamilnadu-641004, INDIA

Abstract: The amount of digital data created and shared via internet has been increasing every day. The number of security attacks and threats has been increased due to poor selection of secret keywords and passwords.Cryptographic algorithms and security protocols are primarily rely on random keys to provide security services.Random numbers and key stream are playing major role in applying the security mechanisms in real time. In this paper, a novel method to generate random key stream using word grid puzzle is proposed.The proposed method is experimented and a minor analysis has been performed in the obtained result.

Keywords: Cryptography, security protocols, Password, Random key stream, Word grid puzzle
Received: May 10, 2020. Revised: February 24, 2021. Accepted: February 26, 2021.
Published: March 2, 2021.

1. Introduction

With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in storage and transmission of digital data [5]. Cryptography is the practice and study of techniques for providing secure communication over an insecure channel [2].In network security, cryptography has a long history by providing a way to store sensitive information or transmit it across insecure networks (i.e. the Internet). The strength of any cryptosystem and security mechanisms are mainly depends on selection of unpredictable random keys.

Diffusion and confusion are the two major building blocks for any cryptographic system. Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible[1, 6]. Symmetric key algorithms are well accepted in the modern communication network. The advantage of symmetric key cryptography is that the key management is very simple. In case of symmetric key method, the key should never be revealedto other users and should be kept secure. The key should be known to sender and the receiver only and no one else [4].Depending on the nature of the randomness source, generators are classified in two categories as follows [6].

A. True random number generators (TRNG), where the source is a natural physical phenomenon and the properties of independence and unpredictability of the generated values are guaranteed by physical laws.

B. Pseudo random number generators (PRNG), where the source of randomness is a random initial value, called seed, which is expanded by means of a deterministic recursive formula, providing a modality for generating random sequences using only software methods.

In this paper, a novel method to generate random key stream with word grid puzzle is proposed.

The rest of the paper is organized as follows: Section II provides the literature survey, Section III briefs about proposed random key generator. Section IV presents the experimental results and analysis. The paper is concluded in Section V.

2. Literature Survey

Each and every encryption algorithm may be block cipher or stream cipher. Both types typically need a random key to achieve its purpose. However, stream cipher needs random key stream of length equals to the information to be encrypted. Cryptanalysis techniques like linear cryptanalysis, n-gram analysis, meet in the middle attack, brute force attack, man in the middle attack are usually performed to identify the secret key [2]. The efficiency of the ciphers are being depends on their throughput and memory requirement. Using of large key spaces with several numbers of rounds with multiple complex operations provide needed security[3].

Users rarely choose passwords that are both hard to guess and easy to remember. To determine how to help users choose good passwords, in [7], the authors performed a controlled trial of the effects of giving users different kinds of advice.

Some guidelines to choose a best password are [passwordgenerator.net]: use a password that has at least 16 characters, use at least one number, one uppercase letter, one lowercase letter and one special symbol. Do not use postcodes, house numbers, phone numbers, birth dates, ID card numbers, and social security number in your passwords. Do not store your critical passwords in the cloud. Encrypt and backup your passwords to different locations.

To provide timely feedbacks to users, every Internet service now imposes a password strength meter (PSM) upon user registration or password change. It is a rare bit of good news in password research that well-designed PSMs do help improves the strength of user-chosen passwords. When choosing passwords for a new web service, most users (77.38%) simply retrieve one of their existing passwords from memory and then reuse (or slightly modify) it [8]

The randomness comes from atmospheric noiseis better than the pseudo-random number algorithms typically used in computer programs. The best data security practice is not to let anyone but yourself generate your most important passwords [random.org]. A method for the human-assisted generation and application of pseudo-random keysfor the purpose of encoding and decoding digital watermarks to and from a digitized data streamis proposed in [US5822432A].

In [9], the authors presented a multilayer image encryption and decryption using random puzzle based method to embed secret data into the cover image. This approach enhances the security and provides robust embedding. An 8×8 Sudoku puzzle which has a 64×64 reference matrix is utilized. The method gives a superior average capacity of 5 bits per pixel. The message is embedded at the sender using random permutation puzzle. At the Receiver end, the user has to rearrange the image thereby solving the puzzle.

