Text Cryptography

# Background:

* In this increasingly sophisticated era almost all the good circles of government, industry, business to personal companies do the work using computers.
* The capabilities possessed by computer devices is no doubt, this is proved by the level of accuracy to a high speed in completing a job.
* Besides the bias advantage obtained from the use of computers, the most important thing to be considered is part of its security which if the information/data stored in the computer suffered damage or loss then it could lead to huge losses.
* The reality of modern technology has changed the landscape of digital multimedia and created unexpected problems related to the security of sending and sharing data in the cyber world. The number of theft cases in the cyber world makes the security of data a matter that needs special attention.Cryptography is a popular way to secure data.
* Cryptography is a crucial instrument to protect information that is communicated using computers. Cryptography is an artistic transformation of data into an unreadable format so that only the intended recipient can understand and use it. Cryptography is the art and science of hiding important and secret information from being infringed upon by unauthorized persons.

# Motivation:

* There are several areas which hold sensitive information and must be secured from third party intruders.

For instance:

* 1. Finance: All kinds of transactions for example the PIN of an ATM card.
  2. Commerce: Sensitive negotiations, Electronic commerce.
  3. Military: Battle plan, Weapon control.
  4. Diplomacy: Sensitive negotiations.
* In each of these cases, there are concerns regarding cyber security and other cases caused by the weakness of the security system.
* The condition of a computer that is not secured properly, will be a great opportunity for the hackers to enter the computer access and steal all the data they want.
* To ensure security, we need a computer security system.
* Security of data in a computer is very important to protect the data from other parties that do not have the authority to determine the content of the data.
* Security concerns relate to risk in areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security.
* There are several techniques for data security one of which is a disguise or cryptographic techniques.
* Cryptography is the art and science to protect the data by transforming it into a specific code and is intended only for people who have the key to change the code back to normal.

# Literature Review:

Few journals which we considered for the review:

1. *Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 13-21 (2017).*
2. *International journal of Intelligent Engineering and Systems, December 11,2020.*
3. *International Journal of Computer Science and Information Technologies, Vol. 7 (4) , 2016.*

* The National Institute of Standards and Technology (NIST) Computer Security Handbook [NIST95] defines the term computer security as follows: **The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources** (includes hardware, software, firmware, information/data, and telecommunications).
* Cryptography is one of the areas of science that studies about the information security / data to avoid adverse effects due to misuse of information by irresponsible parties.
* **Cryptography** is the study that is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.

Cryptography has two important processes.

* 1. Encryption
  2. Decryption
* **Vigenère cipher** is one of the cryptographic algorithms that applies the substitution method.
* Vigenère cipher uses tabula recta tables for the encryption and decryption process. The tabula recta is a square table of alphabets, each row of which is made by shifting the previous one to the left.
* These formulae based on Vigenere cipher algorithm will be used in our project.

