New Programmatic OTP Algorithm

New Programmatic OTP Algorithm

Dr. Sahar Adill Kadum[1], Shaimaa Mehdi kadum jawad[2]
[1]College of Science for Women, University of Babylon, lraq
[2]College of Science for Women, University of Baghdad, lraq.

[1]E-mail: dr.sahar.adill@gmail.com
[2]E-mail: shaimayosif78@gmail.com

Abstract. The huge improvement in the field of data innovation and the web presentation to a surge of infringement to go around and take data, the earnest requirement for the development of information assurance advancements and information encryption procedures. A new Programmatic OTP Algorithm using an unsystematic key generation for ciphering plaintext presented in this paper. This method, based on create randomly a number (n) called add number, where the plaintext characters converted to a binary form and splits into equal parts according to n value with 2n ciphering keys generated. The keys will be distributed on these parts to get ciphered text. Accordingly, one of these keys its generation number will be set for all different n's. The different n's occurred Consecutively to the number of characters consist the plain message unlike the traditional OTP algorithm. This method characterized by a facility that the same generated key can produce different ciphering text using 2n probability. The proposed methodology has been proved as perfect ciphering method compared with OTP using statistical tests

Keywords: Cryptography, Symmetric–key, Asymmetric-key, One-Time-Pad (OTP) algorithm, Unsystematic algorithm.

1. Introduction

Security is essentially the concern of all in all research areas, as it plays a significant role in securing data and information. In order to maintain their data and information secure from intruders and hackers, cybersecurity is a big challenge. Because of the cost involved and the lack of specialists, securing data has become very difficult to manage. Protection is the process that protects data from alteration, degradation, unintended or unauthorized access to data. [1].

With the Internet attaining a degree that merges with our lives, explosively rising over the past few decades, data protection has become a major concern for everyone linked to the internet. Data

protection ensures that our data is available only to the intended user and prohibits data from being changed or altered. To attain the degree of protection, diverse algorithms and methods were developed such as cryptography. Cryptography (a Greek word meaning "hidden writing") is the technique and art of transforming messages in order to make them encrypted and resistant to attack. Cryptography can be described as data encryption techniques based on various algorithms that make the data unreadable to the human eye unless decrypted by the predefined algorithms of the sender [2,3].

This research deals with a new method of encryption that considered to be compared with the OPT. the research organized in to previous research, discuss cryptography discipline, the OTP algorithm, proposed system, and results.

2. Related Work

Many researches have been proposed different techniques and approaches for protect information such as:

Mohammad and Qahtan, et.al. [4], Explains basic knowledge of cryptographic algorithms and contrasts classical cryptographic algorithms with modern cryptographic algorithms based on a variety of criteria, such as key size and technical uniqueness and vulnerability.

Nithin and Vivek, et.al. [5], Suggested new concept of OTP encryption by treating message bits as True / False statements about the pad defined as a private property. Adding messages by testing the secret object declarations and demonstrating that the length of the transmitted OTP containing valuable information does not need to be compromised and can be shorter than the length of the message without sacrificing absolute confidentiality.

Maksim and Zura [6], added new updates to OTP, where the main issue is with the single sword panel such that the inclusion of the one-time switch. The encryption is not secure if the key is used to encrypt more than one message by carrying out the work on reducing the size of the cypher; they have already solved a major onetime problem. Yet it should be remembered that there is not full secrecy in the scheme.

Abiodun and Aman, et.al. [7], Suggested new one-time pad (OTP) algorithm method to allow the same key to use various plain text encryption without revealing any pattern to solve key management, distribution issue of having to send a new key whenever a message is to be transmitted, enabling the one-time pad system to be feasible and enabling as many as the same key generated during encryption to be reusable.

Saad, Ali, and Ammar [8], A security database encryption algorithm called TSFS (Transposition, Substitution, Folding, and Shifting) was suggested to resolve the character set limitations and the number of keys used. The proposal was based on improving the phases of the TSFS encryption algorithm by computing the key matrix determinant that affects the algorithm phase implementation.

