An Enhanced Practical Difficulty of One-Time Pad Algorithm Resolving the Key Management and Distribution Problem

Abiodun Esther Omolara [1], Aman Jantan [2], Oludare Isaac Abiodun[3], Humaira Arshad[4]

Abstract— Information theory and cryptography recognize 'One-Time Pads' as 'Perfect Secrecy' in theory, however, until today, they have remained impractical to use because of its key management and key distribution problems, particularly in having to generate and send a new key each time you need to transmit a message. When a key is used more than once in the One-Time Pad encryption scheme, it becomes vulnerable to a pattern analysis attack (known-Plaintext attack). For this reason, the same key must not be used more than once.This problem can be resolved by modifying the algorithm and enhancing the key so that any statistical relationship between the plaintext and ciphertext will be completely concealed. The methodology employed was a combination of some cryptographic primitives to introduce diffusion into the system and a simple randomized form of steganography to hide where the encryption begins. The performance of the proposed scheme was evaluated against the One-Time Pad when the pads were used more than once and a cryptanalysis was performed on both schemes. The result indicates that the enhanced OTP algorithm was suitable to allow the same key for limitless use of encrypting different Plaintext without revealing any pattern. This will solve the key management/distribution problem of having to send a new key everytime a message is to be transmitted and this allows the One-Time Pad scheme practical and allows the same key generated during encryption to be reusable on other Plaintext as many times as desired.

Index Terms— Cryptography, Cipher, Confusion, Diffusion, One-Time Pad, Security, Crib-Dragging, Cryptanalysis

I. INTRODUCTION

THE need to secure messages to keep secrecy has been growing rapidly over the past decades due to increasing level of education and information among the people and lack of trust from the third party who may happen to reveal the content or make use of it for their own advantage. Breach of security and mismanagement of confidential data intercepted by unauthorized parties are key problems which information security tries to resolve. Cryptography is the field of information science that has to do with disguising message for secure communication in the presence of adversaries. Cryptographic encryption schemes prevent a third party from understanding the transmitted raw data over the unsecured channel during signal transmission.

In this paper, a new method to enhance OTP data encryption by introducing diffusion into the system and a simple randomized form of steganography have been adopted. This will completely mask any potential and statistical relationship between the Plaintext and Ciphertext.

II. PROBLEM DEFINITION

In information theory and cryptography, a term called “One-time pad (OTP)” – is an encryption technique whereby a key can only be used once as a secret for message. In this

scheme, a random key that is equal in length to the plaintext message to be encrypted with no repetition is used. The plaintext character is exclusive-or bitwise with the key, to produce Ciphertext output. Mathematically, the one-time pad can be expressed as;

$C = P \oplus K$, where P = Plaintext, $\oplus$ = Exclusive-Or, K = Key, and C = Ciphertext

The Exclusive-Or is denoted by XOR and represented with the symbol $\oplus$. Decryption simply involves the same bitwise Exclusive-or operation. The main risk of the scheme lies with the pad/key used.Over the years this technique has remained impractical to use because of its key management and key distribution problems, especially having to generate and send a new key each time one needs to transmit a message. The feasible problem here is that of the new key that must be sent always alongside with the message because the key itself is long as the message. Also, the redundancy of English languages, along with ASCII encoding lends itself to statistical tools that allow for the realization of these messages (Belakang, 1991) [1].

This problem exists for a long time probably because the concepts of cryptography often embraces novel concepts and technologies that require a test of time in practice unless proven unsafe. With the emergence of standard ciphers like RSA, DES, Triple DES, AES many people decided not to bother themselves about ciphers like One-Time Pad even though it was the only cipher proven to be computationally secured unlike the standard ciphers that are not proven to be computationally secured but only believed to be hard to break based on their constructions of using hard mathematical problems and based on failure of existing attempts to cryptanalyze them. Also, the dependency of the pad entropy of OTP is high which makes reusing of the pad to be unsafe. Furthermore, the One-Time Pad has bottlenecks in CPU, RAM, disk I/O and key material consumption.

