SPEECH ENCRYPTION
IMPLEMENTATION OF ‘ONE TIME PAD ALGORITHM’ IN MATLAB

Y. Saleem, M. Amjad[1], M. H. Rahman, F. Hayat, T. Izhar, M. Saleem

University of Engineering and Technology, Lahore, Pakistan
[1]Islamia University, Bahawalpur, Pakistan
Corresponding Author E-mail: ysaleem@gmail.com

ABSTRACT—One-Time Pad is one of the most secure encryption technique used to secure highly confidential information over the un-secure network. First, OTP is explained with example. Then it is implemented in MATLAB. The implementation of OTP consists of recording, encryption, and decryption functions, which makes heavy use of MATLAB’s GUI.

Key words– One-time pad, OTP, MATLAB, Encryption, Speech

INTRODUCTION

The One Time Pad (OTP) algorithm is an encryption technique used in cryptography, which is recognized as impossible to crack if proper procedures followed.

Frank Miller in 1882 was the first to describe the one-time pad system for securing telegraphy.The encryption process includes the treatment of every data bit of the original data called ‘Plain Text’ with a bit of secret arbitrary key called ‘Pad’ of the equal length as the ‘Plain Text’.

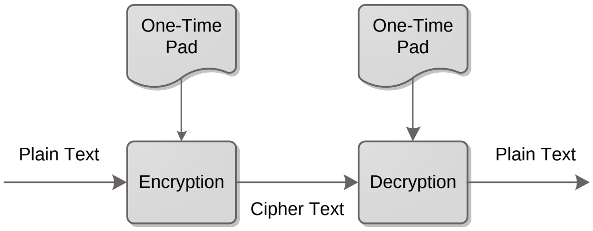


Fig. 1 Block Diagram of One Time Pad Algorithm

The encrypted result ‘Cipher Text’ is impossible to break without having the ‘Pad’, if the used ‘Pad’ is truly random and as large as the ‘Plain Text’.

The pads should never be used again to maintain the security. As long as the pads remain unique, there is nothing that can be used to attach the encryption using statistical analysis or pattern matching.

The term "pad" in the name of Algorithm, derived from the earlier implementations, where the secret key material was distributed as pad of paper, due to its easy destruction (Wikipedia, 2012).

ONE-TIME PAD ALGORITHM

A. Rules of ‘One-Time Pad’ Algorithm

- The Secret key should be as equal as or longer than the message that must be encrypted.
- The key should truly random
- Key and plaintext are calculated modulo 2 (binary), or modulo 10 (digits), or modulo 26 (letters)
- Each key should be used once, and both sender and receiver must immediately destroy their key after use.
- There should only be two copies of the secret key: one for the sender and other for the (*http://users.telenet.be/d.rijmenants/en/onetimepad.htm*)

B. ***Perfectly Secure Cryptosystem:*** If there is a need to send highly confidential information over the non-secure and open channels such as telephone and data network, then there is only one truly secure technique that is One-Time Pad. This is implemented by XOR the original data with the key to make the encrypted data. Then send this data to network. On the receiving side again decrypt the data by simple XOR the encrypted data with key to obtain the safe and secure original signal. (Pro-Technix, 2012)

Key	Data	Encrypt	Decrypt
		K XOR D	*K XOR E*
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Figure 1. **XORing for Encryption & Decryption**

C. ***Real Life Example of One Time Pad using Mod 26:*** Suppose, we have to send the message ‘HASSAN’ to the receiver, and the corresponding key is ‘RAHMAN’. Let’s assign the numeric values to each letter, as ‘0’ to A and so on. The numerical values of corresponding message and key letters are added together through modular addition, modulo 26. The procedure is as follow:

If the sum goes up more than 25, then restart the counter.

The decryption is similar to the encryption but reverse in the order.

Here 'YAZEAA' is the encrypted message sent over the network to the receiver. Here, receiver has to perform the subtraction. If the result is in negative number, then subtract the result from the 26.