**Necessity**

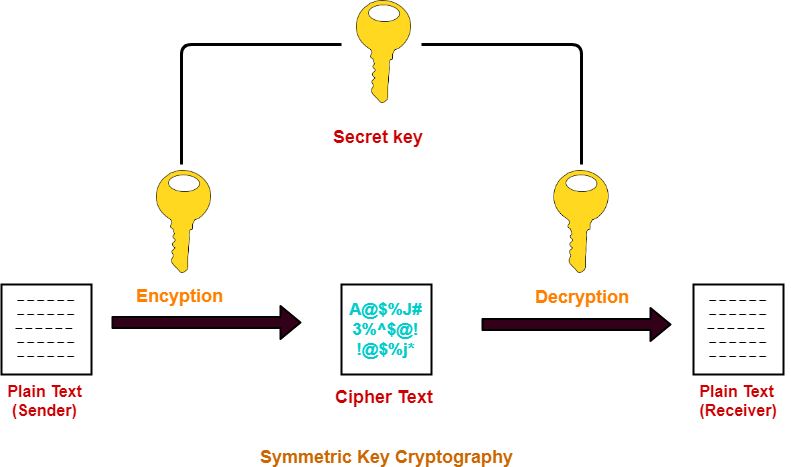
* Today most of us communicate or send data in cyberspace at our own risk. We transmit private information and secrets when we use the Internet for various purposes. Whether we like it or not, the information out there in cyberspace may be hacked by cyber criminals. Information security should be a top concern of all computer users around the world. There is a need for modern cryptography to provide protection and digital keys to ensure that information that is transmitted in cyberspace remains intact and secure.
* Hence, generally speaking, cryptography is all about protecting and safeguarding information from cyber criminals or anyone else other than the intended recipient. Cryptography enables people to communicate on the Internet, transferring crucial and confidential information securely. Therefore, cryptography permits users to use public or private media such as the internet to do online shopping and evade being victims of criminals and password sniffers. This is accomplished by using the latest technological advancements in computer science.
* Cryptography is the science of hiding information in plain sight, in order to conceal it from unauthorized access. It is a technique of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.
* Cryptography makes secure web sites and electronic safe transmissions possible. For a web site to be secure all of the data transmitted between the computers where the data is kept and where it is received must be encrypted. Due to the large number of commercial transactions on the internet, cryptography is very key in ensuring the security of the transactions.
* Cryptography allows you to have confidence in your electronic transactions. Encryption is used in electronic transactions to protect data such as account numbers and transaction amounts, digital signatures replace handwritten signatures or credit card authorizations, and public-key encryption provides confidentiality. Key management is an important aspect in encryption that allows you to apply common encryption policies across all data on all managed devices.
* Cryptography is also used in access control to regulate access such as in satellite and cable TV. Without cryptography, hackers could get into our e-mail, listen in on our phone conversations, tap into cable companies ,acquire free cable service, or break into our bank/brokerage accounts. Time stamping is a cryptographic technique that can certify that a certain electronic document, communication existed or was delivered at a particular time.
* In this digital age, the challenge is to outsmart cyber criminals so that both the sender and intended recipient can enjoy peace of mind. Techniques of encryption and decryption are improved to ensure the highest possible level of security to bona fide internet users. We need to convert our information into unreadable forms so that our data can be protected and will reach its destination safely.By providing codes and digital keys to ensure that what is received is genuine and from the intended sender, the receiver is assured that the data received has not been tampered with during transmission.  
  In general, cryptography is an important way of achieving data confidentiality, data integrity, user authentication and non-repudiation

# Research (Outcome of literature):

## Cryptography:

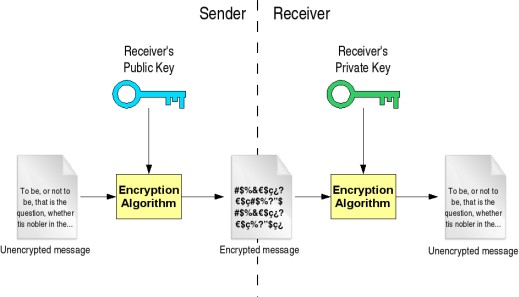
* + Cryptography is a science that is used to maintain the confidentiality of the data, by using certain methods so that data can only be read by a person who is entitled to such data.
* Cryptography, also known as cryptology, thus helps users and institutions to cipher and decipher hidden messages into codes, ciphers and numbers so information can be transmitted safely. Cryptography is initiated by encryption and decryption keys.
* The **encryption** process is carried out on the sender's side. It is involved in converting the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
* The second process, namely **decryption**, is carried out on the receiving side. The process is carried out so that it can restore to the original data form. Here the cipher text is converted back into plaintext using the key
* As discussed earlier, the sole purpose of cryptography is to protect information, email, credit card details and other personal data transmitted across a public network.
* In cryptography, **plaintext** is a simple readable text before being encrypted into ciphertext. The data which can be read and understood without any special measure is called plaintext.
* The transformation of an original message into non-readable message before the transmission is known as **cipher text**. It is a message obtained by some kind of encryption operation on plain text.
  + In the maintenance of the confidentiality of data, cryptography alters original data (plaintext) into data that is encrypted (ciphertext). This process is called the encryption process.
  + Cryptography can be classified into two categories, namely:

1. Shared Key Cryptography
2. Public Key Cryptography
   * **Shared key cryptography** uses one key to encrypt and decrypt messages. This type of cryptography utilizes only one covert digital key. The same digital key is used for encryption and decryption. When the sender of the original data sends the information, he uses the same key to encrypt the information into the unreadable format and the recipient also uses the same key to decrypt the data into a readable format. This is a simple type of cryptography with one serious problem.
   * As the sender and the recipient of a message must both have the same key, they must keep secret from everybody else. The distribution of a single key may open the door to abuse.