Corresponding author: aman@usm.my[2], aioludare@gmail.com[1], styleest2011@gmail.com[3], humeraarshed@gmail.com[4]
amumar99@gmail.com[5] Universiti Sains Malaysia[1,2,3,4], Islamic University of Bahawalpur Pakistan[4]. This research was partially supported by the Fundamental Research Grant Scheme (FRGS) for ‘‘content-based analysis framework for better email forensic and cyber investigation’’ [203/PKOMP/6711426], SFRG Lab, School of Computer Sciences, USM. Penang, 11800, Malaysia.

The problem is that to get optimal and perfect secrecy, Key must be truly random, that is a perfect random number. Random number generation is an important primitive in many cryptographic mechanisms. For example, keys for encryption transformations need to be generated in a manner which is unpredictable to an adversary. Generating a random key typically involves the selection of random numbers or bit sequences. Random number generation presents challenging issues (Stallings, W. 2011) [2].

Perfect secrecy is the notion that, given an encrypted message (or ciphertext) from a perfectly secure encryption system (or cipher), absolutely nothing will be revealed about the unencrypted message (or plaintext) by the ciphertext. Perfect Secrecy: Claude Elwood Shannon (Information- Theoretic, 1916) [3]. Security basic idea was that Ciphertext should provide no “information” about Plaintext but have several equivalent formulations:

(i) Considered two random variables M and C as an independent.
(ii) Then observing what values C takes does not change what one believes the distribution M is
(iii) Knowing what is the value of M does not change the distribution of C.
(iv) The encrypting two different messages m_0 and m_1 result in the same distribution.

Perfect security means that for an encryption algorithm if there is ciphertext produced that uses it, no information about the plaintext is provided without knowledge of the key. If *E* is a perfectly secure encryption function, for any fixed message *m*, there must be, for each ciphertext *c*, at least one key *k* such that $C = E_k(m)$. It has been proved that any cipher with the perfect secrecy property must use keys with effectively the same requirements as one-time pad keys.

Figure 1 presents a sample of encryption and decryption processes.

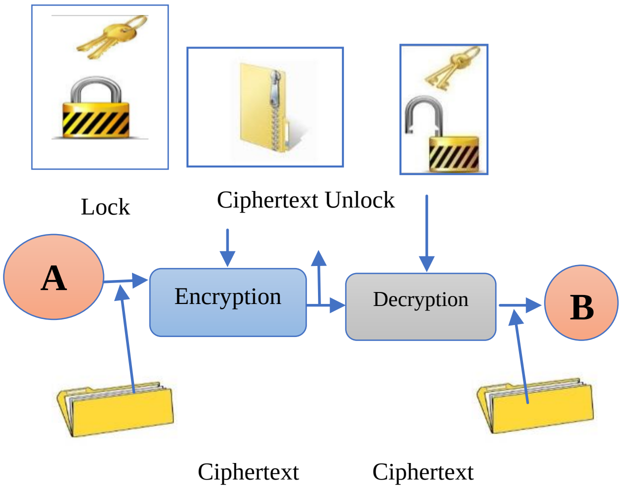

Fig. 1. Encryption and Decryption Process

The OTP in classical cryptography is unconditionally secure due to the absence of any correlation whatsoever between Plaintext - Ciphertext pair and between Plaintext - Key. This is possible as the One Time Key (OTK) is generated by a source of randomness and its length is equal to that of the Plaintext. But in any practical computational environment, a true source of randomness is not possible. Any source of randomness in cryptographic computations generates only a pseudo-random bit string. This combined with the issue of key distribution prevents unconditional or perfect secrecy (Upadhyay, G., & Nene, M. J. 2016) [4]. Key must be used once, any two-time use of key will render ciphertext completely unsecured. A known-Plaintext attack is the key challenge faced when the key is used more than once.

