Hyper Encryption as an Advancement of one Time Pad an Unbreakable Cryptosystem

Ms Sunita, Ms Ritu Malik
School of Engg. & Science B.P.S.M.V Khanpur
Kalan, India

Abstract—The security of cryptosystem has received much attention in recent year. There are a number of cryptographic protocol those provide the attainable security but the need of the everlasting and unbreakable cryptographic has been always permissible. This paper defines the unbreakable cryptographic ONE TIME PAD Protocol. This protocol is theoretically strong but practically loose. So to overcome the limitation of OTP and to use its concept of unbreakable security a new cryptographic approach known as Hyper Encryption was described. Hyper Encryption is provable unbreakable encryption protocol and provides everlasting security with the use of assumption of Bounded Storage Model. This paper represents the Hyper Encryption as an advancement of OTP. This paper show that how the limitation of OTP can be time out by the use of Hyper Encryption with a better practical implementation of the protocol.

Keywords— Encryption, Everlasting Secure System, One Time Pad, Page Server Node, Hyper Encryption

I. INTRODUCTION

The Security of most modern cryptographic schemes depends on the computational power if the today’s encrypted data’s encryption key is revealed to the Adversary and the computation power of eavesdropper increase. Or maybe the brute force approach will be possible in future then our data will be no longer secure. Eavesdropper can record the encrypted data and will be able to read the sensitive encrypted info in near future. So to deal with this situation we have to develop a practical cryptographically system to keep our data secret. Cryptographic System should be like which allows to send data secretly and keep it as a secret forever against an adversary unbounded computational power.

One Time Pad is a provable secure cryptosystem that is developed by Gilbert Vernam in 1918. It use the truly random series of bits as the secret key (Pad) as the same length as the plaintext. The secret Pad (Not Reusable) is shared between the user in a very secure way and after use the pad was destroyed completely. Simple Modular or XOR operation is performed between the plaintext and the secret key to encrypt it. If the truly random sequence of bits is used as key, length of key is taken as the length of plaintext and key was never reused (fully or partially) then it will be impossible to break the system without knowing the key. But practical implementation put some limitation on One Time Pad.

As advancement Rabin described the scheme of Hyper Encryption that provide benefits over the limitation of One Time and provide the everlasting security to the user data. In its basic scheme it takes many PSN servers from which anybody can request a page of random bits. Each page is served only twice then it was destroyed. So the two users who want to transfer data can agree on the same page of random bits and can take this page as a one time pad. After the initial shared secret key it also allows the user to create the new secret pad to make the communication indefinitely. In this paper we will study both the cryptographically secure scheme in brief and will have a comparative study on them.

II. ONE TIME PAD

Firstly we will describe the cryptographically secure unbreakable system ONE TIME PAD. OTP produce the random output that doesn’t have any relationship with the plaintext. Because in the OTP the cipher text contains no information about the plaintext so it is simply unbreakable. OTP is basically a shared secret key scheme.

OTP is first described by the Frank Miller in 1882. It was later described by the Gilbert Vernam in 1918. OTP is basically derived from the VERNAM CIPHER. In the OTP each message is represented as series of binary digit (a series of 0 or 1 with the help of coding mechanism such as ASCII or with the help of Code Book sort of Code Dictionary that has the word listed alphabetically along with the number code for the word). A truly random sequence of 0 and 1 is taken as the key of the same length as of message. The secret key is taken as the pad in OTP because of early implementation where the key material was distributed as the pad of the paper. The secret key pad is distributed between the users in a very secure way mainly (by hand to hand). After the use of the secret pad one time the pad is completely destroyed by both the parties to make it secure. In the OTP the encryption system use a very simple operation like the modular or the XOR. Basically the XOR/Modular operation is performed between the secret pad key and the plaintext digit to make it encrypted. Encryption technique is so simple that it can be done with the pen and paper by hand. If the key is taken truly random as the length of the message and the key is kept secret and used only one time then this scheme will be forever secure and unable to break.
III. OPERATION SCHEME OF OTP:-

The encryption/decryption scheme in the OTP is very simple. Basic XOR/Modular scheme is used for the operation here we will define the scheme in four basic steps:-

Step 1:- in the first step of the encryption scheme firstly the plaintext character string is transferred to the bit string with the help of ASCII coding scheme or with the help of the code book (that can have different number of the digit to represent a corresponding word based on the different country’s code book as the Soviet’s code book use the 4 digit number to represent the code) the code book can be reused for the coding. Both sender and receiver used the same copy of the code book or the coding scheme to code the plaintext or to decode the cipher text. Here we can use another simple scheme to show the implementation we will take the English alphabets \([A,B,C...........X,Y,Z]\) and code them as digits\([0,1,2,3........23,24,25]\) as shown in the table

