Journal of Engineering Technology

Volume 7, Special Issue (Internet of Things) Oct. 2018, PP. 62-73

RESEARCH ARTICLE -ENGINEERNG TECHNOLOGY ASEE

Implementation of One Time Pad based encryption: Way to unbreakable encryption and Introduction of Pseudo OTP generation

Sachin Khedekar[1], Chanchal Sakarwar[2], Mainak Mukhopadhyay[3]

[1]Research Scholar in Birla Institute of Technology, Mesra, Deoghar Campus, Jharkhand, India
[2]Business Analyst, EXL Inductis (India) Pvt. Ltd., Gurgaon, Haryana, India
[3]Head of ECE Department, Birla Institute of Technology, Mesra, Deoghar Campus, Jharkhand, India

Abstract: The objective of this work is to make the One Time Pad (OTP) System of encryption commercially viable which was NOT for the last hundred years after the invention and patented in 1919 by Gilbert Vernam or for more than seventy-five years after Claude Shannon's proof that the OTP based method is the only theoretically unbreakable cryptography exists[1]. In this paper, an OTP generation algorithm and PRN (Pseudo Random Number) sequence generator model (by modifying existing Gold Code Generator as in Global Positioning System) has been proposed. In the proposed algorithm and design, the key or OTP required for encryption for the next message is generated from the last sent message itself both in the transmitter and as well within the receiver resolves the main obstacle regarding generation and communication of new OTP from the transmitter to the receiver for every new message block which is restricting commercially viable OTP based secure communication for a hundred years.

Keywords: Cryptography, One Time Pad, Pseudo OTP, Unbreakable Encryption.

1 Introduction

The plaintext is combined with a random key in One Time Pad (OTP), also called Vernam-cipher or the perfect cipher. It is the only existing crypto algorithm which uses mathematically unbreakable encryption as per Claude Shannon[1], but till today it is not suitable for commercial use as it requires the generation of OTP for every new message sequence. This OTP must be truly random and must be used only once. There must only be two copies of the OTP, one for the sender and one for the receiver. Moreover, secure communication of the OTP from the transmitter to the receiver also becomes an issue to be overtaken[2]. These issues must be resolved in order to make the One Time Pad System of Encryption commercially viable.

The messages which are getting transmitted to the receiver through a valid cryptography process are the most secure data, because if the message is predictable then there is no need for cryptography. The motto of cryptography is to 'protect the message', not to protect the 'key' or 'cryptographic' algorithm or process' first (refer figure 1 and figure 2). Hence if the current message (which are getting encoded with 'the key' and transmitted to the receiver to get decoded by using the same key) is generating the 'next key' for the encryption of the next message, then it is actually working as One Time Pad (OTP) for next message. If the same process is repeated, for every new message we shall get a new OTP. And as per Claude Shannon [1] OTP based encryption techniques are the only one theoretically unbreakable encryption.

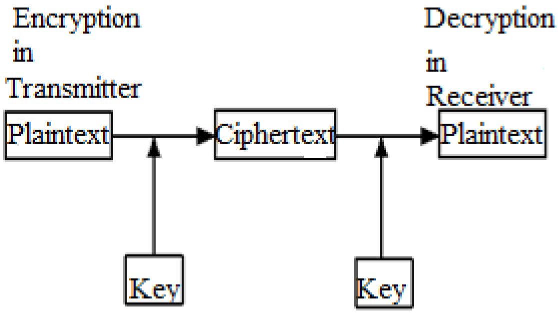

Figure 1: Cryptography process

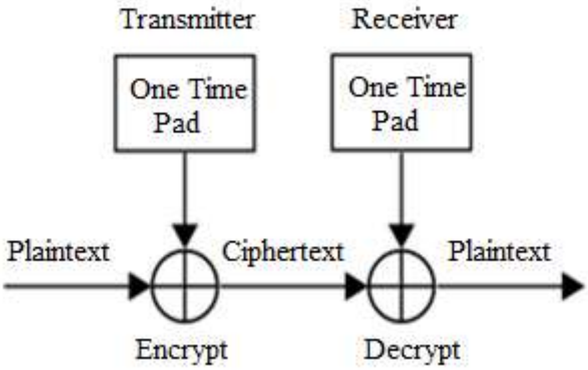

Figure 2: Existing One Time Pad (OTP) encryption-decryption process

In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked but requires the use of a one-time pre-shared key the same size as, or longer than, the message is being sent. In this technique, a plaintext is paired with a random secret key (otherwise call one-time pad) as shown in figure 1 and figure 2. Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition[3]. If the key is truly random, at least as long as the plaintext, never reused in a whole or in part, and kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. As per Claude Shannon [1] whatever technological progress may come in the future, one-time pad encryption (figure 2.) is and will remain, the only truly unbreakable system that provides real long-term message secrecy.