Example: If the same key K is used to send two messages C1 and C2; then plaintext P1 and P2 can be recovered by an eavesdropper. This is referred to as a known-Plaintext attack. This is illustrated as follow:

$$C1 = P1 \oplus K$$
$$C2 = P2 \oplus K$$
$$C1 \oplus C2 = (P1 \oplus K) \oplus (P2 \oplus K)$$
$$C1 \oplus C2 = P1 \oplus P2$$
$$C1 \oplus C2 = P1, P2$$

where,

C1 = Ciphertext 1, C2 = Ciphertext 2, P1 = Plaintext 1, P2 = Plaintext 2 and K = Key

If the same keys are used to send this two messages via an open channel and the eavesdropper was able to intercept C1 and C2, that is both Ciphertexts, the key K cancels out, then he can easily compute the XOR of C1 and C2 and arrive at P1, P2. A good pattern analysis or crib dragging (which will be shown in this paper) will help the eavesdropper reach either or both the Plaintexts. This is a major weak point of OTP and this is because there is enough redundancy in English and ASCII encoding.

Cryptology continues to co-evolve with communication and computing technologies. Prior technological breakthroughs, such as the electro-mechanical devices, telegraph, radio, and personal computers compelled cryptography to replace broken or weak ciphers. Every security expert worries about security problems and tries to find out the secure solution. Because it is a challenging aspect of communications today which touches many spheres including memory space, processing speed, code development and maintenance issues (Miyano, T., & Cho, K. 2016) [5].

Nowadays, memory and processing power are inexpensive and abundant. Capable mathematicians and technologists are highly motivated in their attempts to break encryption; they are succeeding. They have devised many attacks such as, man-in-the-middle, statistical, side channel attacks, and many more (Belakang, a L. 1991) [6], for this reason, we must continue to enhance our ciphers and create new ones that can defeat every form of attacks emerging with technology.

The main goal is to solve the problem of the known-plaintext attack usually used to cryptanalyze the One-Time Pad when the same key is used more than once, thereby allowing the use of the same key to send different messages more than once, and so solving the key management/distribution problem. Also, to improve the One-Time Pad algorithm by removing the 'one time only' limitation that has previously been tagged to the One-Time Pad for it to retain it perfect security.

III. LITERATURE REVIEW

In 1917, Gilbert Vernam invented a cipher solution for the teletype machine [7,8,9]. The United State (U.S.) Army Captain Joseph Mauborgne realized that the character on the key tape could be completely random. Together, they introduced the first One Time Pad encryption system. Since then, One Time Pad systems have been widely used by governments around the world. Outstanding examples of a One Time Pad system include the ‘hotline’ between the White House and the Kremlin and the famous Sigsaly speech encryption system [10].

1. The Mathematical Proof of OTP Security;

According to Alfred Menezes et al. 1997[11,12] in their book, Handbook of Applied Cryptography, a system can be called perfectly secret, or unconditionally secure, when observing ciphertext gives an eavesdropper no additional information about the original plaintext string.
If we let L be the number of bits in the plaintext string, then i ranges from 1 to L in the following definitions:
p_i = the ith bit in the plaintext string,
c_i = the ith bit in the ciphertext string,
k_i = the ith bit in the key string,
P(pi) = the probability that pi was sent
P(p_i | c_i) = the probability that pi was sent given that ci was observed.

A system can be called perfectly secret when P(p_i) = P(p_i | c_i). This section will prove that a One Time Pad system is perfectly secret. In traditional stream cipher systems, the most common method of mixing plaintext data bits with key bits is by performing the XOR operation on the corresponding bits. XOR is short for exclusive OR. The following is a table that defines XOR (the column a as a bit of plain text and column b as its corresponding key bit):

