NEW PASSWORD TECHNIQUE USING TURING MACHINE AND CRYPTOGRAPHY

Sandip Kumar Shrivastav, Bramah Hazela, Vineet Singh
Research Scholar, Asst. Professor, Asst. Professor
Department of Computer Science & Engineering
Amity University, Lucknow, Uttar Pradesh, India

Abstract : Presently multi day's protection is the primary issue to sending data starting with one point then onto the next in information transmission. Encryption of information is the best method for PC science worried about creating plans and recipe to accomplish information and data security. In its game-plan, it enables succession to be encoded as figure content where it is very hard to peruse or perceive the codes where unscrambling is the strategy to changing encoded content into the first message and data. In this paper we present a calculation for information encryption and unscrambling which depends on cryptography and Turing machine technique. Furthermore, information encryption utilizing weird number framework can make accessible physical or considerable security to data—permitting refreshing as it were to approve clients. This calculation is utilized odd number framework to scramble information and we propose a better information encryption and decoding procedure, which will offer better security towards every single imaginable methods for assaults while information transmission.
we develop an adaptively secure utilitarian encryption for Turing machines plot, in light of lack of definition jumbling for circuits. Our work puts no limitations on the sorts of Turing machines that can be related with every mystery key, as in the Turing machines can acknowledge contributions of unbounded length, and there is no restriction to the depiction measure or the space intricacy of the Turing machines.

In this research-paper authors have suggested to generate a new password technique with the help of Turing machine and cryptography method. In this process as an user which are use to create a password for his data security in any type of social media, So the user provide his password as input plaintext to the Turing machine, Turing machine reads the plaintext and change the given data as Turing machine function manage in the state transition with the help of cryptography technique encrypt the data using cryptography method Caesar Cipher which are connected to the network which decrypt the data with the help of Turing machine in the form of cipher text using the sift operation in the cryptography which provide at last given initial input which is given by the user at the starting and generate the password which is want by the user.

Keywords **- Turing machine, Cryptography, Finite state, Password entropy, Encryption, Decryption, User behavior.**