2. Commercially Viable OTP based encryption system.

2.1 Plan of Work

Step 1: Communicate the first PRN sequence or the first OTP to the receiver. (This OTP must be generated by the transmitter independently for the first message only).

Step 2: Input the first message from the user. Encrypt it with the first PRN (OTP) and send it to the receiver.

Step 3: Decrypt the encoded message, at the receiver using the first OTP which is communicated by the Transmitter as mentioned in step 1.

Step 4: **Generate the 2nd (or subsequent PRNs) PRN sequence (key) at the transmitter and receiver from the first message.** (This is the whole new concept we are using in this work which makes OTP based encryption commercially viable.)

Step 5: Input the second message from the user. Use PRN generated (in step 4) to encrypt 2nd message sequence.

Step 6: Transmit the encrypted message to the receiver.

Step 7: Use PRN generated at the receiver (in step 4) to decrypt encrypted sequence. (The receiver has the same circuit from which the New/Next PRN sequence or OTP will be generated from the previous message; **hence, the OTPs are needed not be communicated further from the transmitter to the receiver from now on**. **This hardware modification is also the new concept proposed in this work to make OTP based method commercially viable and practically implementable.**)

Step 8: Repeat the process for all message sequences from step 4. Hence for every new message block of 10 bits length (as considered in this work) our proposed algorithm and design shall generate a new key of 10 bits length which is working as OTP.

2.2 Methodology

2.2.1 The changes proposed in the ONE TIME PAD System of Encryption

- In One Time Pad system, the key used for encryption is truly random. Each encryption bears no relation to the next encryption. Generating a truly random key for each encryption is not viable till today.
- We proposed a model wherein the PRN sequence (key) is generated from the message itself. **Thus, the transmitting and receiving side can generate PRN independently but**

simultaneously. This PRN is used to encrypt the next message sequence in the transmitting side and decrypt the encrypted sequence in the receiving side. This removes the burden of secure transmission of the key or a PRN sequence from the transmitter to the receiver (refer figure 3).

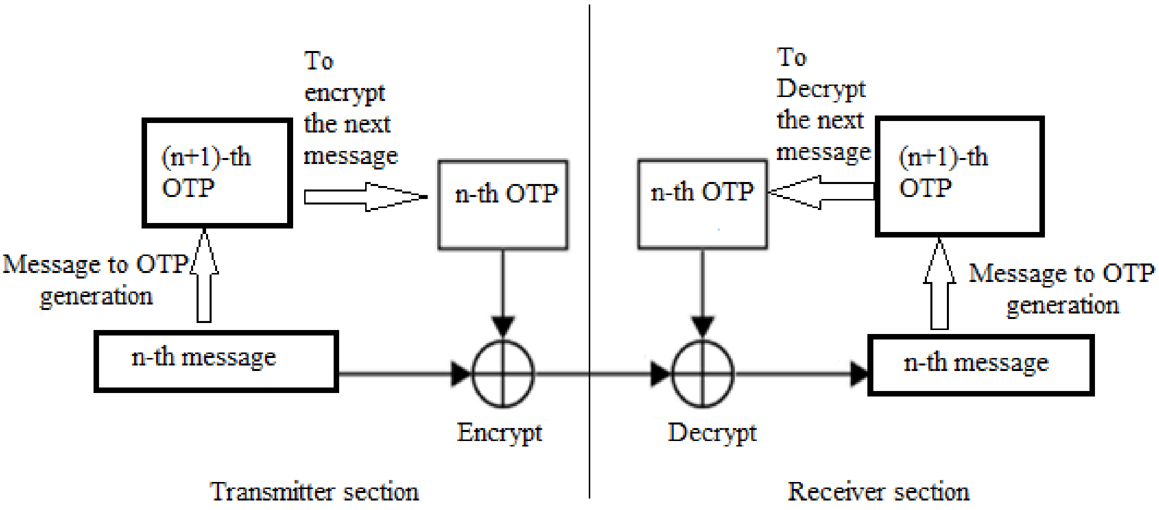

Figure 3: Proposed OTP based encryption-decryption process.