TABLE I
DEFINES XOR

a	b	an XOR b
b	0	0
0	1	1
1	0	1
1	1	0

The sender makes ciphertext by XOR-ing plain text and key one bit at a time:
ci = pi XOR ki ……………………………equation (1)
where ci, pi, and ki are as defined above. Because the One Time Pad key is completely random and unpredictable, two conclusions can be drawn:
First, the probability of observing any One Time Pad key bit is equal to the probability of observing any other One Time Key bit.
Second, knowing all the previous values of the key in a sequence tells us nothing about the next key bit.
By stating another definition, P(ki) = the probability that ki was used to create ci the first conclusion drawn above can be written as;
P(Ki = 1) = P(Ki = 0) = 1/2 for all i……….. equation (2)
In other words, a bit of One Time Key is just as likely to be a 1 as a 0 at any time. The second conclusion drawn above allows us to consider triples of the key, ciphertext, and plain text for a value of I without regard for other triples.
Equation (1) leads to an important observation: knowing any two of {pi, ci, ki } determines the third. Likewise, given one of {pi, ci, ki }, a second one can be written in terms of the third.
For example, P(ci = 1 | ki = 0) = P(pi=1); in other words, if we know for a fact that the key bit is 0, then plain text and cipher text must be equal. In order to show that P(pi | ci) = P(pi), we first need to show P(c_i) = P(ci | pi). Using equation (1), we will do this explicitly by first deriving the distribution of P(c_i). Next, we will derive the distribution of P(ci | pi) given that the plain text bit is a 0 and then given that it is a 1.

Distribution of P(C_i)
P(c_i = 1) = P(c_i = 1 | ki = 1) P(ki = 1) + P(c_i = 1 | ki = 0) P(ki = 0) by the definition of conditional probability = P(pi = 0) P(ki = 1) + P(pi = 1) P(ki = 0) by equation (1)
= P(pi = 0) (1/2) + P(pi = 1) (1/2) by equation (2)
= (1/2) [P(pi = 0) + P(pi = 1)] regrouping
= 1/2 since pi can only be 1 or 0
P(ci = 0) = P(ci = 0 | ki = 1) P(ki = 1) + P(ci = 0 | ki = 0) P(ki = 0) by the definition of conditional probability
= P(pi = 1) P(ki = 1) + P(pi = 0) P(ki = 0) by equation (1)
= P(pi =1) (1/2) + P(pi = 0) (1/2) by equation (2)
= (1/2) [P(pi =1) + P(pi = 0)] regrouping
= 1/2 since pi can only be 1 or 0
Distribution of P(c_i | p_i)
If pi = 0:
P(ci = 0 | pi = 0) = P(ki = 0) by equation (1)
= 1/2 by equation (2)
P(ci = 1 | pi = 0) = P(ki = 1) by equation (1)
= 1/2 by equation (2)
If pi =1:
P(ci = 0 | pi = 1) = P(ki =1) by equation (1)
= 1/2 by equation (2) P(ci=1 | pi=1)
= P(ki=0) by equation (1)
= 1/2 by equation (2)
It is clear from the distributions derived above that P(ci | pi) = P(ci). Recall that a system can be called perfectly secret when P(pi)
= P(pi | ci). Using the definition of conditional probability, the joint probability, P(pi and ci), the probability that pi and ci are observed, can be written in the following two (equivalent) forms: P(pi and ci)
= P(ci | pi) P(pi) and P(pi and ci)
= P(pi | ci) P(ci). Combining the two equations gives P(pi | ci) P(ci)
= P(ci | pi) P(pi).
Since P(ci | pi) = P(ci) as shown above, these two terms cancel, leaving P(pi | ci)
= P(pi), which is the condition for perfect secrecy.

Although, the proof has yielded significant result based on a condition for perfect secrecy. However, there is still a practical difficulty of using an OTP and this can be explained further in this paper.

2. Practical difficulty of using an OTP

The practical difficulty of using an OTP is that the pad/key bytes cannot be reused. This means that even for a two-way communication, each entity must have a sufficient supply of key material on hand so that they don’t run out of keys before new ones can be generated. People are not interested in modifying the algorithm, they are more interested in improving the way the key is generated either by trying to

introduce a true random instance or modifying the algorithm that generates the keys to create a lifetime supply of key.
Their implementation only tries to solve the problem of getting true randomness but does not solve the distribution/management of key material as different keys still have to be sent for different messages.The proposed algorithm solves the key problem by making it possible to use the same key to encrypt different messages and not reveal any pattern that could be exploited by the attacker.

At the advent of binary systems for computational analysis (computers), memory and processing power was expensive and hard to obtain. This led to brilliant mathematical implementations of encryption that protected data, including communication. Due to the impracticality of OTPs, modern encryption was borne which is based upon limited, finite size keys and produces creative attacks other than a 'brute force' attack. Capable mathematicians and technologists are highly motivated in their attempts to break encryption; they are succeeding. They have devised many attacks such as man-in-the-middle, statistical, side channel attacks, and many more (Belakang, an L. 1991) [13,14].