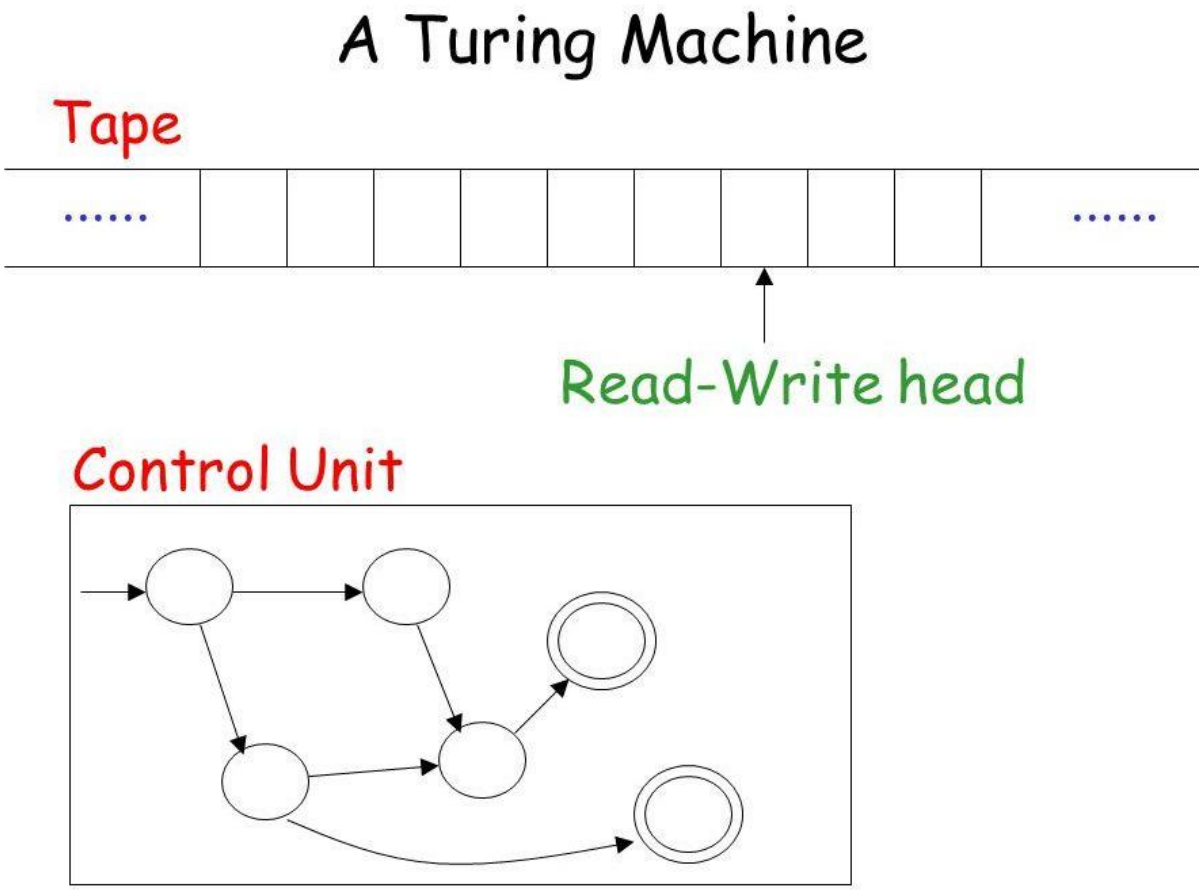
Introduction

TM Presented by Alan Turing in 1936. Turing – Machine can comparably perform math and algorithmic system which can be performed just by individuals or PCs. A straight forward scientific model of a PC. Models the processing capacity of a PC. A (TM) is a limited finite state machine with an unbounded tape and a tape head that can peruse or keep in touch with one tape cell and move left or right. It regularly acknowledges the information string, or finishes its calculation, by entering a last or tolerating state. Tape is use for info and working storage.

Turing-Machine have following component-

- Controller
- Read/Write Head

- Tape



Turing machine is logical and physical gadget. The Turing machine can be logical gadget then we convert it to physical gadget one model we can make a TM that invert a string. Each machine have an information and a yield between the information and yield there is process The contribution to any TM is only a String. The procedure here we will make it as indicated by our need later we will perceive how to structure it the output is likewise a string.

Our objective in planning any Turing machine is to actualize our thought in term of states and advances so we have to think about our resources. The just asset that we have is long tape it's precisely like an exhibit.

Tape

According to Turing, "When an individual makes image on a 1-dimensional paper in the midst of estimation process (as opposed to 2-D paper) can be seen as a tape restricted into cells."

Here is what you can do with this tape

- you can read cell by cell
- you can change the content of the cell
- you can move to the right or to the left
- you can use as much as you want from the tape it's like infinite storage store as elements as you wish

Controller

In current PCs the Theoretical partner of focal handling unit is Controller. It comprises of an improved type of limited state machine, and accordingly envelops the preparing some portion of the machine.

Head

It goes about as the middle person between the tape and the control units. The control part can collaborate with the tape by perusing from the present position of the head and furthermore keeping in touch with the present position. The Control can likewise make the head move to the neighboring places of the tape.

At the point when the Turing Machine chooses to move the head left (or right), the tape substance stay unaltered. The tape is of vast length on the right-hand side; it is anyway not unbounded on the left-hand side. We can along these lines envision the areas on the tape as filed, beginning from 0 at the furthest left position and after that expanding by 1 with each area to one side. There is one extraordinary case that happens when a Turing Machine is at present at position 0 and attempts to move the head one stage to one side; when this occurs, the Turing Machine quits executing and we state that the machine hangs.