3. Cryptography

Cryptography is the science for encryption and decryption, with the goal that the data is made sure about the wonder for the sender and the collector just, it will likely confidentiality, integrity and authenticity. It becomes essential apparatus for protecting the exchange of data between online systems with complete mystery. The two essential systems for encoding information are: "symmetric cryptography", which involves the use of a similar key to encrypt/ decrypt information; and “asymmetric cryptography”, which utilizes public and private keys to encrypt/ decrypt information [9].

3.1. Symmetric – key cryptography

The symmetric – key cryptography calculations might be called traditional algorithms, the encrypting and decrypting keys are equivalent subsequently named secret keys or secret-key algorithms likewise called (Single key encryption, Private-key encryption, Symmetric-key encryption, One-key encryption). The encryption key can be developed out of the decryption key or other way around. These sorts of calculations will in general be snappy and less asset concentrated in encryption and decoding. AES, CAST, DES, triple DES, and Blow fish are instances of symmetric algorithms. Symmetric algorithms are separated into two classifications: stream cipher OTP one of stream cipher instance and block ciphers relying upon the handling of discourse tests [9].

3.2. Asymmetric -key cryptography

These encryption algorithms are called public key algorithms because of the public accessibility of their encryption keys. Various keys are utilized for encryption and decryption in asymmetric. It is extremely hard to get the decryption key from the encryption key. The encryption key is public, while the decryption key is private so as to maintain a strategic distance from anybody from decrypting the secret message so just the recipient can decrypt it, "key-sets" can be made accessible inside a system to encourage the user to have both public and private keys. The public key is planned accessible to everybody with the goal that anybody can send messages, however the private key is just made accessible to the individual it has a place with. One of its significant burdens is more slow speed, when contrasted with symmetric algorithms. RSA, DSA, and PGP are instances of asymmetric algorithms [9, 10, 11].

4. One Time Pad (OTP) Algorithm

A binary added substance stream cipher is the One-Time- Pad encryption technique, where a stream of truly arbitrary keys is created and then joined by a 'exclusive OR' (XOR) addition with the plain text for encryption or with the cipher text for decryption. It is conceivable to prove that if the associated preconditions are met, a stream cipher encryption method is unbreakable. [12]:

- Key length is equal to the length of the plain text.
- The key is arbitrary.
- The key utilized once.

Two by two is used for the OTP encryption method keys. Each consumer retains one duplicate of the key and the keys are safely disseminated until encryption. Consistent protection during their dissemination and capability guarantees the security and validity of the One Time Pad keys. This means that untouchables will not be able to misuse the key.. With OTP encryption, the key utilized for encoding the message is totally arbitrary with a length of the message itself. That is the reason the main conceivable assault to such a figure is a beast power assault.

Decryption process characterized by plain text = key ⊕ iphered text. On the off chance that the key stream digits are created freely and arbitrarily, the cipher is known as a one-time cushion and is genuinely secure against a cipher text-only attack [12].

5. Proposed Methodology

The proposed method is a symmetric cipher category called unsystematic key generation ciphering algorithm. Unsystematic generation method depends on generating a random number n for each character in the plain text. For each n there will be 2^n probability generated key, the selected key its order number will be sets to all the generated keys of the reset n's characters of the plain text. In other word, each character has its own n and 2^n probability generated key but with a same order number to all n's. The proposed methodology is illustrated in (1, 2, and 3) algorithms.

Algorithm (1): Unsystematic Cipher Encryption Process

Input**:** plain text (message)
Output**:** cipher text, l, n.
Step 1: compute l (message length) from plain text
Step 2**:** obtain ASCII value of each character in the plain text.
Step 3: convert the ASCII values to a binary form.
Step 4: According to n generate add number (n) using algorithm (2).
Step 5: The binary stream of plain text will be divided into equal parts of n base.
If these partitions cannot divide into equal parts then
Build the parts in descending order, i.e. begin with parts contain much bits then less then less until distribute all the bits as a parts to reach to a balanced division.
Step 6**:** distribute the generated keys on step 5
Step 7: if the added part end with bit "0" then involved part will remains as it
Else
added part end with bit "1" then involved part will be complemented

5.1. Ciphering Key Generation Algorithm

The number of generated keys must equal to the number of characters consist the plaintext. As the number of n's is large the more complicated process. In this situation, the solution becomes harder and the security increases. Algorithm (2) illustrates unsystematic key cipher generation.