MESSAGE TEXT with assigned values					
H	A	S	S	A	N
7	0	18	18	0	13
PAD / KEY with assigned values					
R	A	H	M	A	N
17	0	7	12	0	13
Message + Key					
24	0	25	30	0	26
Message + Key (mod 26)					
24	0	25	4	0	0
Cipher Text					
Y	A	Z	E	A	A

Figure 2. **Encryption of Message**

Cipher Text with assigned values					
Y	A	Z	E	A	A
24	0	25	4	0	0
PAD / KEY with assigned values					
R	A	H	M	A	N
17	0	7	12	0	13
Cipher Text - Key					
7	0	18	-8	0	-13
Cipher Text - Key (mod 26)					
7	0	18	18	0	13
MESSAGE TEXT with assigned values					
7	0	18	18	0	13
H	A	S	S	A	N

Figure 3. Decryption of Message

MATLAB GRAPHICAL USER INTERFACE (GUI)

Within MATLAB, GUI tools enable the programmer to perform tasks such as creating and customizing plots (*plottools*), fitting curves and surfaces (*cftool*), and filtering and analyzing signals (*sptool*).The implementation of OTP in MATLAB requires extensive use of GUI (graphical user interface). This GUI enables users to carry on tasks interactively through interactive controls such as dialog boxes, buttons and sliders (MathWorks, 2012), (One Time Pad, 2012).

There are two methods to create GUI environment:

a) Creating a MATLAB GUI Interactively

b) Creating a MATLAB GUI Programmatically

GUIDE (GUI development environment) is provider of tools for the designing, analyzing and programming GUIs. Using the GUIDE Layout Editor, the user can design his GUI graphically. Then GUIDE automatically generates the code of MATLABthat defines all component properties and establishes its framework for GUI callbacks (routines that execute when a user interacts with a GUI component).

The design and development can be controlled better by creating MATLAB code that defines all properties and behaviors of component. There is built-in functionality in MATLAB create your GUI programmatically. These include user interface controls(such as dialog boxes, sliders and push buttons), containers (such as button groups and panels), and for Windows users also ActiveX controls. (Yan Zhang, 2009)

Matlab Impelmentation of otp algorithm

The basic implementation of One-Time Pad is as follow:

a) Record the speech from microphone.

b) Convert it to digital format.

c) Encrypt it using Encryption algorithm with secret key.

d) Send the voice to other site digitally.

e) The reciever will receive the 'cipher' encrypted sound.

f) Eecrypt it using Decryption algorithm with secret key.

The implementation of One Time Pad algorithm in MATLAB contains multiple function calling. Each function or method has specific purpose. There are total four methods, that include Main Method (named OnetimePad), Recording, Encryption, and Decryption methods.

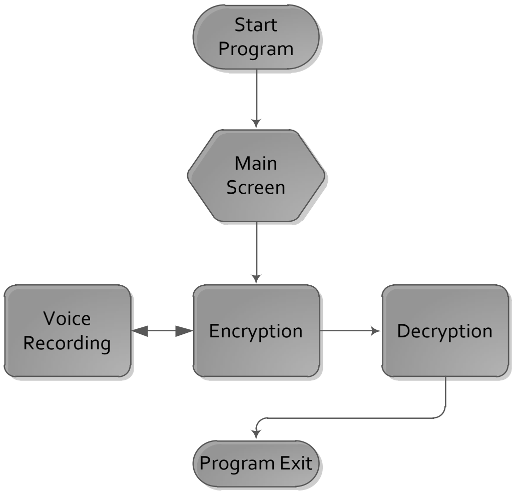


Figure 4. **Methods of One Time Pad Algorithum**

Each of the four methods and their programming is explained in details:

A. ***'One Time Pad' Function:*** The 'One Time Pad' function is the main function that is executed as the program runs. It calls all two working methods 'Encryption Process', and 'Decryption Process', by clicking on the respective button.

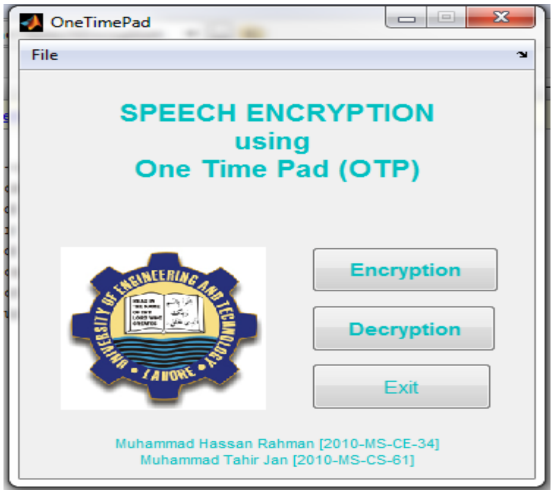

OneTimePad
File
SPEECH ENCRYPTION
using
One Time Pad (OTP)
UNIVERSITY OF ENGINEERING AND TECHNOLOGY LAHORE
Encryption
Decryption
Exit
Muhammad Hassan Rahman [2010-MS-CE-34]
Muhammad Tahir Jan [2010-MS-CS-61]