2.2.2 The proposed algorithm to make ONE TIME PAD Commercially Viable

List of abbreviation used -

Tx: Transmitter

Rx: Receiver

K_0 : First OTP (which has to be generated separately to communicate the first message to the Rx. This is a onetime process at the beginning)

M_n : *n*-th message

K_n : *n*-th Key(PRN)

T_n : *n*-th Transmission

Step 1: K_0 generated separately, M_0 also generated.

Step 2: K_0 will be communicated to Rx as first OTP. (This is a onetime process at the beginning.)

Step 3: So in Tx: $M_0 \oplus K_0 = T_0$ → and in Rx: $T_0 \oplus K_0 = M_0$ ($\oplus$ represents Exclusive-OR operation)

Step 4: Now M_0 will generate the K_1 (Both in the Tx and Rx independently)

(This is the novelty or newness of this method and accordingly, PRN sequence generator's design will be modified next)

Step 5 : Go back to Step 3, and the process will continue as stated in Step 4.

In Tx and Rx: M_{n-1} will generate the K_n (subscript 'n' denotes the n^{th} communication)

Tx: $M_n \oplus K_n = T_n$ →(transmitted to the receiver) Rx: $T_n \oplus K_n = M_n$ (**cause in the receiver K_n has been generated independently by the last message received and decrypt i.e by M_{n-1}.**)

Therefore, the algorithm can be given as simply:

In Tx: $M_n \oplus K_n = T_n$ (Message encrypted and Transmitted)

In Rx: $T_n \oplus K_n = M_n$ (Transmission received and message decrypted)

In Tx and Rx: $M_{i-1} \rightarrow K_i$ (M_{n-1} shall generate K_n independently both in Tx and Rx)

Now the next immediate question is how we will generate NEXT KEY (OTP) from the last message itself for every new message. For that we will propose a design of PRN sequence generator in the following sections by modifying existing GPS Gold Code sequence generator.

3. Proposed PRN (OTP) sequence generator which will generate new OTP for every new message from the last message

3.1 Gold Code

We are using Gold Code and/or Gold Code generator in this work to implement the above-mentioned novel algorithm and accordingly, we will modify the existing Gold code generator (as depicted in figure 4, modified or proposed modification over the existing Gold Code generator has been encircled by the blue line).

Gold codes can be summarized as:

A set of bit sequences required by Communication systems that [4] [5]:

- Are simple to produce with hardware or software.
- Have a low cross-correlation with other sequences in the set.
- Easy to tell the sequences apart even when corrupted by noise.

Gold Code is such a class of 2N-1 sequences of length 2N-1-

- Created by XOR-ing MLSRS (Maximum Length Shift Register Sequence) generated by different taps.
- Each seed gives a different Gold code.
- Each code is somewhat different than the others.