The one-time pad system was modified by using the concepts of 10's complement operation. The eavesdropper come across confusion by observing decimal and binary combination with added concept of complements (Patil, S., Patil, A., & Kumar, A. 2012)[15]. Another attempt at improving the algorithm was made by using a conventional block cipher and one-way hash algorithm to design the one-time pad algorithm. This algorithm proposed by them totally balance the insufficiencies of the conventional block cipher, and exploit the benefits of the one-way hash algorithm (Tang, S., & Liu, F. 2012) [16].

Penchalaiah modified the One-Time pad algorithm to work without any secret key overhead while on the transmission (since the key is along as message) by using two algorithms, a Key Exchanging Algorithm, and a Random Bit Generation algorithm (Penchalaiah, P. 2013) [17].
The problem of key distribution and protection was solved using elliptic curve cryptography. An overview of Koblitz method of encoding was provided and a hybrid security mechanism based on OTP was developed (Katti, J. 2015) [18]. The One-Time Pad was modified with 2's complement approach to introduce more complexity and make the task of cryptanalyzing any ciphertext recovered to be more difficult (Devipriya, M., & Sasikala, G. 2015) [19].

Another attempt at handling the randomness of the key was to use a simple quantum circuit to generate a truly random OTP using quantum superposition states (Upadhyay, G., & Nene, M. J. 2016) [20].
A one-time pad cryptographic method was designed using a star network of N Lorenz subsystems, referred to as augmented Lorenz equations, which generates chaotic time series as pseudorandom numbers to be used for masking a plaintext (Miyano, T., & Cho, K. 2016) [21].

3. Related works on enhanced OTP

There are publications and extant literature on OTP cipher and its enhancements. Much quantum key distribution (QKD) system has been expanded to quantum network manager using OTP encryption [22]. This outline does not just handle the switch and QKD protocol startup processes but as well handles multiplexing and synchronization of secret key streams. An encryption algorithm based on OTP technique to provide sufficient privacy of images using chaos theory has been stated in (C. Jeyamala et al., 2010) [23]. The investigation results of the study have been evaluated with benchmark images and are compared with different image encryption algorithms reported in the literature. Key sensitivity analysis, key space analysis, and numerical analysis proved that this algorithm proposes better security at minor calculational overhead. ln (M. Borowski et al., 2012) [24], Borowski and Lesniewicz presented a hardware generation of binary random sequences with the latent output rate of 100 Mbit/s to eliminate the limitation associated with accessibility of lengthy one-time keys.
A new study on OTP encryption enhancement as in (Patil, M. Devare and A. Kumar 2009) [25], has shown that the random key stream can be employed to generate a lifetime supply of keys for OTPs. Random key generation can easily be created by permutation methods. These methods can be adopted in combination with other procedure such as substitution and encryption function for successful results. The objective of this study is to demonstrate how OTP encryption technique can be accomplished by a combining of these techniques. In (S.G. Srikantaswamy, and H.D. Phaneendra)[26], two new methods of OTP encryption enhancement based on I O'S complement and XOR operations have been presented that do not depend on the original cipher about OTP cipher.

IV. PROPOSED METHOD

As seen from the literature, when the one-time pad is used more than once, it becomes susceptible to a Known-plaintext attack which is why the key cannot be used more than once. The algorithm proposed in this paper makes the One-Time pad still retain its perfect stance even when the same pads/keys are used numerous times.

1. The proposed algorithm is divided into two phases;

(i) Encryption Phase – this is the period or the process of converting information or data into a code, especially to prevent unauthorized access
(ii) Decryption Phase – this is the period or the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.
The Random Number used to generate the system will be retrieved from two sources. Using a single source of random number can create an open channel for trapdoor or could be from a predictable random source. Therefore, we implemented this system by getting the random numbers from two sources.