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |

For example: - we will take the HYPER ENCRYPTION as our Plain text and code it as follow

Plaintext: - HYPER ENCRYPTION

Coded plaintext:-72415417 41321724151981413

Step 2: - The second step of the encryption scheme is to be agree on the shared secret key(pad). Truly random number are chosen to be used as the one time pad in this scheme. Earlier these secret random number are chosen and printed on a pad securely handed to both the parties but today there are many other way by which both the parties can be agreed on the same shared secret. There are only two copies of one time pad key and these copies are not reusable. Each page of the OTP is destroyed completely by the user after its use. The One Time Pad key is the most crucial part of this encryption scheme. The secret key length should be same as the length of the plaintext and to be truly random. Suppose for the example. We take the random key as OTP shared secret key: - 76 36 18 48 24 44 58 11 88 08 13 03 74 81 49. This key should have to be truly random and as the length of the plaintext. The security of the encryption system depends on the security of this random key so the key should be kept secret.

Step 3:- In the step 3\(^\text{rd}\) we will apply one of the basic operation as XOR or modular arithmetic operation to perform the encryption of data. We here first do the addition of the coded plaintext digit and then mod26 operation is performed on the addition bits. But if we implement this encryption scheme as the software we will prefer the XOR operation for the encryption of data. So in this way OTP used the easiest operation for encryption that can be done with the help of pen and paper by hand. For ex:-

Plaintext: - 7 24 15 4 17

Secret key:-76 36 18 48 24

Addition (plaintext +Secret Key) =83 60 33 52 41

Mod 26 of addition = 05 08 07 00 15

Cipher text = 05 08 07 00 15

Step 4:- Step 4 can be the optional step in this encryption system. If you wish you can convert the resulting cipher text back to the character form from the numerical sequence by using the same decoding scheme that was used in the step 1\(^\text{st}\) of this encryption scheme. But this step doesn’t add any extra security to the encryption system. This can be used because transmission of character can be cheaper then to transmit the number.

Example: - Encryption Scheme

1. Plaintext:- HYPER ENCRYPTION
2. Coded Plaintext:-

<table>
<thead>
<tr>
<th>H</th>
<th>Y</th>
<th>P</th>
<th>E</th>
<th>R</th>
<th>E</th>
<th>N</th>
<th>C</th>
<th>R</th>
<th>Y</th>
<th>P</th>
<th>T</th>
<th>I</th>
<th>O</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>24</td>
<td>15</td>
<td>4</td>
<td>17</td>
<td>4</td>
<td>13</td>
<td>2</td>
<td>17</td>
<td>24</td>
<td>15</td>
<td>19</td>
<td>8</td>
<td>14</td>
<td>13</td>
</tr>
</tbody>
</table>

So the coded plain text is:-07 24 15 04 17 04 13 02 17 24 15 19 08 14 13

[3] Random secret key:- 76 36 18 48 24 44 58 21 88 08 13 03 74 81 49


Plaintext

| 7 | 24 | 15 | 4 | 17 | 4 | 13 | 2 | 17 | 24 | 15 | 19 | 8 | 14 | 13 |

Secret key

| 76 | 36 | 18 | 48 | 24 | 44 | 58 | 21 | 88 | 08 | 13 | 03 | 74 | 81 | 49 |

Plaintext +Secret pad =

| 83 | 60 | 33 | 52 | 41 | 48 | 71 | 23 | 105 | 32 | 28 | 22 | 82 | 95 | 62 |

[5] Cipher text = Plaintext +Secret Key (mod 26)

| 05 | 08 | 07 | 0 | 15 | 22 | 19 | 23 | 01 | 06 | 02 | 22 | 04 | 17 | 10 |

[6] Decode the cipher text character back to the numerical sequence as in step (1)

| 05 | 08 | 07 | 0 | 15 | 22 | 19 | 23 | 01 | 06 | 02 | 22 | 04 | 17 | 10 |

© 2014, IJARCSSE All Rights Reserved
So now the user has encrypted its plaintext to the Cipher text with the help of the OTP for Decryption of Cipher text back to the plaintext the receiver has to perform the reverse operation of OTP.

Plaintext: - HYPER ENCRYPTION
Cipher text: - EIHAP WTXBGCWERK

Decryption Scheme: - For the Decryption with OTP user has to perform the reverse operation of the encryption scheme.