In [10], a steganography method based on data embedding is introduced by using Sudoku solution matrix. In this scheme RGB value of Cover-image contains both secret information and key (Sudoku). RG component contains Secret information and B component contains key value. Same Sudoku solution matrix is used for embedding and extraction phase.
The word grid puzzle is ann×n matrix which contains words in a jumbled manner. In the proposed method, a novel method to generate random key streamwith word grid puzzle is proposed.

3. Proposed Random Key Stream Generator

This section presents the overall working model of the proposed random stream generation process. Random key stream generation involves two requirements. First requirement is the word grid puzzle which is n×n matrix and it consists of words in a jumbled manner. Second requirement is the words that are to be searched in the given word grid. Once the words to be searched in the word grid is found then the particular cells in the grid is alone made as 0 or -1. This indicates that the concerned cells are visited.Further, various kinds of 2-D array scanningare performed on the grid to generate different random key streams of various length.

The sequence of operation involved in generating random key stream using word grid puzzle is shown in Figure 1.

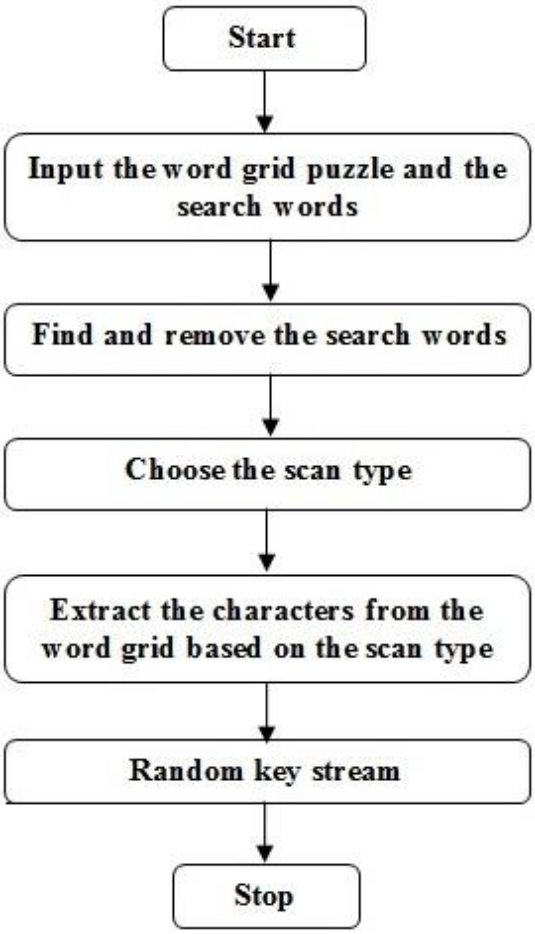

Figure. 1 Flowchart of proposed random key stream generation

3.1 Algorithm for Random Key Stream Generation

In this section, the sequence of steps involved in generation of random key stream is given.

Input: Word grid puzzle, Search words, Scan type **Output:** Random key stream

Step 1: Start the process.
Step 2: Input the word grid puzzle and the corresponding search words.
Step 3: Find and remove the search words.
Step 4: Input the matrix scantype.
Step 5: Extract characters from the word grid based on the chosen scantype.
Step 6: Store the obtained characters as random key stream.
Step 7: Stop the process.

3.2 ScanTypes

Scan is the process of traversing all the cells of a 2-D matrix in a sequential pattern. The traversals can be an odd position scanning, even position scanning, snake scanning, zig-zagscanning, diagonal scanning, spiral scanning, etc. The sample scanning types are briefed below:

- **Odd scanning:** To generate random key streams by using the characters present in the odd locationin the grid.
- **Even scanning:** To generate random key streams by using the characters present in the even locationin the grid.
- **Diagonal scanning:** To generate random key streams by using the characters present in the diagonal locationin the grid.
- **Zig-Zagscanning:** To generate random key stream by using the characters present in the zigzag locationin the grid.
- **Mid left:** To generate random key streams by using the characters present in the middle and towards the beginning of the grid. Similarly, Mid right.
- **Upper triangular scanning:** To generate random key streams by using the characters present in the upper triangular of the grid. Similarly, Lower triangular scanning.

The size of key stream that are to be generated from the grid depends on the size of the key mentioned in the algorithm. For instance, if the chosen algorithm is Data Encryption Standard, the 64 bits will be derived. Also, the kind of scanning and volume of the key stream are depends on the understanding between the sender and the receiver.