3.2. Modified Gold code generator to generate PRN sequence (Key) from the previous message: Introduction of 'Pseudo OTP'

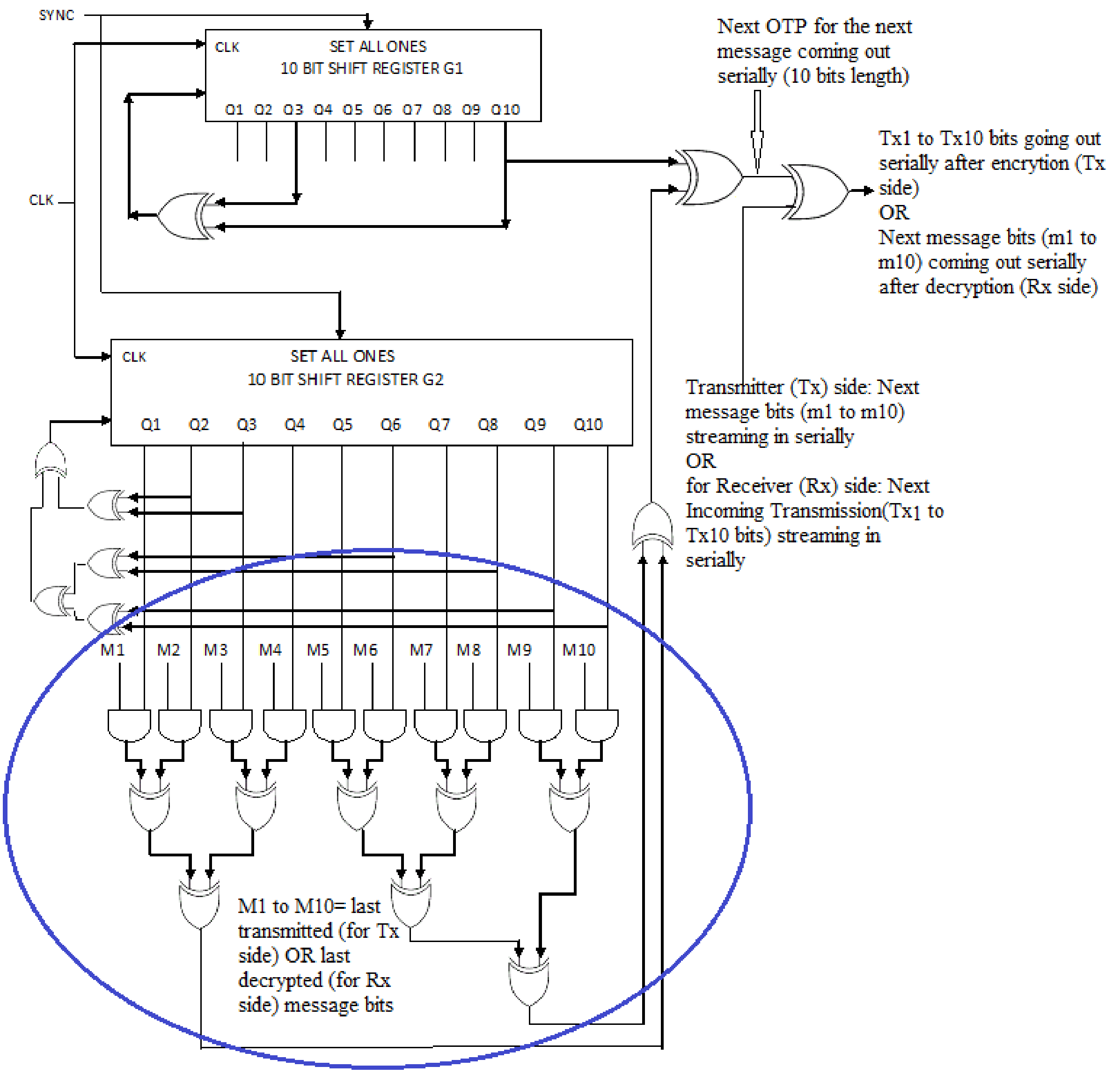
SYNC
CLK
CLK
SET ALL ONES
10 BIT SHIFT REGISTER G1
Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10
Next OTP for the next message coming out serially (10 bits length)
Tx1 to Tx10 bits going out serially after encrytion (Tx side)
OR
Next message bits (m1 to m10) coming out serially after decryption (Rx side)
CLK
SET ALL ONES
10 BIT SHIFT REGISTER G2
Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10
Transmitter (Tx) side: Next message bits (m1 to m10) streaming in serially
OR
for Receiver (Rx) side: Next Incoming Transmission(Tx1 to Tx10 bits) streaming in serially
M1 M2 M3 M4 M5 M6 M7 M8 M9 M10
M1 to M10= last transmitted (for Tx side) OR last decrypted (for Rx side) message bits

Figure 4: PRN/Modified Gold Code sequence generator

In figure 4, the modified gold code sequence generator has been proposed. Proposed modification or the addendum portion encircled by a blue line. In the added or modified design (unlike the actual Gold Code generator) PRN sequence can be changed according to previous message bits (M1-M10), depend on the arrangement of 0s and 1s in message bits M1- M10, G2 sequence will get changed, which is producing the next PRN / Gold sequence/OTP at the output after Modulo-2 (EX - OR) addition with G1 sequence. Thus, the Output Gold Code sequence will change for the next message and in turn for every new message block, we can have a new PRN sequence. As PRN sequences are not theoretically the true random sequences, we can term those generated PRNs from our Modified

Gold Code Generator as **Pseudo OTP** and also can term our modified Gold Code Generator as **Pseudo OTP generator**.