Most random numbers used in computer programs are pseudo-random, which means they are generated in a predictable fashion using a mathematical formula. This may be fine for many purposes, but it does not give complete security. Our first source of randomness is from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. Another element was introduced so that we can get complete randomness by throwing a ten-sided dice.

A unique binary sequence which is the initialization vector (IV) was employed in each encryption operation. A non-repeating initialization vector that changes as each Plaintext is encrypted is also employed to introduce complete diffusion of the Plaintext and to ensure distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key.

2. The One-Time Pad And Proposed Scheme

In this proposed scheme, two keys were introduced. Normally, when the key is uniform and random, we say there is perfect security but it is almost impossible to get a truly random key. We used two keys so that even if one of the random numbers has a trapdoor and can be predicted, the other will be impossible to be predicted or brute forced and combining both keys will surely give a for of randomness.

Randomly chosen bits/bytes were added to the Plaintext before encryption to reduce the redundancy in English and ASCII encoding and as a form of steganography which makes it impossible to retrieve the key or Plaintext at the beginning of the ciphertext. The Cipher block chaining mode was used to completely diffuse the plaintext so that each time there is a new Plaintext to be encrypted, it always gives a different CipherText even though the same key/pad was used and also a varying initialization vector was also employed in constructing the algorithm.

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

The results were formally presented in accordance with the tests on communications technique employed.

(i) Testing the One-Time Pad and Proposed Scheme when Key is Re-Used

We considered two Plaintext sent with the same key using the OTP and the proposed scheme and cryptanalyze both using pattern analysis (crib dragging).

Plaintext 1: S C H O O L
Randomly chosen bit/bytes for Plaintext 1= 06 71 32
SCHOOL (S = 53, C = 43, H = 48, O = 4F, O = 4F, L = 4C)
Key 1= 6C
Key 2 = KEY (A string or passphrase)
(K = 4B, E = 45, Y = 59)
Perform an Exclusive-OR on both keys

```
  4B
   45   ⊕  6          = 3B
   59
```

New Transformed key = 3B

Therefore, we need to XOR the random bits together with the Plaintext and the key

```
          06 71   32   S C H O O L

          06 71   32   53   43   48   4F   4F   4C
          ⊕  ⊕⊕⊕⊕⊕⊕⊕⊕
          3B 3D   77   7E   16   6E   1D   69   1D
          3D ⊕⊕⊕⊕⊕⊕⊕⊕
      3B   3B   3B   3B   3B   3B   3B   3B
      77   7E   16   6E   1D   69   1D   6A
```

Finally; the Ciphertext to be sent becomes 3D 77 7E 16 6E 1D 69 1D 6A

An inverse gives the Plaintext
Using thesame Key for Plaintext 2, we get,
Plaintext 2: T H E R E
Randomly chosen bit/bytes for Plaintext 2 = 425712
T H E R E (T = 54, H = 48, E = 45, R=52, E = 45)
Key = 3B

```
          42 57   12   T H E R E

          42 57   12   53   48   45   52   45
          ⊕  ⊕⊕⊕⊕⊕⊕⊕
          3B 79   15   3C   53   20   5E   37
          79 ⊕⊕⊕⊕⊕⊕⊕
      3B   3B   3B   3B   3B   3B   3B
      15   3C   53   20   5E   37   49
```

Finally; the Ciphertext to be sent becomes 79 15 3C 53 20 5E 37 49 . An inverse gives the Plaintext

(ii) To perform a crib dragging or pattern matching on this proposed scheme;

suppose the two Ciphertexts where intercepted by an eavesdropper, and both are XORed

```
   3D  77   7E   16   6E   1D   69   1D   6A
⊕ 79   15   3C   53   20   5E   37   49
   44  62   42   45   4E   43   5E   54
```

In crib dragging, we guess a word that might appear in one of the messages. Like in the English word, we know ‘TH’ or ‘THE’ is often used. Let's try ‘THE’. After encoding “THE” as a hexadecimal string, we will get “544845”.