3.3 Illustration for the Proposed Method

In this section, the proposed random key stream generation method is illustrated with a sample word grid puzzle. The sample word grid is shown in Table 1. The search words of the word grid are Intellect, Infinity formula, Elite, Paratrooper and Integrity.

Table 1.Sample Word Grid

Q	B	D	H	I	Y	X	A	P	O	L	M	I	F	T	Y
D	A	P	U	L	M	K	G	F	E	F	S	N	H	D	B
S	C	N	Q	P	T	G	A	G	Y	O	A	F	U	T	G
G	N	F	R	O	G	S	G	T	Q	A	Q	I	I	C	Z
B	M	J	H	L	C	A	I	P	G	L	B	N	P	E	C
M	T	K	J	M	N	R	X	S	X	D	N	I	I	L	D
D	F	W	U	Z	G	D	B	O	J	E	Y	T	N	L	J
B	L	T	P	E	N	S	F	K	X	L	R	Y	R	E	Q
Y	J	U	T	Z	M	R	R	J	Y	I	U	F	F	T	P
U	B	N	D	B	I	B	S	H	M	T	O	O	U	N	L
P	I	I	B	J	T	Y	H	S	V	E	L	R	D	I	V
O	X	V	M	F	E	X	X	E	L	U	P	M	G	U	X
P	A	R	A	T	R	O	O	P	E	R	A	U	Q	Y	R
W	Z	Z	C	Q	H	Q	H	Y	D	U	Q	L	O	I	W
F	R	V	V	G	P	Z	O	M	H	M	I	A	D	H	U
A	T	B	N	O	P	R	H	F	M	Z	N	D	T	J	A

Table 2.Word Grid after Highlighting the Search Words

Q	B	D	H	I	Y	X	A	P	O	L	M	I	F	T	Y
D	A	P	U	L	M	K	G	F	E	F	S	N	H	D	B
S	C	N	Q	P	T	G	A	G	Y	O	A	F	U	T	G
G	N	F	R	O	G	S	G	T	Q	A	Q	I	I	C	Z
B	M	J	H	L	C	A	I	P	G	L	B	N	P	E	C
M	T	K	J	M	N	R	X	S	X	D	N	I	I	L	D
D	F	W	U	Z	G	D	B	O	J	E	Y	T	N	L	J
B	L	T	P	E	N	S	F	K	X	L	R	Y	R	E	Q
Y	J	U	T	Z	M	R	R	J	Y	I	U	F	F	T	P
U	B	N	D	B	I	B	S	H	M	T	O	O	U	N	L
P	I	I	B	J	T	Y	H	S	V	E	L	R	D	I	V
O	X	V	M	F	E	X	X	E	L	U	P	M	G	U	X
P	A	R	A	T	R	O	O	P	E	R	A	U	Q	Y	R
W	Z	Z	C	Q	H	Q	H	Y	D	U	Q	L	O	I	W
F	R	V	V	G	P	Z	O	M	H	M	I	A	D	H	U
A	T	B	N	O	P	R	H	F	M	Z	N	D	T	J	A

Further, find the search words in the word grid and the word grid after removing the search words is shown in Table 2. The remaining characters present in the word grid (matrix) are utilized to generate random key streams.Also, different types of

scanning are can be performed in the grid to generate random key streams of any required size. Each scanning paves way for a unique key stream for the same grid.

The random key streams obtained by using few of the scan types are given below:

- **Key stream obtained using odd scan:**
  QDIXPLITDPLKFFNDSNPMGOF
  TGFOSTAICBJLAPLNEMKMRSD
  ILDWZDOETLBTESKLYEYUZRJ
  IFTUNBBHTONPIJYSERIOVFXE
  UMUPRTOPRUYWZQQYULIFVG
  ZMMAHABORFZDJ
- **Key stream obtained using Zig-Zag scan:**QBDHIYXAPOLMIFTYBDH
  NSFEFGKMLUPASCNQPTMAGY
  OAFUTGZCIIQAQTGSGORFNB
  MJHLCAIPGLBNPECDLIINDXSX
  RNMJKTDFWUZGDBOJEYTNLJ
  QERYRLXKFSNEPTLYJUTZMRR
  JYIUFFTPLNUOOTMHSBIBDNB
  PIIBJTYHSVELRDIVXUGMPULE
  XXEFMVXPARATROOPERAUQ
  YRWIOLQUDYHQHQCZZFRVV
  GPZOMHMIADHUAJTDNZMFHR
  PONBT
- **Key stream obtained using spiral scan:**QBDHIYXAPOLMIFTYBGZ
  CDJQPLVXRWUAJTDNZMFHRP
  ONBTAFWPOPUYBDMBGSDAP
  ULMKGFEFSNHDTCELLETNIUY
  IHDAIMHMOZPGVVRZAXIBJLF
  TMNCNQPTMAGYOAFUIPINRF
  UDGQOLQUDYHQHQCZRVINU
  TWKJFROGSGTQAQINITYFORM
  UAREPOORTAMBDTPUJHLCAIP
  GLBNYRUOLPULEXXEFJBZEZ
  MNRXSXDELITEVSHYTIMNGD
  BOJXYMHSBRSFKJR