1. Cipher text: EIHAP WTXBGCWERK
2. Decoded Cipher text: -

<table>
<thead>
<tr>
<th>E</th>
<th>I</th>
<th>H</th>
<th>A</th>
<th>P</th>
<th>W</th>
<th>T</th>
<th>X</th>
<th>B</th>
<th>G</th>
<th>C</th>
<th>W</th>
<th>E</th>
<th>R</th>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td>05</td>
<td>08</td>
<td>07</td>
<td>0</td>
<td>15</td>
<td>22</td>
<td>19</td>
<td>23</td>
<td>01</td>
<td>06</td>
<td>02</td>
<td>22</td>
<td>04</td>
<td>17</td>
<td>10</td>
</tr>
</tbody>
</table>

3. Random Secret: - 76 36 18 48 24 44 58 21 88 08 13 03 74 81 49
4. Cipher text - Secret Key =

<table>
<thead>
<tr>
<th>Cipher text</th>
<th>Secret Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>05  08  07</td>
<td>0  0  15</td>
</tr>
</tbody>
</table>

- Subtract

\[
\begin{align*}
76 & - 71 = 15 \\
36 & - 28 = 08 \\
18 & - 11 = 07 \\
48 & - 48 = 00 \\
24 & - 22 = 02 \\
44 & - 39 = 05 \\
58 & - 2 = 56 \\
21 & - 19 = 02 \\
88 & - 08 = 80 \\
08 & - 13 = 05 \\
13 & - 03 = 10 \\
74 & - 74 = 00 \\
81 & - 03 = 78 \\
49 & - 49 = 00 
\end{align*}
\]

5. Plaintext = (Cipher text - Secret key) mod 26 =

| 7 | 24 | 15 | 4 | 17 | 4 | 13 | 0 | 2 | 17 | 24 | 15 | 19 | 8 | 14 | 13 |

6. Decode the Plaintext numeric Sequence back to the character form

| H | Y | P | E | R | E | N | C | R | Y | P | T | I | O | N |

So now the user has decrypted Cipher text back to the plaintext

Cipher text: - EIHAP WTXBGCWERK
Plain text: - HYPER ENCRYPTION

In this example the User A send plaintext HYPER ENCRYPTION to the user B with the help of modular addition scheme and the user B receive the cipher text EIHAP WTXBGCWERK for A and decrypt the cipher text back to the plaintext by using the same scheme of the modular addition but in reverse order. The scheme described here is so simple that it can be implemented by hand also without the need of complicated encryption software. But there are many problems that limit out the practical use of OTP.

IV. ADVANTAGES AND DISADVANTAGES OF OTP

Advantages of OTP:-
1. The One Time Pad is most optimal cryptosystem with theoretically perfect secrecy.
2. It is the most practical method that can be done on paper
3. One Time Pad can be used in Supercomputer
4. OTP can be mimicked with Stream Cipher
5. The OTP is only algorithm associated with Quantum Key Distribution.
6. OTP cipher text doesn’t provide any info about plain text this make it unbreakable system

Limitation of OTP:-
1. OTP requires the truly random One Time Pad which is practically non-trivial problem.
2. Secure Generation of Secure Pad (which must be as long as the message) and its exchange between the users is the most crucial problem of OTP.
3. OTP requires the unlimited number of random key because it allows one secret key to be used for single time.
4. The security of OTP scheme is only as secure as the security of OTP key
5. The need of an absolute synchronization between sender and receiver
6. Careful treatment of the secret pad to make it secure form Adversary and secure dispose of the key pad after being used it single time to prevent it from reuse is a serious issue.
7. If the Secret pad is lost or the pad is finished during the transaction then user have to drop its transaction and can start it again after sharing the new OTP.