XOR our crib word “544845” at each position of the Ciphertexts and analyze the result.

```
44   62   42   45   4E   43   5E   54
54   48   45
10   2A   07
```

If we convert the hexadecimal string ’ 10 2A 07’ to its character symbol, we get ‘DLE * BEL’

(iii) To perform crib dragging/pattern matching on the same plaintext using OTP;

Plaintext 1: SCHOOL
Key = 6C 4B 45 59 63 21
S C H O O L

```
53   43   48   4F   4F   4C
⊕⊕⊕⊕⊕⊕
6C   4B  45   59   63   21
3F   08   0D   16   2C   6D
```

Plaintext 2: THERE
Key = 6C 4B 45 59 63 21
T H E R E

```
54   48   45   52   45
⊕⊕⊕⊕⊕
6C   4B  45   59   63
38   03   00   0B   26
```

If both Ciphertexts is intercepted, then when both are XORed, the plaintext can be recovered

```
3F   08   0D   16   2C   6D
⊕⊕⊕⊕⊕
38   03   00   0B   26
07   0B   0D   1D   0A
```

Let's try ‘THE’. After encoding “THE” as a hexadecimal string, we will get “544845”.

XOR our crib word “544845” at each position of the Ciphertexts and analyze the result.

07 0B 0D 1D 0A
⊕⊕⊕
54 48 45
53 43 48

If we convert the hexadecimal string ‘53 43 48’ to it character symbol, we get ‘T H E’
The Plaintext is already been recovered. If we try guessing the word ‘SCHOOL’ and try both methods, we will recover the Plaintexts completely when pad/key is used more than once. This proves the onetime pad is completely open to being used by the eavesdropper if encryption is done with the same key multiple times. Table 2 presented Comparison between the Proposed OTP Encryption and the OTP when Key is used Twice.

TABLE II
COMPARISON OF RESULT BETWEEN THE PROPOSED OTP ENCRYPTION AND THE OTP WHEN KEY IS USED TWICE

Encryption Scheme	Method	Security Level	Known-Plaintext Attack
Proposed Scheme	Simple Steganography, Message Diffusion	Complete Concealing of relationship between plaintext and ciphertext	Not possible
One-Time Pad (when key is used twice)	XOR Operation	Information about the plaintext is contained within the encrypted text	Crib-dragging/pattern analysis is possible to recover plaintext

In Table II, it is can be understood that the proposed scheme under the security level that there is a complete concealing of the relationship between plaintext and ciphertext. Also, the information about the plaintext is not contained within the encrypted text. Therefore, Known-Plaintext Attack is not possible, but in One-Time Pad (when the key is used twice), information about the plaintext is contained within the encrypted text, hence, vulnerable to hackers that may be able to use crib dragging/pattern analysis to recover the plaintext.

VI. CONCLUSION

The One-Time Pad is said to be simple and theoretically unbreakable yet it is not been implemented in a practical way due to the problem of key management and distribution of keys. Good ciphers become useless when they are managed and implemented the wrong way. Therefore, this study has enhanced the practical difficulty of One-Time Pad Algorithm that resolves the key management/distribution problem. Therefore, in conclusion, the research objectives were achieved, as the proposed scheme or algorithm resolve the problem of having to generate a key/pad each time a message is to be sent. Therefore, this proposed scheme resolves the problem of having to generate a key/pad each time a message is to be sent, thereby solving the problem of key distribution and management in One-Time Pad encryption scheme.

Future work can be on how to improve on the long key of encrypting in OTP using a key scheduling algorithm why still maintaining the “Perfect Security” cliche we know of OTP.

ACKNOWLEDGMENT

The authors would like to express profound gratitude to the Student of Security and Forensic Lab School of Computer Sciences, Universiti Sains Malaysia and IMECS 2018 reviewer on this work for their valuable comments and suggestions that improve the presentation of this research.