Similar to this, various other types of scanning can be applied on the grid to generatedifferent and unique random key streams. Scan which produces less amount of bit streams can be utilized to generate keys for play fair, DES, and AES algorithms. Scan which produces more amount of bit streams can be utilized to generate keys for stream ciphers.

3.4Salient Features of the Proposed Method

The following are the salient features of the proposed method:

- The proposed method can be used to generate keys of variable size. Hence, it can be utilized to generate keys for both block and stream ciphers.
- The Word Grid puzzle and the words present in the grid are known to the communicating persons. It may not giveanysuspicion to the intruders/attackers about the purpose of sharing the puzzles.
- The overhead associated with key generation, key distribution and keeping the key secure can be reduced.
- The generated key stream can be used for padding, initialization vectors, and salt values, session keys, etc.

4. Experimental Results And Analysis

The proposed method is experimented using Python language and the system configuration isProcessor IntelCore i3 CPU, Clock speed 3.07 GHz, RAM 4GB and the operating system is Windows (64bit).The experimental result of the proposed method is given in Table 3for few scan types. From the result, it is observed that the bit stream is

random and hence suitable to generate keys for cryptographic applications.

Table 3. Experimental results of the proposed method

Scan	Random key stream in binary format
Odd	1010001100010010010011011000101000010011001001001101010010001001010000100110 01 0010111000110100011010011101000100101001110011101010000100110110001111001111 10 0011010101001001111110100111010100100000110010011000011100001010010101001100 100 0001101000010011001001110100010110011011001011100110110100101010011100010010 01 0011001100100010010101111011010100010010011111000101101010010011001000010101 01 0010001011010011100101110011001011001100010110110011010101101101010100101001 01 0100100110001101010100101010110011101000010100001010010001010100100111110011 10 1010000100100110010101011001101001110001011010010100100110011111010110100011 01 0110001000101101010110011011010101101000010100101010100100111110100001010010 10 1010110110011010111101101010100011010001101100110101011001100100100110001101 01 0110100011110110101001101100110110000011001000100000110000101001111101001010 00 1101011010100010010010 10
Zig-Zag	1010001100001010001001001000100100110110011011000100000110100001001111100110 01 0011011001001100011010101001111001100001010001001001000100111010100111000110 10 0010110001101000111100101110011011001100101010110100001000001101001110000111 00 1110101000110100001010100100110110000011000111101100110011111000001100011010 10 1011010100100011110110101000011100100110010011010001100000110100011010100100 01 1110100111000111100111110100101000110100111010000101001101100101010010001001 10 0100001110000011001001101000010001111001100100001010011101010000100010110000 11 1000100100110010010011001001100111010001001011000101001110110001010010100111 01 0011011001010100101110101001000100100011010101111010101101101010001111000100 10 0001010011111001010100010110110011010100100111010011001001010101000110001011 01 0010101100110100101001100101100010010111000110101001110011101000101101000010 10 1001001100101100110010101010101101010010110101001101101001010100101001010101 10 0110010011010101100011010001101010100101000010011001001110101010110011111001 11 1101010010011011001000101001110000101001001100001010001001001110100001010100 00 1001001100100110000101001010101010010110011001000101001110101101000101100110 01 0100101000100100100110101101011000101010110001111001101101000010101011001100 10 0010110110001011000100010110001101001101101011010110001010000100000110100101 00 0001101010010100101001111100111110100001000101101001010000011010101101000110 11 0011010010101011110010011001111100110010100011010101100010010110011001000101 00 0110010001010001100001110110101011010100011010100101010110101011010001111010 00 0101101010011111001101100100010011011001001100000110001001001000101010110000 01 1001010101010010001001001110101101010011011000110100100010100101010000100111 11 0011101000010101010 0
Upper triangle	1010001100001010001001001000100100110110011011000100000110100001001111100110 01 0011011001001100011010101001111001100000110100001010101100110010011011001011 10 0011110001101000101100011010100111001110100100010001001000010100111010100011 01 0000101010010011011000001100011110110011001111100000110001101010101101010010 00 1111010010100111110001111010011100011110101001010001100000110100011001001100 10 0110000111011010100110010000111000001100100110100001000111100110010000101001 11 0101000010001011000011100111010100101011000101001110110001000100100111010010 01 1001001100110010001001000100100001010011111001010100010110110011010100100111 01 0011001001010100011010010111011000100110010100101011001101001010001011010001 10 0101010110011001001101010110001101000110101010010100001001101101010010011111 00 1111101010110011101001100100010110011001010010100010010010011010110101000010 01 1011000111101010110110001010101101000110110011010010100111110010011010111100 10 001010101100000 1