V. HYPER ENCRYPTION:-

Introduction:- Hyper Encryption is a form of encryption invented by Michael O.Rabin. Hyper Encryption is a shared secret key block cipher scheme. Block size is taken usually of m=32/64. Hyper Encryption is the first encryption scheme
provedly providing the everlasting secrecy against the computationally unbounded Adversary. To make the system everlasting secret the system use the assumption of Bounded Storage Model introduced by Maurer. Hyper Encryption uses the shared secret key together with the public random bits. Although anyone can see the data but the decryption by
the Adversary without knowing the secret key is not feasible because of the limited storage space available to the Adversary as the assumption of BSM. It use the random key bit as secret pad as in OTP but if the secret key is compromised even then the message encrypted before the key compromise will be perfectly secure. Hyper Encryption
work with the multiple servers known as the Page Server Node (PSN). From which any user can request the random bits
page with the help of a secret key. A single page can be given only to the two users having the same shared secret key.
After that the page was destroyed completely by the PSN. This page of random bits is further used as the shared secret
pad b/w the user as in the OTP encryption scheme. After sharing the initial secret key through a secure way that used to
take the random bits page from the PSN all other transaction like making the secret pad and doing the message
transaction can be done on the public network. It also allows creating the new One Time Pad to make the continuity
of communication. It allows both the user to send the exponential number of message by using the initial shared secret key.
Hyper Encryption use the Fingerprinting scheme to share the OTP on the network and to authenticate the data

VI. OPERATION SCHEME OF HYPER ENCRYPTION:-

Hyper Encryption is a system that allows the two parties to transfer the secure data starting with an initial secret key and to make use of the publically available computer for random data. The parties can use the random page to create the one
tome pad. If we want to achieve the unconditional security then we must work with the private key cryptosystem private
key encryption in which the sender and receiver work with the same secret key.

Hyper encryption also initially starts with the sharing of a secret key. This shared secret key length depends upon the
length of the message. This key is shared b/w the sender and receiver with the help of a key distribution protocol such as Diffie- Hellman key Exchange protocol.

Then this shared secret key is used to request the Random bits pages from the PSN (Page Server Node). PSN gives
random bits page to the requesting user. PSN gives the pages by different type of operation. PSN usually store the pages
of random bits associated with a shared secret key. User access the random page with the help of the shared secret key
PSN gives the random bit page to the user who requested it with the secret key. The single page is given to only two
users with the same secret key. After that a new page is associated with the secret key. These random pages are used to
create the OTP for the encryption scheme.

After downloading the page from the PSN the both users A and B make sure that they have downloaded the same page of
Random bits that they are going to use as OTP by using the method of Page Reconciliation. Basically the page
reconciliation protocol used here use the Fingerprinting method for reconciliation.

In this the User A and User B computes the Fingerprints of the pages they have downloaded and then user A send its
fingerprint to user B and user B compare these fingerprint with its own. In this way both determine the common pages
they have downloaded. These pages work as the One Time Pad for the data encryption. A part of One Time Pad is always
kept for extending the Pad and the remainder of the Pad for the Encryption and Authentication of the message. User A
basically XOR the pad with the plaintext to make it secret and then A also compute the MAC (Message Authentication
Code) with a part of the secret key and send it with the Cipher text. User B verifies the MAC and then decrypts
the message. And then the Pad is destroyed completely to ensure that it can’t be reused.

In this way the Hyper Encryption provide everlasting security with assumption of Bounded Storage Model (BSM). In
BSM this is assume that the Adversary has the unbounded computational power but he has the limited storage capacity.
If there is the case that Adversary will be able to access the user transaction but he can’t be able to store the whole
message transaction at the same time If by some how the Adversary will be able to access the user’s secret key but his
storage capacity is limited so at the time when he will be able to use the secret key for adversary the secret key will no
longer be in use for the user, may be the user have already access the PSN random page. SO if the Adversary tries to
access the PSN page he will get the different page. Or somehow if the Adversary became able to access the PSN page
same as the User then at the time of page reconciliation the different page of the users will be discarded to make OTP.
And it will be impossible or having a very low probability that the Adversary can generate a page whose fingerprint is
same as of as the user random page fingerprint. So it is proved that with the help of the BSM Hyper Encryption provide
 everlasting security. That is impossible to break like OTP but it also provides the easier practical implementation of the
encryption scheme as compare to OTP.

Procedure of Hyper Encryption:- Suppose in this procedure we have two user A and B both want to transfer data in a
very secure way then to use the Hyper Encryption they can follow the following procedure

[1] Initially the user A and B should share a secret key (S) of length $N_{(2)}^a$ $a$ where $N(s) =$ System Block Size
And $a =$ number of PSN random pages to be used for OTP
Suppose $N(s) = 64$ and $a = 30$ then the initial shared key will be of 64.30=1920 Byte
[2] In the second step both the user will download the random page from PSN by sending request by the shared
secret key. In the best case user will download at least $a$ pages.
Random Page $\alpha =$ $(\alpha_1, \alpha_2, \alpha_3, ....... \alpha(n))$ n is the total number of random pages.
[3] In the 3rd step both user will do page reconciliation. They will generate the Fingerprints (F) of the random pages
they have downloaded send to each other thus check for the common pages they have downloaded.
They check if $A [ F(\alpha_i)] = B[F(\alpha_i)]$ or not. If the Fingerprints are not equal then the pages will be discarded

© 2014, IJARCSSE All Rights Reserved Page | 527
In the 4th step the user will create the One Time Pad (X) of the common random pages they both have downloaded. This OTP is further used for the encryption as the secret key.