Figure 5. **'One Time Pad' (Main Function)'s GUI**

The development of this GUI is consisting of usage of the static text, push button, and axes. The Title is written using the 'static text'. The button is embedded using the 'push button' option. The Logo is display on the GUI using the axes and use of the command 'imshow'.

The programming code of this GUI contains the pre-defined 'GUI Initialization Code' which is already written (built-in) when new GUIDE is developed. When Encryption button is clicked, it calls the 'Encryption Process', on pressing the Decryption button, 'Decryption Process' is executed. When Exit Button is pressed, the Program terminates.

B. ***'Recording Process' Function:*** When the 'Encryption Process' is executed by click the Encryption button on the main screen, the first thing is add the original voice to the database. If there is no voice sound saved before, or if new sound is record, the 'Record' button is pressed on the 'Encryption Process' GUI. It calls the 'Record Process' function.

The development of this GUI is consisting of usage of the static text, push button, and axes. The Title is written using the 'static text'. The button is embedded using the 'push button' option. The Plot is display on the GUI using the axes.

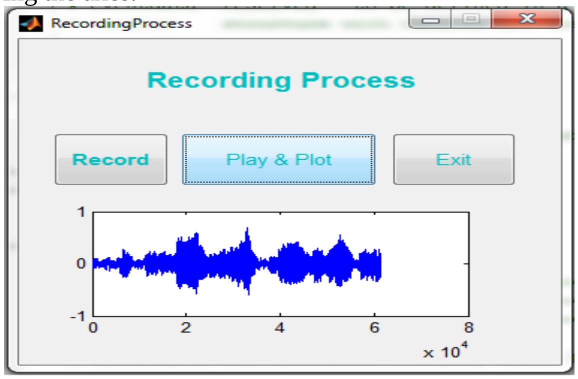


Figure 6. **'Recording Process's GUI**

The programming code of this GUI contains the pre-defined 'GUI Initialization Code' which is already written (built-in) when new GUIDE is developed.

When 'Record' Button is clicked, the empty text file is written on the disk in which all the sound information will be saved. Then the built-in audio recorder is called to save the speech. audiorecorder (Fs,nBits,nChannels);

Then the wait bar is displayed until the complete recording of the sound file waitbar (0,'Please Wait, Recording');

Then the recorded sound wave file is converted to uint8 data type by using this command.

Getaudiodata (recorder, 'uint8');

Then the recorded data in decimal format is converted to the binary format using this command.

BinaryData=dec2bin(OriginalSpeech);

Then the binary data will be saved in the text file for further processing in the encryption process.

When 'Play & Plot' button is pressed, the recorded original voice is played and plot is displayed on the area specified by axes on the GUI. The recorded file is read by 'wavread' and played by 'wavplay' commands, and the plot is display by using the 'plot command'.

When 'Exit' button is pressed, it terminate the 'Recording Process' and give control back to the 'Encryption Process'