4. Results

Case 1: PRN (OTP) Generation for the different message sequences -

Seed or the first G1 sequence (set by the user):7B$_H$ (0001111011)$_2$

Seed or first G2 sequence (set by the user): 1C8$_H$ (0111001000)$_2$

First message sequence for which OTP is generated: M0: 315$_H$ (1100010101)$_2$

(all data are in Hexadecimal format) first OTP is K_0= 012$_H$ (as mentioned in Step 1 and 2 in section 2.1)

Table 1: Generated PRN and encrypted messages for given input sequences from the proposed design as depicted in figure 4 (different message sequence of 10 bits as in the first column of the table).

Input Message Sequence (M_i)	**G1 Sequence**	**G2 Sequence**	**PRN Generated (K_i)**	**Encrypted Message** T_i ($M_i \oplus K_i$)
M_0= 2FE$_H$	038$_H$	02A$_H$	**K_1=3AF$_H$**	T_0=3DD$_H$ ($M_0 \oplus K_0$)
M_1=0A1$_H$	3F8$_H$	363$_H$	**K_2=003$_H$**	T_1=30E$_H$ ($M_1 \oplus K_1$)
M_2=0B2$_H$	1C7$_H$	345$_H$	**K_3=309$_H$**	T_2=0B1$_H$ ($M_2 \oplus K_2$)
M_3=2DC$_H$	2E4$_H$	313$_H$	**K_4=373$_H$**	T_3=1D5$_H$ ($M_3 \oplus K_3$)
M_4=333$_H$	3A9$_H$	3B2$_H$	**K_5=22D$_H$**	T_4=040$_H$ ($M_4 \oplus K_4$)

Case 2: PRN (OTP) Generation for the SAME message sequences -

Seed or the first G1 sequence (set by the user):038_H $(0000111000)_2$

Seed or first G2 sequence (set by the user): $02A_H$ $(0000101010)_2$

First message sequence for which OTP is generated: M0: $2FE_H$ $(1011111110)_2$

(all data are in Hexadecimal format) first OTP is $K_0= 123_H$ (as mentioned in Step 1 and 2 in section 2.1)

Table 2: Generated PRN and encrypted messages for given input sequences from the proposed design as depicted in figure 4 (SAME message sequence of 10 bits as in the first column of the table).

Input Message Sequence (M_i)	**G1 Sequence**	**G2 Sequence**	**PRN Generated (K_i)**	**Encrypted Message** T_i $(M_i \oplus K_i)$
$M_0= 315_H$	$07B_H$	$1C8_H$	$\mathbf{K_1=1FD_H}$	$T_0=307_H$ $(M_0 \oplus K_0)$
$M_1=0E6_H$	363_H	240_H	$\mathbf{K_2=34E_H}$	$T_1=11B_H$ $(M_1 \oplus K_1)$
$M_2=0E6_H$	$30D_H$	$0AA_H$	$\mathbf{K_3=136_H}$	$T_2=3A8_H$ $(M_2 \oplus K_2)$
$M_3=0E6_H$	393_H	236_H	$\mathbf{K_4=0A1_H}$	$T_3=1D0_H$ $(M_3 \oplus K_3)$
$M_4=0E6_H$	234_H	329_H	$\mathbf{K_4=3F5_H}$	$T_4=047_H$ $(M_4 \oplus K_4)$

4.1 Novelty Analysis of the Proposed Modified Design and Algorithm

From the results as listed in Table 1 and 2, a few unique and novel outcomes can be observed clearly.

1. Only the first OTP needs to be generated at the beginning in the transmitter side. The same OTP just needs to be communicated to the receiver as mentioned in Step 1 and 2 in section 2.1.

2. After that for every new message, a new OTP will be generated, **but that OTP need not to be communicated to the receiver** (**The traditional obstacle for which One Time Pad is not commercially viable**). The receiver will itself generate the next OTP just like it has been generated within the transmitter from the last message decrypted, and that is the novelty and uniqueness of the proposed algorithms and modified Gold Code Generator as depicted in figure no.4.

3.The most important robustness of the proposed method can be clearly observed from the result as listed in Table 2, i.e. even for the same message sequence (i.e. 0E6$_H$ in this case) applied every time, the algorithm and the modified Gold Code Generator will generate NEW OTPs (1FD$_H$, 34E$_H$, 136$_H$, 0A1$_H$, 3F5$_H$, etc.).

4. As Gold Codes itself have very low cross correlations with each other, we can clearly say this process and modified design can be used as OTP based system (or as **Pseudo OTP** to be precise) **which is practically unbreakable as well as commercially viable**.