A Turing Machine can conceivably run always when executing; we allude to this conduct as separating. We would in a perfect world anyway have our Turing Machine stop. This normally happens when it achieves a state what's more, a situation for the head whereby it doesn't have any next state to go it. We distinguish three unique cases for when our Turing Machine stops. Turing-Machine in a general sense plays out specific exercises on the tape which are according to the accompanying:

- Perusing a word for the preparing of word transformation.
- Composing another word in the cell being right now filtered.
- Moving the cell left/right of the present cell.

Automata

Automata hypothesis is the investigation of conceptual machines and automata, just as the computational issues that can be explained utilizing them. It is a hypothesis in hypothetical software engineering and discrete arithmetic (a subject of concentrate in both science and software engineering).

The figure at right represents a limited state machine, which has a place with an outstanding kind of robot. This robot comprises of states (spoke to in the figure by circles) and advances (spoken to by bolts). As the machine sees an image of information, it makes a change (or hop) to another state, as per its progress work, which takes the present state and the ongoing image as its sources of info.

Automata hypothesis is firmly identified with formal language hypothesis. A machine is a limited portrayal of a formal language that might be a boundless set. Automata are frequently characterized by the class of formal dialects they can perceive, ordinarily shown by the Chomsky progressive system, which depicts the relations between different dialects and sorts of formalized rationales.

Automata assume a noteworthy job in principle of calculation, compiler development, computerized reasoning, parsing and formal confirmation.

The component of machine include is:

Data sources: Having a limited arrangement of info key pointer 'M' it is expected that succession of images is chosen. The set 'M' speaks to {a1, a2, a3… .. ai} where 'k' is the 'quantity of-inputs'.

Out-puts: Moreover input it likewise has a limited set 'N' which speaks to values {b1, b2, and b3… … .bj} where 'm' speaks to 'words-of – yields'.

Components of automata:

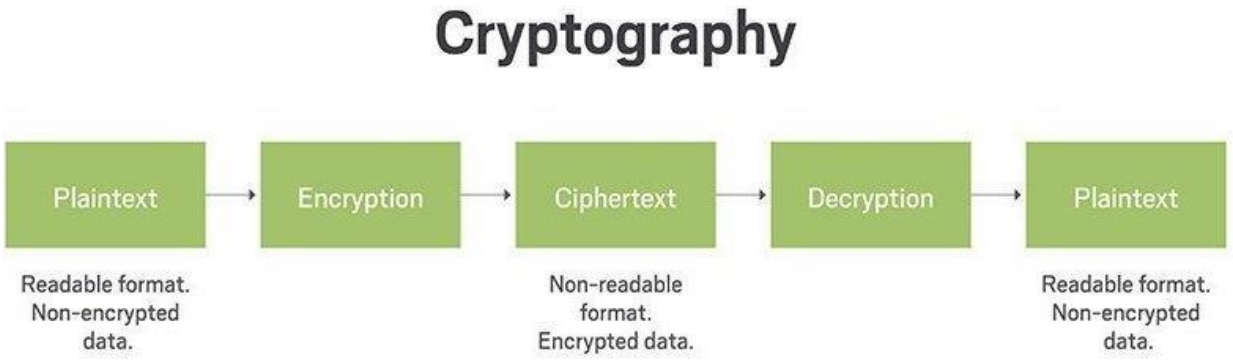
- PDA (Push-Down- Automata)
- A Finite-State-Machine
- Turing machine
- Linear-Bounded –Automata

Cryptography

Web Communication: Cryptography and Network Security. Cryptography, which interprets as "mystery composing," alludes to the study of disguising the importance of information so just determined gatherings comprehend a transmission's contents.

Cryptography is a technique for securing data and correspondences using codes so those for whom the data is expected can peruse and process it.

Cryptography is immovably related to the controls of cryptology and cryptanalysis. It fuses methods, for instance, microdots, mixing words with pictures, and various ways to deal with disguise information away or travel. In any case, in the present PC driven world, cryptography is as often as possible associated with scrambling plaintext (basic substance, a portion of the time insinuated as clear text) into cipher text (a technique called encryption), by then back again (known as decoding). Individuals who practice this field are known as cryptographers.