Algorithm (2): Unsystematic Cipher Key Generation

Input: length of plain text (l)
Output: ciphered keys.
Step 1: read the l value
Step 2: Generate added number (n) according to l using Random function. The added number n must be in the interval $1 \leq n \leq l$.
Step 3: according to n value there will be 2^n probability of ciphered keys.
Step 4: select one of these probability of a specific n. The order number of a selected probability will be sets for all reset n's probabilities of other characters.

Algorithm (3): Unsystematic Cipher Decryption Process

Input: cipher text, n, l.
Output: plain text
Step 1: Read the value of n, l.
Step 2: Generate decoding keys according to n value using algorithm (2).
Step 3: Distributed the ciphered text of a specific key probability to retrieve the plain text.

Note: the specific key probability known for sender and receiver parties according to an agreement protocol between them.

Case Study

To encrypt the message "hello my world" using unsystematic algorithm:
- Generate add number n randomly using random function.

- Generate ciphered key of length (n) with (2^n) key probabilities. Each character in the message 'Hello my worlds' has (2^n) probabilities for each n. Table 1, illustrates the unsystematic encryption process.

Table 1. Encryption processes with key of 2^r probability.

Plain text	Cipher text	Generated Ciphering Key
Hello my world	10000101101101101110001011101010100000101011000110111011010001010110110011101011110110011101101011010010101111111011011100010001101000101011010100111001101010000110101100110111	67476825716451

A set of statistical tests and National Institute of Standards and Technology (NIST) are used for measure the generated key randomness, these procedures are useful in detecting deviations of a binary sequence from randomness. These tests are included for deciding whether the binary sequence are really random sequence [12]. The statical tests used in this paper are Frequency (Monobit) Test, Frequency Test within a Block, Linear Complexity Test, and Runs Test [13]. Table 2, shows the statistical tests results using unsystematic key generation algorithm.

Table 2. Statistical Test Results using Unsystematic Algorithm.

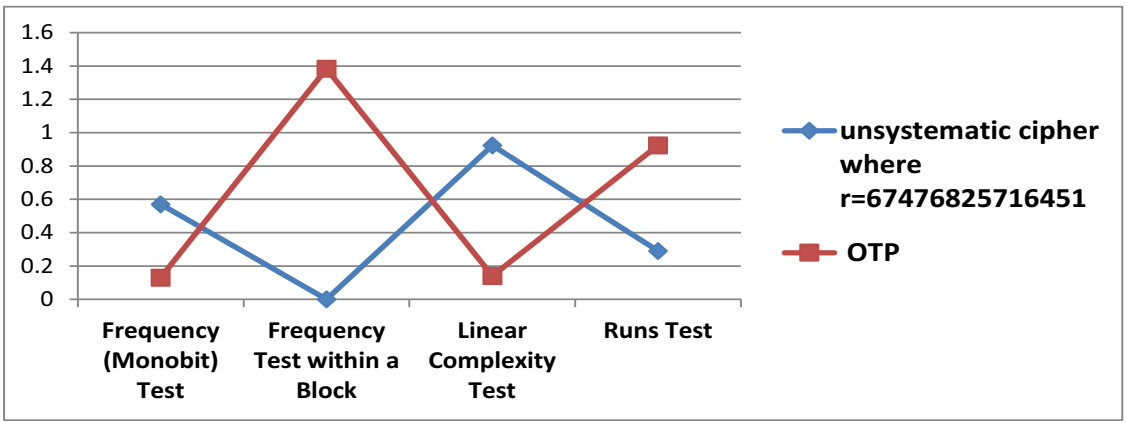
Statistical Test	Results
Frequency (Monobit) Test	0.570750388058174
Frequency Test within a Block	0.000126626169982884
Linear Complexity Test	0.923490427213445
Runs Test	0.289568624112342

While, creation of One-Time Pad key that depends on the selected key chosen randomly. Applying the statistical tests of OTP shown in table 3.