4.2 Cross-correlation between generated OTPs

It is desired for PRN sequences or as well as for Gold Codes the correlation between two PRN sequences or two gold codes should be less or very less. In our case of 10bits long OTP sequences generated for the SAME message sequence as in table 2 (i.e. 1FD$_H$, 34E$_H$, 136$_H$, 0A1$_H$, 3F5$_H$, etc. as first 5 OTPs) we have listed the simple bit to bit correlation (modulo 2 addition or bit to bit Ex-Or operation) in Table no. 3, where a perfect matching between two sequences indicated by the decimal value of 10. A negative value indicates two sequences are negatively correlated, and a value of 0 indicates two sequences are uncorrelated.

Table 3: Cross-correlation between generated OTPs of table 2 for the same message sequences

OTPs	1FD	34E	136	0A1	3F5
1FD	10_{10}				
34E	-2_{10}	10_{10}			
136	0_{10}	0_{10}	10_{10}		
0A1	0_{10}	-6_{10}	-2_{10}	10_{10}	
3F5	$+6_{10}$	-2_{10}	0_{10}	$+2_{10}$	10_{10}

From the above data of bit by bit cross-correlation, it can be clearly observed that even for the **same message sequence** our proposed algorithm and modified Gold Code Generator is producing **uncorrelated OTPs or OTPs with very low cross-correlation** except in two possible pairs (out of 10 possible pairs among five OTPs) where the cross-correlation values are 6_{10} (Maximum value is 10_{10} i.e. the autocorrelation.). Now above bit by bit Cross-correlation has been investigated for the repeated **same message sequences** (which are uncommon in real life) and **even then our proposed**

methodology and design generating different OTPs mostly with low cross-correlation and this is the true novelty of proposed Pseudo OTP generator **which will open the possibilities of using the theoretically unbreakable cryptography or OTP based encryption commercially and or practically**.

4.3 Possibilities of Hacking or Cracking the system

As our proposed Pseudo OTP generator shall generate uncorrelated or low cross-correlated OTPs for every new message, cracking or hacking by predicting the next OTPs are almost impossible unless hackers own the whole Transmitter or Receiver's site physically. Even if in certain situation hackers able to predict the future series of OTPs partially, the user just simply needs to change the input message at the transmitter side and the whole process will recommence with the new sequence of OTPs cause in this novel design next OTP shall depend on the current message. Hence, the proposed Pseudo OTP generator is foolproof in a realistic way as per the theoretical proofs of Claudie Shannon (1940).

5. Conclusion

A whole new concept of Pseudo OTP generation has been proposed to make One Time Pad based encryption practically and commercially feasible to achieve truly unbreakable cryptography. We have proposed an algorithm in which the next key or PRN shall be generated from the current message both in the transmitter and receiver which will practically work as OTP. Even for the same message sequences, different PRN sequence has been generated successfully. This PRN sequence is used to encrypt the message sequence as OTP. According to the proposed algorithm, we have also modified the existing Gold Code Generator used in GPS to generate the new OTP for every new message block practically. OTP so generated are of the same length of message block thus satisfying the criteria of unbreakable cryptography as per Claude Shannon[1]. Our proposed modified design and algorithm also hereby overcome the main disadvantages of the One Time Pad system i.e communication of every OTP for every message to the receiver as receiver itself can generate the OTPs independently for the next incoming message from the last decrypted message. With all these OTP based cryptography systems can become commercially viable which was not for a hundred years after the inception.

Acknowledgment

Authors would like to thank Birla Institute of Technology, Mesra, Jharkhand, India for providing research facility.

References

[1] Claude Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, 28 (4), pp. 656–715, 1949.

[2] Oded Goldreich, "Foundations of Cryptography", Vol. 2, Basic Applications, 2002.

[3] Zaeniah and Bambang Eka Purnama, "An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm", International Journal of Advanced Computer Science and Applications (IJACSA), 6(9), 2015.

[4] Lars R. Knudsen & Matthew Robshaw, “The Block Cipher Companion”, Springer Science & Business Media, pp. 1–14, ISBN 9783642173424, Retrieved 26 July 2017.

[5] Holmes & Jack K, “Spread Spectrum Systems for GNSS and Wireless Communications”, GNSS Technology and Applications Series, 45, Artech House, ISBN 978-1-59693-083-4, 30 June 2007.