**Public key cryptography –**

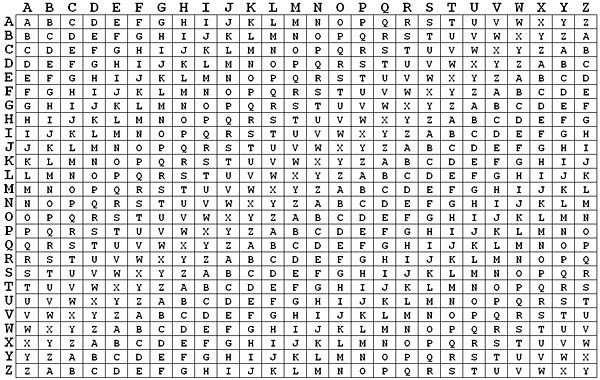
* + Unlike the secret digital key cryptography concept, the public digital key utilizes a pair of complementary keys (a public key and a private key) to encrypt and decrypt messages. The two keys are mathematically related such that a message encoded with one key can only be decoded with the other key.
  + The two-key system enables the parties to communicate more securely. In this type of cryptography, each communicating party has a pair of keys. One key is secret while another is considered public. The public key is shared among them. When sending information, the sender will use the public key to encrypt the information. Once the recipient gets the encrypted information, he uses his secret key to decrypt the information into a readable format.



PART 2

## Vigenere Cipher Algorithm:

* + The Vigenère cipher is a substitution method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution in which each alphabet can be replaced with several cipher alphabets.
  + In the substitution method, the key will have an important role in the strength of the encoding, the better the key the stronger the results of encryption.
  + This algorithm uses shared key type of cryptography.
  + The Vigenère cipher uses a 26×26 table with **A** to **Z** as the row heading and column heading.
  + The first row of this table has 26 English letters. Starting with the second row, each row has the letters shifted to the left by one position in a cyclic way.



* + To encrypt, pick a letter in the plaintext and its corresponding letter in the keyword, use the keyword letter and the plaintext letter as the row index and column index, respectively. The entry at the row-column intersection is the letter in the ciphertext.

For example, in the plaintext if the first letter is **M** and its corresponding keyword letter is **H**. This means that the row of **H** and the column of **M** are used, and the entry **T** at the intersection is the encrypted result.

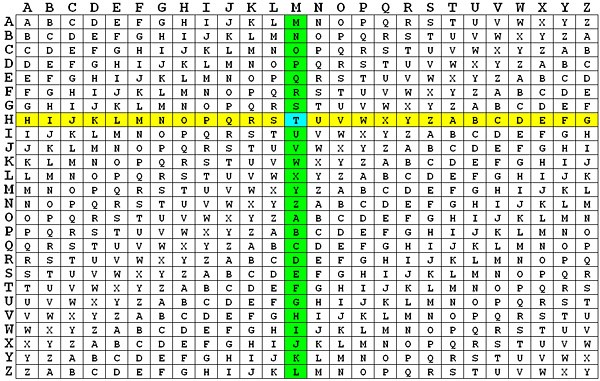
* + If the plaintext is longer than the keyword, repeat the letters of the keyword in the same order till it’s length becomes equal to the length of the plain text.
  + Example:

Plain text: MOUNTAIN Keyword: HAT

* + This can be written as

MOUNTAIN (8 letters)

HATHATHA (8 letters)



* + To decrypt, pick a letter in the ciphertext and its corresponding letter in the keyword.
  + Use the keyword letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plaintext letter.
  + For example, to decrypt the first letter **T** in the ciphertext, we find the corresponding letter in the keyword.The corresponding letter is **H**.

Then, the row of **H** is used to find the corresponding letter **T** and the column that contains **T** provides the plaintext letter **M**.

* + Encryption and decryption process using vigenere cipher algorithm can be represented mathematically:

Encryption : Ci = (Pi + Ki) mod 26 Decryption : Pi¬ = (Ci + Ki) mod 26

Where C0....Cn is ciphertext,

P0....Pn is plaintext and

K0...Kn is key.

