EJALONIBU OLUWABUSAYO MARY

15/ENG02/019

ASSIGNMENT

A NOTE ON AUTO KEY CIPHER AND COMPUTER CRIMES

AUTO KEY CIPHERS

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 Vigenère in 1586, and is in general more secure than the Vigenere cipher.

An autokey cipher (also known as the autoclave cipher) is a cipher that incorporates the message (the 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.

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.

In modern cryptography, self-synchronizing stream ciphers are autokey ciphers.

METHOD

The autokey cipher, as used by members of the American Cryptogram Association, starts with a relatively-short keyword, the primer, and appends the message to it. If, for example, the keyword is "QUEENLY" and the message is "ATTACK AT DAWN", the key would be "QUEENLYATTACKATDAWN".

A tabula recta is used for auto key cipher as shown below;



Plaintext: ATTACK AT DAWN...

Key: QUEENL YA TTACK AT DAWN....

Ciphertext: QNXEPV YT WTWP...

The ciphertext message would thus be "QNXEPVYTWTWP".

To decrypt the message, the recipient would start by writing down the agreed-on key again.

QUEENLY

The first letter of the key, Q, would then be taken, and that row would be found in a tabula recta. That column for the first letter of the ciphertext would be looked across, also Q in this case, and the letter to the top would be retrieved, A. Now, that letter would be added to the end of the key:

QUEENLYA

Then, since the next letter in the key is U and the next letter in the ciphertext is N, the U row is looked across to find the N to retrieve T:

QUEENLYAT

That continues until the entire key is reconstructed, when the primer can be removed from the start.

**COMPUTER CRIMES**

'Computer crime' could reasonably include a wide variety of criminal offences and unlawful activities related to or having connection to computers.

Computer crimes can be classified essentially under two headings;

where computer is either (a) a tool, or (b) a target, to perform an unlawful act.

The computer is a tool for an unlawful act where the offence reflects a modification of a conventional crime by making use of information technology and modern communication tools. There are certain crimes where the computer itself is the target, that is, to say such crimes which have evolved due to the advancement in information technology itself. Of course, there might be instances where the computer is a tool as well as the target of a crime.

**Kinds of computer crimes/offences**

A few common computer crimes have been stated below;

(A) Conventional crimes through computer: cyber defamation, digital forgery, cyber pornography, cyber stalking/harassment, Internet fraud, financial crimes, online gambling, and sale of illegal articles.

(B) Crimes committed on a computer network: hacking/unauthorized access, denial of service.

(C) Crimes relating to data alteration/destruction: virus/worms/Trojan horses/logic bomb, theft of Internet hours, data diddling, salami attacks, steganography

(D) Crimes relating to electronic mail: spamming/bombing, spoofing

**How to protect yourself against cybercrime**

* Use a full-service internet security suite
* Use strong passwords
* Keep your software updated
* Strengthen your home network
* Take measures to help protect yourself against identity theft
* Keep up to date on major security breaches