**SOPEJU OLUWABUSUYI FEYIKEMI**

**15/ENG02/046**

**MAY 2020.**

AUTOKEY CIPHER

The Autokey Cipher is a polyalphabetic substitution cipher. It is closely related to the Vigenere cipher but uses a different method of generating the key. It was invented by Blaise de Vigenere in 1586 and is in general more secure than the Vigenere cipher.

An autokey cipher is a cipher that incorporates the message (plaintext) into the key. The key is generated from the message in some automated fashion, sometimes by selecting certain letters from the text or, more commonly, by adding a short primer key to the front of the message.

Similar to other polyalphabetic substitution ciphers, the autokey cipher algorithm is about changing plaintext letters based on secret key letters. Each letter of the message is shifted along some alphabet positions. The number of positions is equal to the place in the alphabet of the current key letter.

To simplify calculations, one can use a table which contains in subsequent row alphabets with letters shifted along increasingly larger number of positions. The table is called tabula recta. Tabula recta is a square with 26 copies of the alphabet, the first line starting with 'A', the next line starting with 'B', etc. In order to encrypt a plaintext, one locates the row with the first letter to be encrypted, and the column with the first letter of the key. The letter where the line and column cross is the ciphertext letter.

There are two forms of autokey cipher: key-autokey and text-autokey ciphers.

A key-autokey cipher uses previous members of the keystream to determine the next element in the keystream.

A text-autokey uses the previous message text to determine the next element in the keystream.

To break the cipher, the intruder should try to guess some parts of plaintext (for example, trying some common sequences of letters). Comparing them to plaintext allows to receive some characters of the secret key. One should try to find such letters which result in disclosure of correct words among the secret key characters.

Unlike in other similar ciphers, after using all secret key letters, the algorithm doesn't go back to its first letter but starts to take plaintext letters as new key letters.

Due to avoid repetition of the same secret key letters, the cipher is resistant to attacks based on dividing ciphertext into parts corresponding to subsequent secret key characters.

Modern autokey ciphers use very different encryption methods, but they follow the same approach of using either key bytes or plaintext bytes to generate more key bytes. Most modern stream ciphers are based on pseudorandom number generators: the key is used to initialize the generator, and either key bytes or plaintext bytes are fed back into the generator to produce more bytes.

Some stream ciphers are said to be "self-synchronizing", because the next key byte usually depends only on the previous N bytes of the message. If a byte in the message is lost or corrupted, therefore, the key-stream will also be corrupted.

COMPUTER CRIME

Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Computer crime describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like hacking, are uniquely related to computers.

Examples of Computer Crimes

* Improperly accessing a computer, system, or network
* Modifying, damaging, using, disclosing, copying, or taking programs or data
* Introducing a virus or other contaminant into a computer system
* Using a computer in a scheme to defraud
* Interfering with someone else's computer access or use
* Using encryption in aid of a crime
* Falsifying email source information
* Stealing an information service from a provider.

Losing a computer or a web account due to cybercrime can be very damaging, especially as we continue to rely more and more on these networks to conduct business. There are, however, certain things you can do to help protect yourself.

Much of cybercrime is fraud involving the use of a computer. Learn the warning signs of fraudulent behavior and wire fraud. Be extremely careful when giving out sensitive personal information such as social security numbers and bank account access codes over the Internet.

Otherwise, take basic precautions for keeping your data private. Use passwords that are difficult to hack and change them frequently. Don't conduct financial transactions on public computers or over unprotected networks. You should also install a good anti-virus program on your computer and keep it updated. Finally, be careful about downloading software from disreputable websites as it can contain spyware, viruses, or other malware.