Data Encryption Using Morse Code

Aditya Pathak*, Anmol Kaur, Sagar
Department of Computer Science and Engineering, Chandigarh Engineering College, Landran
Email Id: *adityapathak2874@gmail.com

Abstract: **Cryptography in general means hiding, while in technical terms cryptography means protecting data from unauthorized access of someone, or cryptography can be considered as a method that ciphers the data so that the data can neither be read nor understood by humans. With the increasing level of internet consumption, the security of our data is the main concern. Due to increasing cyber-attacks, and over-relying on the internet, a lot of users' data has been compromised. This has brought our attention to data security and cryptographic algorithms. Data security ensures the data of users is not being compromised and is present in such a format that an intruder won't get access to our data, it ensures that the data is accessible to the intended user only, and anybody else can neither read nor change the data. To achieve such security, some algorithms or processes are needed. One such algorithm can be derived using Morse code since data in Morse code uses dots and dashes to represent alphabets and numbers. Even if such encryption is used directly, it may cause some threat to the user'sdata as anyone with knowledge of Morse code can easily decrypt it, so to get more safety, the encrypted data is needed to be encrypted again with some other algorithm. Now, other than data safety, the safety of the algorithm is also required, as if someone gets to know about the algorithm, they can decrypt the data. The Python programming language provides a module named Cryptography in which Fernet can be used to encrypt the algorithm file as well as the data file again. Cryptography in python uses a symmetric encryption technique, i.e., it uses the same key to encrypt and decrypt the data. This technique is faster compared to asymmetric techniques. This paper demonstrates how Morse code, time & Python's Cryptography module can be used together to provide maximum data safety.**

Keywords- **Cryptography, encryption, decryption, Morse code, Data Security, Symmetric Encryption & Asymmetric encryption.**

I. INTRODUCTION

Cryptography – The term cryptography is derived from a Greek word which is kryptos which means hidden. It can be considered as a method of securing data so that the intended recipient of the data can only read the content of the data [1]. This cryptography is closely associated with encryption and decryption. Encryption refers to converting the content into a non-readable form which is more commonly called cipher text, while opposite to it, decryption uses an algorithm that converts encrypted content to a human-readable form or the process by whicha readable content is changed to cipher text is called encryption while changing of this cipher text to human-readable form is called decryption [5].

Cryptography can be used to send some critical data because it ensures that even if the data is leaked, the intruder does not get any idea about the content of the data. Nowadays, the most common form of encryption involves the use of a key that can be used for both encrypting and decrypting the data; this ensures that the data can only be accessed through a key only. To get higher safety this key too must be generated by some algorithm and maximum salting should be done. Hence, it can be concluded that cryptography is the fabrication of users' data so that it can remain hidden from intruders.

Morse code is the oldest method used for wireless data transfer in an encrypted format. In earlier times this was used in telegraphs, which sent the alphabet in the form of long and short sounds. The long sound represented a dash, while the short sound represented dots of Morse code. To send Morse code data, the sender was required to send the data at a rhythm as the dash lasted for three times the time of dots, this makes it quite clear that Morse code is not a code that can be understood by humans easily without proper training.

II. LITERATURE REVIEW

There are many existing methods of communication which people use to communicate and share their information among others, some such languages use our general text such as that we write in our normal English, or that deaf and blind people use to communicate which is sign language or Braille script, etc. One such language is Morse code which could either be transmitted as a light signal or by sound transmission, even this can be used for encryption technology [10].

This Morse code can now be used as an algorithm for cryptography, other than that this can also be used for sending and receiving a video message by using Eye's blinks as the Morse code, this can be implemented by Open CV [7].

Further, this technology can be upgraded with more secure encryption and pattern rotation and salting which has been discussed below.

Existing Methods of Morse codes' implementation

- **Government officials** – This technology has been used for a long time by government officials either to send or receive data safely [8].
- **Communication** – Morse code has been being usedfor a very long time; it was even invented for faster data transfer.
- **Conveying message secretly** – Morse codes' sound can also be used to convey some important data to the intended person as if there is no source to see the code.

III. NEED FOR ENCRYPTION

There is not just one use of encryption, with the rising use of the internet and cyber-attacks, every organization prefers better security both for them and their consumers. Encryption is also one such strategy that provides security by scrambling the readable form of data into a non-readable form.

1. Authentication: In this era of the internet, a certificate is used by websites for authentication of the public and private keys, this is done by an SSL certificate [4].

2. Privacy: Encryption guarantees that the data will be safe and no other mid-person would be able to read the data.This method prevents the access of users' private content by other organizations, hackers, spammers, internet service providers, etc.