The Caesar cipher is a standout amongst the most reliable known and least difficult cipher. It is a sort of substitution cipher in which each letter in the plaintext is 'moved' a particular number of spots down the letter set. For example, with a move of 1, A future replaced by B, B would advance toward getting to be C, and so forth. The technique is named after Julius Caesar, who obviously used it to talk with his officers.

Logically complex encryption plans, for instance, the Vigenère figures use the Caesar cipher as one part of the encryption methodology. The for the most part known ROT13 'encryption' is basically a Caesar cipher with a parity of 13. The Caesar cipher offers essentially no correspondence security, and it will be exhibited that it will in general be viably approached the underlying venture by hand.

Example

To pass a scrambled message starting with one individual then onto the next, it is first important that the two gatherings have the 'key' for the cipher, so the sender may encode it and the collector may unscramble it. For the Caesar cipher, the key is the quantity of characters to move the figure letter set.

Here is a brisk case of the encryption and decoding steps required with the Caesar cipher. The content we will encode is 'safeguard the east mass of the mansion', with a move (key) of 1.

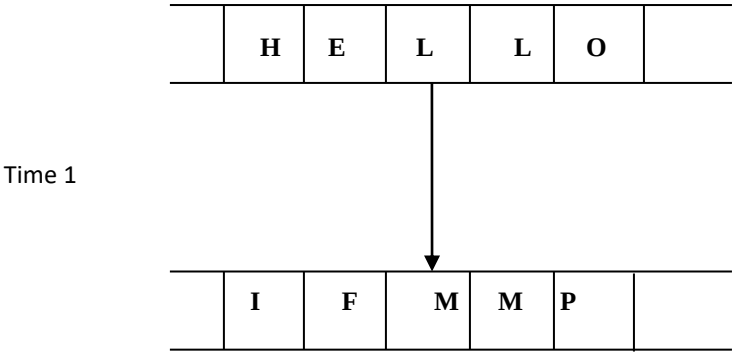
Methodology

As we know that about TM:

- Controller
- Read/Write Head
- Tape

User provide to create a password as a example “HELLO”

Time 0



With the help of Caesar cipher encryption method in the Turing machine Read and Write Operation which convert the value of encryption at the shifting of 1 in the word.

Read H

Write I

Moves right

Read O

Write P

Halt

Decrypt the data with the help of Caesar cipher and create cipher text of found data.

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: bcdefghijklmnopqrstuvwxyza

Clearly, if an alternate key is utilized, the figure letter set will be moved an alternate sum.

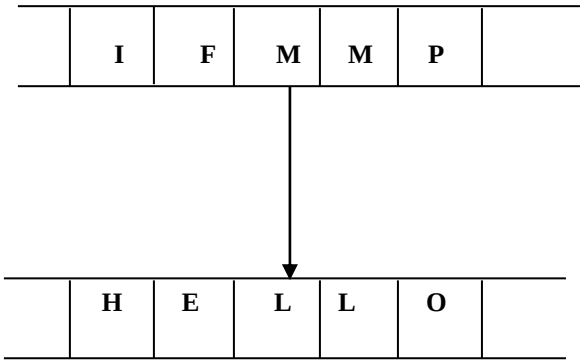
First we interpret the majority of our characters to numbers, 'a'=0, 'b'=1, 'c'=2, ... , 'z'=25. We would now be able to speak to the caesar cipher encryption work, e(x), where x is the character we are scrambling, as:

$$e(x) = (x + k) \pmod{26}$$

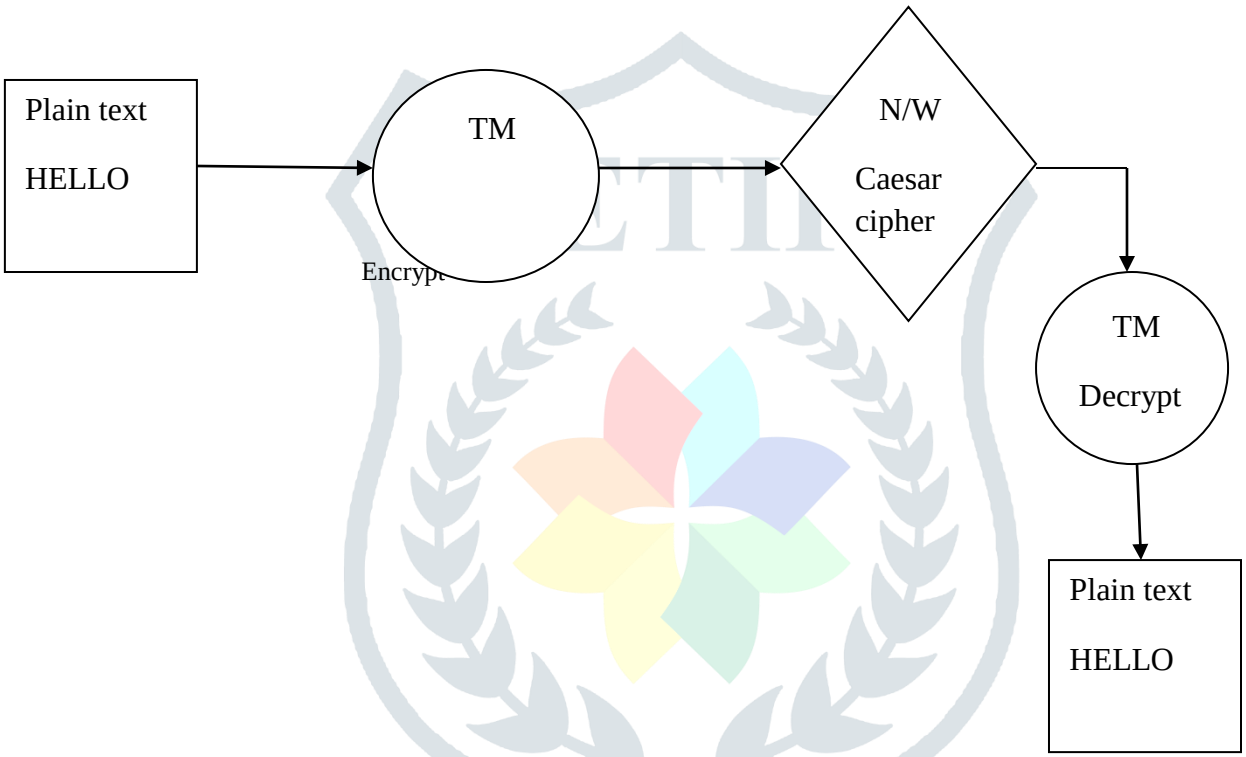
Movement of key k is connected to each letter. In the wake of applying this capacity the outcome is a number which should then be made an interpretation of over into a letter. The decoding capacity is:

$$e(x) = (x - k) \pmod{26}$$

Which convert the value in the given form with the help of Turing machine and decrypt of the data.



Find the input password as output given by the user is “HELLO”.



CONCLUSION

The encryption and decoding plan planned by utilizing PC hypothesis machine is significantly simpler to structure and furthermore the amazing encryption can be produced by utilizing these devices which are hard to unscramble yet exceptionally simple to encode by utilizing a specific plan which is utilized in a few different ways, as we have appeared few here however its utilization is perpetual in light of the fact that now a days the correspondence media is propelling the delicate data is exchanged all the time and these sort of encryption can enable us to verify our information since security is significant in the correspondence between two gatherings in light of the fact that the touchy data can't be undermined at any expense.

REFERENCES

[1] *Theory of Computer Science (Automata, Languages and Computation) By K.L.P Mishra And N. Chandrasekaran 3rd Edition Published In 2009*
[2] The Church-Turing Thesis: *Breaking the Myth*

[3] Vishwa gupta, “Advance cryptography algorithm for improving data security,” Volume 2, Issue 1, January 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[4] Taizo Anan, “*Paper encryption technology*,” unpublished.