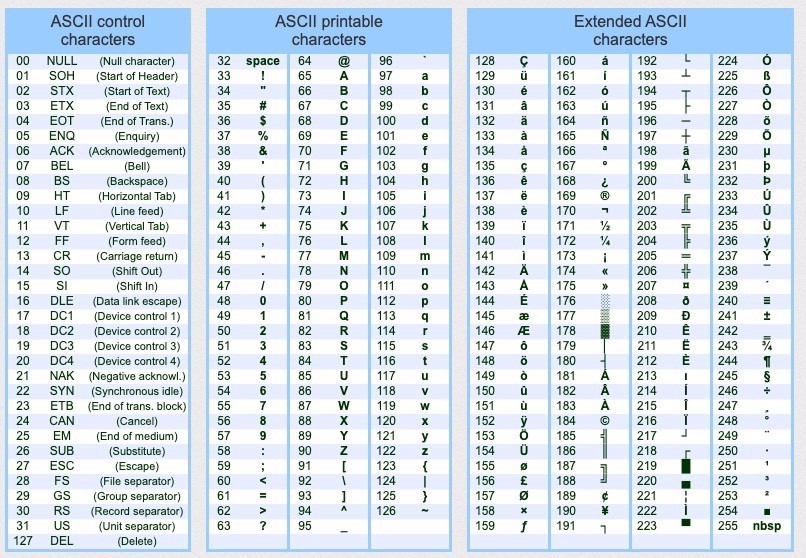
* + If a Vigenere cipher is applied in a computer application, it uses the ASCII table which has 256 characters.
  + Hence, it can mathematically be represented as:

Encryption : Ci = (Pi + Ki) mod 256 Decryption : Pi = (Ci + Ki) mod 256

* Where:

𝐶i= cipher text

𝑃i = plain text

Ki = key, ranging from 0 to 255Hence, 256 has been selected as a constant modulo.

## Working process:

* + Consider the plain text: **NEVER**
  + Consider the keyword: **0)’\*0** (the keyword is generated using a random generator).

## Encryption process:

* + Write the corresponding ASCII values of the plain text: N ---> 78

E ---> 69

V ---> 86

E ---> 69

R ---> 82

Write the corresponding ASCII values of the keyword:

0 ---> 48

) ---> 41

‘ ---> 39

\* ---> 42

0 ---> 48

* + Apply the formula of encryption on to the plaintext and the keyword:

C0=(78+48) mod 256 = 126 character ~

C1=(69+41) mod 256 = 110 character n C2=(86+39) mod 256 = 125 character } C3=(69+42) mod 256 = 111 character o C4=(82+48) mod 256 = 130 character é

Hence, the encrypted text is **~n}oé**.

## Decryption process:

* + Write the corresponding ASCII values of the encrypted text:

~ ---> 126

n ---> 110

} ---> 125

o ---> 111

é ---> 130

* + Write the corresponding ASCII values of the keyword: 0 ---> 48

) ---> 41

‘ ---> 39

\* ---> 42

0 ---> 48

* + Apply the formula of decryption on to the encrypted text and the keyword:

P0=(126-48) mod 256 = 78 character N

P1=(110-41) mod 256 = 69 character E

P2=(125-39) mod 256 = 86 character V

P3=(111-42) mod 256 = 69 character E

P4=(130-48) mod 256 = 82 character R

Now, we get the required plain text: **NEVER**.

# Research Gap:

* Vigenere Cipher is regarded as the simplest and the most weakest method. Meaning, it is very easy to be detected by the intruder.
* In Vigenere Cipher, the length of the key is small compared to the length of the plain text. This forces the key to be repeated to equate its length with the plaintext. Hence, it is more likely to repeat the same cipher text for the length of the plain text.
* The computational complexity of this cipher is much lesser than most modern ciphers, making it fit for lightweight applications where resources are limited.
* In Vigenere Cipher Algorithm, there is no limit on the duration of the key utilization.

These limitations can be overcomed by using a multi-level encryption scheme which uses five keys for encrypting each character and it makes cryptanalysis impossible without detecting all the five keys.

# Problem Statement:

The underlying respective architecture of most IT systems, including the desktop computer and internet, does not guarantee security. Users with malicious intents have always found a way of exploiting one vulnerability or the other. An attack that affects the confidentiality of information often presents the platform for the integrity of such information to be compromised. Intercepted information on transit would make little or no sense to an interceptor if he is not able to decipher the content of the information.

This explains why it is very necessary to ensure that even when an intruder or unauthorised user successfully obtains access to some information the confidentiality and integrity of the information remain uncompromised.