3. Regulatory Compliance: There are many government organizations and private agencies that have thepolicy of making it compulsory for the organization to encrypt the personal data of users. HIPAA, PCI-DSS, and GDPR are some samplings of regulatory or compliancestandards that enforce encryption.

IV. MORSE CODE

A. *History of Morse Code*

Morse code is a method of communication that was invented by Samuel Morse for faster message transfer. This technology was used a lot in his time in radiotelegraphs. In this, each character of the alphabet and numbers is assignedto a symbol consisting of dots (.) and dashes (_) [6]

B. *The International Morse Code*

In the proposed paper we have discussed various strategies that can be implemented over Morse code. To provide more data security to users several more changes are made in the international morse code symbols like rotation and salting.

The international Morse Code symbol is mentioned in bellow chart.

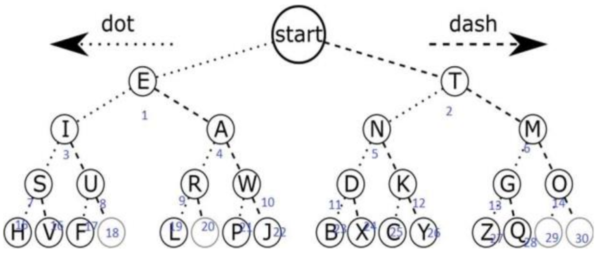
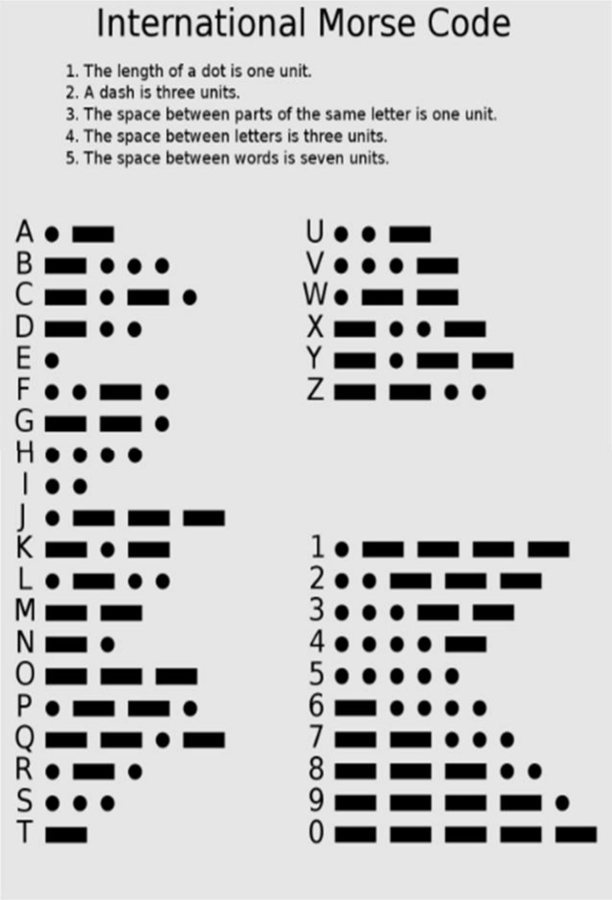


Fig 1: Morse Code tree [3]

C. *Scenario of our Morse Model*

In this model, we will be using the morse code only for character encryption, but at the same time for safety this encrypted data will be rotated according to the time at which it has been saved, if the data contains the word Helloin it, then it's morse equivalent will be ".... . .-.. .-.. ---". Consider if this data is saved at a time when the second is 1,then the Morse code will shift 1 unit right and give the output code and its last character will contain the original Morse value of 1. So, the code at this time will be ".. ..-. -- -- .--. .----". Now if someone will try to decrypt the generated code, he will get the out text as "ifmmp1" which is meaningless if compared to the original text.


International Morse Code
1. The length of a dot is one unit.
2. A dash is three units.
3. The space between parts of the same letter is one unit.
4. The space between letters is three units.
5. The space between words is seven units.
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
1
2
3
4
5
6
7
8
9
0

The International Morse Code [2].

Later on, more modifications will be made to the code so that the decryption will get more difficult for the user all the encryption steps and algorithms are mentioned further in the paper.

V. STRATEGIES INVOLVED

The following are the strategies that have been included for storing the data of the user so that even if some intruder gets the method to break Morse code even then he won't beable to decrypt the data. This means not only circular rotation and Morse but certain strategies will be used to provide more data security.