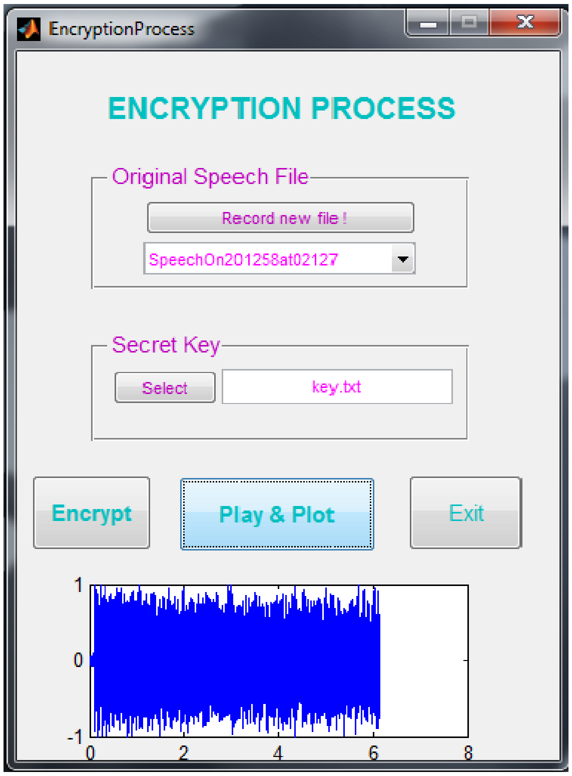
C. ***'Encryption Process' Function:*** When the 'Encryption Process' executed, the first thing the user have to have to do is, add the original voice, either by recording a new voice, or by selecting the previously recorded voice.

When 'Record' button is pressed, it calls the 'Recording Process', which is already explained in the last heading. The other option is select the previously recorded voice by using the popup menu, and select the desired option.

The second job is to select the 'Secret Key' by clicking the 'Select' button; a browse window will be opened, giving the choice to the used to select the key. The key is taken as text file that contain the binary data only. One thing, to remember is that, in OTP the secret key must be at least equal or larger than the original file. The edit text box will show the selected key's name on the screen.

The development of this GUI is consisting of usage of the static text, push button, popup menu, edit box and axes. The Title is written using the 'static text'. Selecting of the original speech is using the 'popup menu'. The selection of secret key is displayed on the screen is displayed by 'edit box'. The button is embedded using the 'push button' option. The Plot is display on the GUI using the axes.

The programming code of this GUI contains the pre-defined 'GUI Initialization Code' which is already written (built-in) when new GUIDE is developed.



SpeechOn201258at02127

key.txt

Figure 7. **'Encryption Process's GUI**

When 'Record' Button is clicked, the 'Record Process' is called. The following line of code will generate the file name on current date and time format.

ce=fix(clock);

File Name = strcat('SpeechOn', int2str(ce(1)),)

The built-in methods of Popup menu, and edit box is written in the 'Encryption Process' are defined by MATLAB.

When 'Encryption' button is pressed, first, the original speech file is open in read only mode. Then the secret key is opened in read only mode. Then bit wise XOR function is performed on both files of original speech file and secret key.

```
for j=1:TotalFile
Encrypted Data(1,j)=
Bitxor (new Sound(1,j),new Key File(1,j))
end
```

Then, the data is saved in the uint8 format, and then all the MATLAB workspace variables are saved to a file by using this command:

saveEncryptionRegister;

Then all the encrypted data is written into a new file and a message box appears at the end of the encryption to inform the user, the completion of the encryption process.

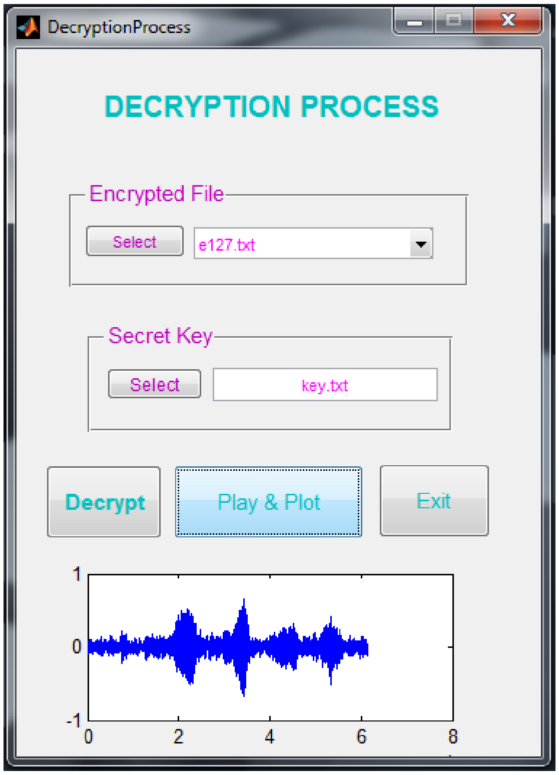
When 'Plot & Play' button is pressed, the 'audiorecorder' records the sound of the file saved by name of "EncryptionRegister". The sound file is written on the disk by using the command 'wavwrite', and played by using 'wavread' and plotted by using the 'plot' command respectively.