REFERENCES

[1] C.E. Shannon, The redundancy of English. In Cybernetics; Transactions of the 7th Conference, New York: Josiah Macy, Jr. Foundation 1951, pp. 248-272.
[2] W. Stallings, Cryptography and network security: principles and practices. 2006, Pearson Education India.
[3] C.E. Shannon, “Communication in the presence of noise,” Proceedings of the IRE, 1949, 37, 1, pp. 10-21.
[4] G. Upadhyay, M.J. Nene, One-time pad generation using quantum superposition states. In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2016, May, IEEE International Conference on, pp. 1882-1886. IEEE.
[5] M. Lobier, M. Dubois, and S. Valdois, “The role of visual processing speed in reading speed development. 2013, PLoS One, 8, 4, e58097.
[6] N. H. Beebe, “A Bibliography of Papers in Lecture Notes in Computer Science, 2012: Volumes 6121–7125. Computer Science, 6121.
[7] F.B Wrixon. “Codes, Ciphers & Other Cryptic & Clandestine Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet,” 1998, Black Dog & Leventhal Pub.
[8] P.E.T.R. Voborník, “Migration of the Perfect Cipher to the Current Computing Environment,” WSEAS transactions on information science and applications, 2014, pp. 196-203.
[9] D. Strobel, I.C. Paar, M. Kasper, “Side-channel analysis attacks on stream ciphers. 2009, Masterarbeit Ruhr-Universitat Bochum.
[10] Bellovin, S. M. (2011). Frank Miller: Inventor of the one-time pad. Cryptologia, 2011, 35, 3, pp. 203-222.
[11] A. J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, “Handbook of applied cryptography,” 1996, CRC Press.
[12] C.J. Colbourn, and J.H. Dinitz, “Handbook of combinatorial designs,” 2006, CRC Press.
[13] F.X. Standaert, “Introduction to side-channel attacks,” In Secure Integrated Circuits and Systems,” 2010, pp. 27-42). Springer US.
[14] F.X. Standaert, “Introduction to side-channel attacks” In Secure Integrated Circuits and Systems, 2010, pp. 27-42. Springer US.
[15] C. Blum, and X. Li, “Swarm intelligence in optimization,” In Swarm Intelligence, 2008, pp. 43-85. Springer Berlin Heidelberg.
[16] D. Trček, H. Abie, Å., Skomedal, I. Starc, “Advanced framework for digital forensic technologies and procedures. Journal of forensic sciences, 2010, 55,6, pp. 1471-1480.
[17] D. Boneh, and X Boyen, “Efficient selective-ID secure identity-based encryption without random oracles. In International Conference on the Theory and Applications of Cryptographic Techniques, May 2004, pp. 223-238. Springer, Berlin, Heidelberg.
[18] J. Katti, S. Pote, and B.K. Lande, “Two-Level Encryption based on One Time Pad and Koblitz Method of Encoding. International Journal of Computer Applications, 2015, pp. 122,15.
[19] F.G. Deng, and G.L. Long, Secure direct communication with a quantum one-time pad. Physical Review A, 2004, 69,5, 052319.
[20] M. Herrero-Collantes, and J.C. Garcia-Escartin, “Quantum random number generators,” Reviews of Modern Physics, 2017, 89,1, 015004.

[21] T. Miyano, and K. Cho, “Chaos-based one-time pad cryptography,” In Information Theory and Its Applications (ISITA), 2016 International Symposium on pp. 156-160. IEEE.

[22] T. Lange, and T. Takagi, “Post-Quantum Cryptography 8th International Workshop”, PQCrypto 2017, Utrecht, The Netherlands, June 2017, pp. 26-28, Proceedings.

[23] C. Jeyamala, S. GopiGanesh, and GS. Raman, “An Image Encryption Scheme Based on One Time Pads,” A Chaotic Approach, Second International Conference on Computing, Communication and Networking Technologies, 2010, pp. 1-6.

[24] M. Borowski and M. Lesniewicz, Modern usage of "old" onetime pad, IEEE Conference on Communications and Information Systems, 2012, pp. 1 - 5.

[25] S. Patil, M. Devare and A. Kumar, Modified One Time Pad Data Security Scheme: Random Key Generation Approach," International Journal of Computer Science and Security, 2009, pp. 138-145.

[26] SG. Srikantaswamy and HD. Phaneendra, Enhanced One Time Pad Cipher with More Arithmetic and Logical Operations with Flexible Key Generation Algorithm, International Journal of Network Security & Its Applications, 2011, pp. 243-248.