A. *Time and Circular Shift/ Fourth Level*

As discussed earlier, Circular rotation similar to the circular array will be made while encrypting and decryptingthe data, so that no intruder can access the data directly by decoding the Morse code. This is the fourth level of encryption, i.e., the easiest encryption, in this only the morse data will be circularly rotated (as if time in second is2 then the order will be like A will change to C and Z will be B i.e., alphabets will start with C and end with B) and this data will be stored in the file, to get hold of the shift the value of time will be added behind the morse content. This time will be playing a major role at all levels of encryption.

B. *Salting/ Third Level*

In this stage, the data encrypted will be stored (data converted to Morse code) in the form of a string now here the decrypting function will decrypt and get the value of time from data that is already placed at the end of the string.

Salting is a method of insertion of data/ character in mid of some content or password to avoid string creation by concatenating some random or known patterns [8]. This is the most used step in the case of the cyber security field, it protects the content to be found by random guesses. Salting provides a longer length to content that increase the time being taken to break the password as well as it also saves the data even if it's decrypted as salted character generally do not form a pattern.

Now since we have that value of time, and length of string, we will divide the length of the string by time and get the integer value, the morse string will be split by a factor of two; in these parts, another string that has already been shifted according to that time will be placed in encrypted form, with an order that the next character will beat a position

Next position = ((time*position of the previous character)
% 26),
Now this step will make it impossible to match the pattern and even decrypt the data.

To decrypt this data since the value of time will remain at the end, the user will simply break at the same position, decrypt and remove the character at the first position.

C. *File Encryption/ Second Level*

At this level we have generated a strongly encrypted content, now the next task will encrypt the file in which encrypted morse code is present here a python package called Fernet will be used to generate a key, and this key will be used to encrypt the file in the next step a random sequence of data will be generated which will be used to decrypt the content (morse code) and this data is completelyrandom.

This step too will involve all the steps which are on the third level, i.e.; salting will be done even at this place too, to provide maximum data security.

D. *Encryption of Encryptor and Decryptor/ FirstLevel*

As the name suggests in this the program that is encrypting the data will be encrypted and will be decryptedonly while the encrypting or decrypting function is called and as soon as the function executes, the main encryptor program gets encrypted.

VI. ALGORITHM

A. For Encryption

```
1. Begin.
2. Get Content or content location.
3. Encrypt the content to Morse code.
4. Add ten modulo of time in encrypted Morse code.
5. Use the modulo and perform salting.
   5.1. Rotate the alphabet according to time.
   5.2. Place the first salting at the position Morse code [time].
   5.3. Next salting will be placed according to the formula Next position = ((time*position of the previous character) % 26
   5.4. Return this salted content.
6. Encrypt the Salted file by fernet and generate a key forit.
7. Repeat step 5 on the key.
8. Encrypt the file which contains the algorithm of encryption using External Fernet.
9. End.
```

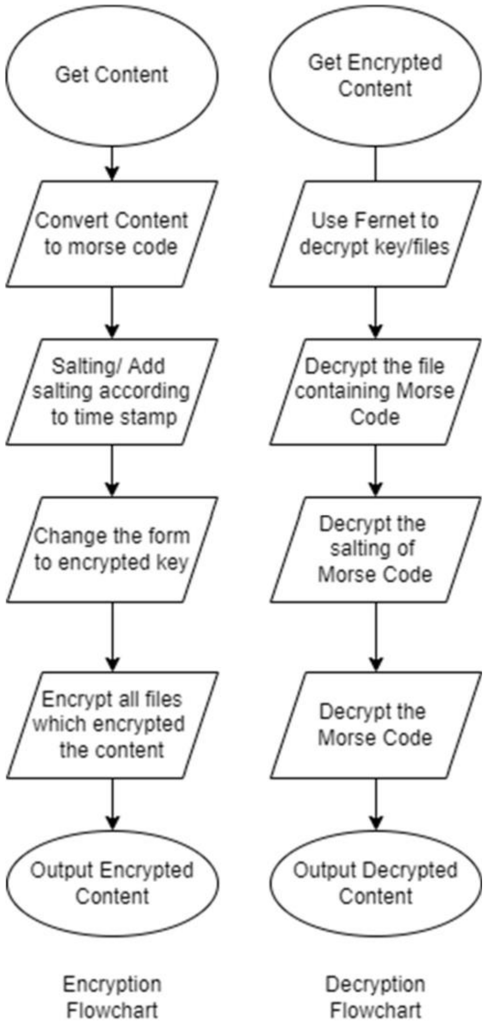

Get Content
Convert Content to morse code
Salting/ Add salting according to time stamp
Change the form to encrypted key
Encrypt all files which encrypted the content
Output Encrypted Content
Encryption Flowchart
Get Encrypted Content
Use Fernet to decrypt key/files
Decrypt the file containing Morse Code
Decrypt the salting of Morse Code
Decrypt the Morse Code
Output Decrypted Content
Decryption Flowchart

FIG 2:Encryption and Decryption Flowchart.