Table 3. Statistical Test Results for OTP.

Statistical Test	Results
Generte one Time Pad	bPp54IiXwl1QEe
Frequency (Monobit) Test	0.130570018115736
Frequency Test within a Block	1.38363372115078
Linear Complexity Test	0.139700565012938
Runs Test	0.923490427213445

Figure 1, illustrate the comparison between the proposed method and OTP.



Figures 1. Statistical Tests Comparison of Unsymmetrical Cipher Algorithm with OTP.

6. Conclusion

The primary commitments benchmark of Unsystematic Algorithm approach is concluded as follows:

1- The new method is progressively worthwhile in expanding the arbitrariness ciphering key to retrieve the plain text. Different keys are generated based on mathematical solutions.
2- Each character is encoded with various private keys. This gives significant level of security, and effective unpredictability.
3- The randomness of generated add numbers makes the encryption procedure hard to break.
4- This algorithm provides confidentiality, authentication, data integrity, and access control.

Future Work

The proposed algorithm can be implemented in storing the data cloudy. Also, the plain text extended to include images, videos, audio, etc.

References

[1] Adnan Noor, 2011, Modifying Hebbian Network For Text Cipher, Baghdad Science Journal, Vol.**8** (4).
[2] E Abdullah Kawther, Hussein Nada; 2018, A Secure Enhancement For Encoding/Decoding Data Using Elliptic Curve cryptography, Iraq Journal Of Science, Vol **59**, No.1a, pp. 189-198.ISSN:0067-2904.
[3] A Abdulameer Saad, H Kashmar Ali, et al, 2020, A Cryptosystem For Data Security Based On TSFS Algorithm, Baghdad Science Journal ,P-ISSN:2078-8665,E-ISSN:2411-7986, Open Access, Vol. **17** (2), pp. 567-574.
[4] Ubaidullah. Mohammed, et.al;" A Review on Symmetric Key Encryption Techniques in Cryptography"**,** International Journal of Computer Applications, Volume 147 – No.10, August ,2016.

[5] Nagaraj Nithin, et.al, 2016, Re-visiting the One-Time Pad", nithin@nias.iisc.ernet.in,pgvaidya@nias.iisc.ernet.in, http://www.geocities.com/nias,GlobalResearch,Bangalore, INDIA.

[6] Iavich Maksim, Kevanishvili Zura, 2018, MODIFIED ONE TIME PAD**,** Scientific and Practical Cyber Security Journal ISSN: 2587-4667.

[7] Esthe Abiodun, 2018, An Enhanced Practical Difficulty of One-Time Pad Algorithm Resolving the Key Management and Distribution Problem, Proceedings of the International Multi Conference of Engineers and Computer Scientists, Vole I IMECS 2018, Hong Kong, March pp.14-16.

[8] Abdulameer Saad A., Kashmar Ali H., et al, 2020, A Cryptosystem for Database Security Based on TSFS Algorithm, Open Access Baghdad Science Journal, P-ISSN: 2078-8665, Vol. **17**(2), pp: 567-574, E-ISSN: 2411-79860.

[9] Alemami Yahia, Mohamed Mohamad Afendee, Atiewi. Saleh, 2019; Research on Various Cryptography Techniques, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-**8**, Issue-2S3.

[10] Agrawal.Monika, Mishra. Pradeep, 2012, A Comparative Survey on Symmetric Key Encryption Techniques, International Journal on Computer Science and Engineering (IJCSE), Vol. **4**, No. 05.

[11] Mijanur R., Tushar K., et al, 2012, Implementation of RSA Algorithm for Speech Data encryption and Decryption, International Journal of Computer Science and Network Security, vol. **12**, no. 13, pp. 74-82, Mar. 2012.

[12] Otto Kugler CEO, mils electronic gesmbh & cokg | leopold-wedl-strasse 16 | 6068 mils | Austria. ,https://www.cryptomuseum.com/manuf/mils/files/mils_otp_proof.pdf

[13] Rukhin Andrew, Soto .Juan, et.al; 2010, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application', NIST Special Publication 800-22 Revision 1a.