The execution time taken to generatekey streams by using various scan types is given in Table 4. From the table, it is inferred that the execution time to generate the bit streams is vary less and hence it is suitable for real time applications.

Table 4. Execution time

S.No.	Scan type	Time take (seconds)
1.	Odd	0.4266
2.	Even	0.4489
3.	Zig-Zag	0.8353
4.	Spiral	0.8433
5.	Upper triangle	0.8746

5. Conclusion and Future Work

In this paper, a novel and simple method to generate the random key stream using Word Grid Puzzle is developed. The proposed method is a new notion to generate random key streams. The generated bit stream is random and the execution time is less than 1 seconds. This new methodology for generating key stream using Word Grid puzzle is an effective and secure method by confusing the attackers about the actual purpose of sharing the puzzles. In future, randomness testing is performed with NIST SP 800-22 test cases to access the randomness of the proposed random number generator. To apply the generated random numbers to encrypt/decrypt images.

References

[1]. C. Shannon, “Communication Theory of Secrecy Systems”, Bell Systems Technical Journal, Vol. 15, pp. 57-64, 1998.

[2]. Natarajan, Sairam, ManikandanGanesan, and Krishnan Ganesan, “A novel approach for data security enhancement using multi-level encryption scheme" International Journal of Computer Science and Information Technologies, Vol. 2, no. 1, pp. 469-473, 2011.

[3]. S G Srikantaswamy and H D Phaneendra, “Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption”, International Journal on Cryptography and Information Security, Vol. 2, No. 4, pp. 39-49, December 2012.

[4]. SomdipDey, JoyshreeNath and AshokeNath, “An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm”, International Journal of Computer Applications, Vol. 46, No. 20, pp. 46- 53, May 2012.

[5]. T. Sivakumar and T. Anusha, “A New Symmetric Cryptosystem using Randomized Parameters of SHA-512 and MD5 Hash Functions”, International Journal of Innovations in Engineering and Technology, Vol. 6, No. 4, pp. 600-606, April 2016.

[6]. William Stallings, “Cryptography and Network Security-Principles and

Practice", Pearson Education, New Delhi, 2013.

[7]. J. Yan, A. Blackwell, R. Anderson, A Grant, "Password memorability and security: empirical results, IEEE Security & Privacy, Volume: 2, Issue: 5, pp.25-31, Sept.-Oct. 2004.

[8]. Ding Wang, Debiao He, Haibo Cheng, Ping Wang, "fuzzy PSM: A New Password Strength Meter Using Fuzzy Probabilistic Context-Free Grammars", *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) July 2016*, France, pp. 595-606, 2016, ISSN 2158-3927.

[9]. Siva ShankarS and Rengarajan A, "Puzzle based Highly Secure Steganography", IEEEInternational Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, India, pp. 16-18 Feb. 2017.

[10]. Suman Chakraborty and Samir K Bandopadhyay, "Steganography Method Based on Data Embedding by sudoku solution Matrix", International Journal of Engineering Science Invention, Vol. 2, No. 7, pp.36-42, 2013

[11]. https://www.random.org/passwords/

[12]. https://passwordsgenerator.net/

[13]. Method for human-assisted random key generation and application for digital watermark system, US Patent US5822432A.