B. For Decryption

To decrypt the data, we have a lot more tasks than compared to encryption. The steps involved in it are mentioned below:

```
1. Begin.
2. Get content/ file location.
3. Decrypt the file that performs the decryption task.
4. We have the key now
   4.1. Use time & formula to get the location of saltedcharacters.
   4.2. Store the locations of characters in an array.
```

    4.3. Start selecting an element from the end of thearray.
    4.4. Remove the character at the location given by thearray.
    4.5. Repeat step 4.4 until the array is empty.
    4.6. Return the string.

5. Repeat step 4 on the string that has been returned.
6. From this, get the time stamp from the string and remove the salting according to the formula.
7. Parse this string to Morse Code Decrypting function.
8. Return String.
9. End.

Consider a word Cryptograph is given for encryption thenthe outputs are as follows:

1. After Morse Code Conversion/ Fourth Level

   --. ...- -.-. - -..- ... -.- ...- . - .-.. ....-

   At time stamp 4.

2. The encrypted data produced by fernet, this data doesnot contain salting for now, “*gAAAAABin5m4in2cR19HGsBdG8EdAV9XR0PASB UqhO7DiyJBFUqo2lMWjNVNHqQOLxkQYxiRdzatt_ 8eIh3UwpHEskxKBbLR_O5ibzDTWSmCavfd-dOQIU2aoUiVSnxz30mdNvFPBLGvceYCLkuiESUv9 VV1Pa-dHw==*”

This method has been tested and implemented and the result was quite large which will be impossible to find if tried.

VII. MORSE CODE AND OTHER TECHNIQUES

The most popular division of cryptography at present is:

a) Symmetric Key Encryption and
b) Asymmetric Key Encryption.

In symmetric key encryption, both encryption and decryption are done using the same key, while in the case of asymmetric both the keys are different which means there is a public key for encryption while a private key for decryption. In comparison, the symmetric key system is a lot faster than that of the asymmetric key system. The algorithm discussed here too works on the basis of the symmetric key system [9].

VIII. CONCLUSION

Cryptography is an essential part of communication anddata transfer fields; it provides maximum security fromany intruder or hacker from getting a user’s data. While using various encryption technology the best strategy willbe to use a dynamic key and dynamic salting as this willgive a higher edge from guessing and even if someone willtry to decrypt, he/ she will need to know the saltingparameters and strategies which is used to do that salting. This method will be quite useful as this gets the characterand convert it to morse code which means it even increasesthe length of encrypted data and later salting on thisencrypted morse code makes it more difficult even tocreate a character from salted morse code, after this the encryption using fernet’s key and again encrypting andsalting on the fernet’s key makes a double layer of dualsafety wall, with a long length, this makes it among the most difficult encryptions to decrypt, even it is Symmetric.

REFERENCES

[1] https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

[2] https://en.wikipedia.org/wiki/Morse_code#/media/File: International_Morse_Code.svg

[3] https://stackoverflow.com/questions/46922333/c- unknown-memory-issue-binary-tree-exercise

[4] https://www.simplilearn.com/data-encryption-methods-article Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi, Research on Various Cryptography Techniques, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019

[5] Manisha Barse, Rodney Manuel, Morse Code - A Security Enhancer, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[6] Sumanth Naga Deepak, B Rohit, Ch Akhil, D Sai Surya Chandra Bharath and Kolla Bhanu Prakash, An Approach for Morse Code Translation from Eye Blinks Using Tree Based Machine Learning Algorithms and OpenCV, Journal of Physics: Conference Series, ICASSCT 2021, 1921 (2021) 012070IOP, doi:10.1088/1742-6596/1921/1/012070

[7] Ashwini Aher, Karishma Musale, Surabhi Pagar, Sayali Morwal, Implementation of Smart Mobile App for Blind & DeafPerson Using Morse Code, International Journal of Research in Advent Technology, Vol.2, No.2, February 2014 E-ISSN: 2321-9637

[8] Sanjeev Kumar Mandal, A R Deepti, A Review Paper on Encryption Techniques, 2019 IJRAR June 2019, Volume 6, Issue 2

[9] Soumya Krishnan and Dr.K.Selvakumar, Securing Data And Information In The Cloud Using Dna And Morse Coding Techniques Journal of University of Shanghai for Science and Technology, Volume 23, Issue 11, November – 2021 ISSN: 1007-6735.