When 'Exit' button is pressed, the 'encryption process' terminated and the control back is it transferred back to the main screen of the 'One Time Pad'.

D. ***'Decryption Process' Function:*** When the 'Decryption Process' executed, the first thing the user have to have to do is, add the encrypted voice, by selecting from the pop-up menu.

The second job is to select the 'Secret Key' by clicking the 'Select' button; a browse window will be opened, giving the choice to the used to select the key. The key is taken as text file that contain the binary data only. The edit text box will show the selected key's name on the screen.

The development of this GUI is consisting of usage of the static text, push button, popup menu, edit box and axes. The Title is written using the 'static text'. Selecting of the encrypted speech is using the 'popup menu'. The selection of secret key is displayed on the screen is displayed by 'edit box'. The button is embedded using the 'push button' option. The Plot is display on the GUI using the axes.



e127.txt

key.txt

Figure 8. **'Decryption Process's GUI**

The programming code of this GUI contains the pre-defined 'GUI Initialization Code' which is already written (built-in) when new GUIDE is developed.

When 'Select' Button is clicked from the 'Encrypted Speech' option, the browser box opens to select the desired encrypted file which the user wants to decrypt. The popup menu will show the selected encrypted file.

When 'Select' Button is pressed from the 'Secret Key' option, the browser box opens to select the desired key. The key should be same which is used for the encryption of the original file.

The built-in methods of Popup menu, and edit box is written in the 'Encryption Process' are defined by MATLAB.

When 'Decryption' button is pressed, first, the encrypted speech file is open in read only mode. Then the secret key is opened in read only mode. Then bit wise XOR function is performed on both files of original speech file and secret key.

```
for j=1:TotalFile
DecryptedData(1,j)=
bitxor(newSound(1,j),newKeyFile(1,j))
end
```

Then, the data is saved in the uint8 format, and then all the MATLAB workspace variables are saved to a file by using this command:

```
saveDecryptionRegister;
```

Then all the decrypted data is written into a new file and a message box appears at the end of the decryption to inform the user, the completion of the decryption process.

When 'Plot & Play' button is pressed, the 'audiorecorder' records the sound of the file saved by name of "DecryptionRegister". The sound file is written on the disk by using the command 'wavwrite', and played by using 'wavread' and plotted by using the 'plot' command respectively.

When 'Exit' button is pressed, the 'decryption process' terminated and the control back is it transferred back to the main screen of the 'One Time Pad'.

APPLICATION

The One-Time Pad is considered as the most secure type of encryption. Now a days, it is used in secure transmission and receiving of image processing, computer networks, medical data, and web access. (Fengling, 2010), (Jeyamala, 2010),(Yan Zhang, 1996)
Most of the online money transfers and online banking uses the OTP algorithm at the back end. (DonghuaXu et al., 2002)

EXPLOITS

VENONA, the successful operation took place by British to 'hit' the encrypted information by Soviet intelligence, as they compromised the security by re-used one-time pads after some time. Therefore, it is strongly advised to destroy the pad after the use.

REFERENCES

Donghua Xu, Chenghuai Lu and Andre Dos Santos, Protecting Web Usage of Credit Cards Using OTP Cookie Encryption, Proceeding of ACSAC, 18: 1-8(2002).

Fengling, Highly efficient OTP Key Generation For Medical Data Protection, 5th proceeding of ICIEA, 5: 330-335(2010).

Jeyamala, Image Encryption Scheme Based on One Time Pads: A Choatic Approach , Proceeding of International conference on ICCCNT, 1:1-6(2010)

Yan Zhang, A Novel Scheme for Secure Network Coding Using One-time Pad,Proceeding of International conference on NSWCTC, 1: 92-98(2009).

Internet website, Wikipedia, http://en.wikipedia.org/wiki/One-time_pad, (2012).

Internet website, One Time Pad, http://users.telenet.be/d.rijmenants/en/onetimepad.htm, (2012).

Internet website,Pro-Technix, http://www.pro-technix.com/information/crypto/pages/vernam_base.html, (2012).

Internet website,MathWorks, http://www.mathworks.com/discovery/matlab-gui.html, (2012).