User A will compute the Cipher text as \( C = M \oplus X \)

\( C = \) Cipher text  
\( M = \) Message  
\( X = \) OTP Secret key

User B will decrypt in the same way as \( P = C \oplus X \)

\( P = \) Plaintext  
\( M = \) Message  
\( X = \) OTP shared secret key

In this way both the user will be able to transfer their message in a provable secure, unbreakable way.

VII. ADVANTAGES/ LIMITATION OF HYPER ENCRYPTION

Advantages of Hyper Encryption:-

1. Hyper Encryption the optimal cryptosystem provides the unbreakable security to the user.
2. By the Use of the BSM it provides the everlasting security.
3. It provides the feature of extending the OTP with the help of the initial shared secret.
4. If the Secret key of the user is compromised even then the earlier encrypted message will be unbreakable.
5. Hyper Encryption uses the Rabin Fingerprinting scheme for the Authentication Purpose making the scheme more reliable.

Limitation of Hyper Encryption:-

1. The initial shared secret key length is very large.
2. Choosing of PSN for downloading the random page.
3. Reconciliation protocol can create problem if the Reconciliation message lost or processed as unordered way.
4. It is a complex method that can’t be implemented simply on paper.

VIII. HYPER ENCRYPTION AS AN ADVANCEMENT OF ONE TIME PAD:-

As we studied in this paper earlier One Time Pad uses a shared random secret pad as its key for the encryption scheme. But the generation of truly random sequence, exchange of pad secretly, use of the pad only single time and completely destroying the secret pad were being the problems. These problems make the OTP encryption system practical implementation difficult. So to overcome the practical problem and to use the concept of perfect security of One Time Pad the Hyper Encryption was introduced. It gives the solution to many problem of the OTP. But it still uses the basic concept of One Time Encryption scheme. Hyper Encryption initially shares a secret key. With the help of this key and use of PSN user download the pages of random bit these random bit pages are later used as One Time Pad key for encryption. The PSN work as the creator of random pages. Thus creation of random bit page became easy in Hyper Encryption as compare to OTP in which user have to keep track of the truly randomness of the secret pad. By the use of PSN the user only have to be sure about the security of initially shared secret key as compare to OTP in which the user have to be insure about the security of whole one time pad. In Hyper Encryption the user access the random page by the use of the PSN on a public network by using the secret key. In OTP the single time use of the secret pad is managed by the user so it has the probability of human error but In Hyper Encryption the PSN itself manage the property of single time use of the secret pad by associating the secret key with the random page and the page with the a secret key can be accessed only twice by the users. So it makes it more practical and easy to use the encryption scheme. In OTP the security of secret key is basically the security of encrypted data but in Hyper Encryption if the secret key is compromised to the adversary even then because of the assumption of BSM the encrypted data earlier by the key will be unbreakable. In this way we can say that the Hyper Encryption has all the property of a cryptographically unbreakable system. It uses the basic scheme of OTP with some advance assumption of BSM and proves to be a system giving the everlasting security to data. Hyper Encryption also provides a better practical implementation as compare to OTP.

IX. CONCLUSION:-

This paper has presented a study of two unbreakable encryption systems. In this we present the OTP as a provable secure unbreakable system. OTP is a cryptographically secure but practically loose system. We try to represent a more advance form of unbreakable encryption system, Hyper Encryption as the system that finds out the way trough all limitation of the OTP. Hyper Encryption, a cryptosystem that is provably secure against the unbounded computational power of the Adversary by the BSM assumption of storage space bound on Adversary. Hyper Encryption is information theoretically secure and also the cipher text remains unbreakable if the key is compromised by some way to Adversary. Hyper Encryption is cryptographically unbreakable scheme of encryption system with an easy way to practical implementation with a very basic model of everlasting security. This paper presents the Hyper Encryption as a system that find its way on the limitation of OTP scheme towards providing the everlasting security to the user data.

ACKNOWLEDGEMENT

I would like to express my deep gratitude to Assistant Professor Ms. Sunita, my research work supervisor, for her valuable and constructive suggestions during the planning and development of this research work. Her willingness to give her time so generously has been very much appreciated.
REFERENCES:


