ENWELU EBUBE CHARLES

15/ENG02/022

COMPUTER ENGINEERING

COE 522 CRYPTOGRAPHY PRINCIPLES AND APPLICATION

 ASSIGNMENT 3

**QUESTION ONE**

**Explain the Autokey cipher**

**SOLUTION**

 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.

There are two forms of autokey cipher: *key-autokey* and *text-autokey* ciphers. A key-autokey cipher uses previous members of the [keystream](https://en.wikipedia.org/wiki/Keystream%22%20%5Co%20%22Keystream) 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-synchronising [stream ciphers](https://en.wikipedia.org/wiki/Stream_cipher) are autokey ciphers.

This cipher was invented in 1586 by [Blaise de Vigenère](https://en.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re%22%20%5Co%20%22Blaise%20de%20Vigen%C3%A8re) with a reciprocal table of ten alphabets. Vigenère's version used an agreed-upon letter of the alphabet as a primer, making the key by writing down that letter and then the rest of the message.

More popular autokeys use a [tabula recta](https://en.wikipedia.org/wiki/Tabula_recta), a square with 26 copies of the alphabet, the first line starting with 'A', the next line starting with 'B' etc. Instead of a single letter, a short agreed-on keyword is used, and the key is generated by writing down the primer and then the rest of the message, as in Vigenère's version. To encrypt a plaintext, the row with the first letter of the message and the column with the first letter of the key are located. The letter in which the row and the column cross is the ciphertext letter.

**Encryption**
Encryption using the Autokey Cipher is very similar to the Vigenère Cipher, except in the creation of the keystream.

The keystream is made by starting with the keyword or keyphrase, and then appending to the end of this the plaintext itself.

We then use a Tabula Recta to find the keystream letter across the top, and the plaintext letter down the left, and use the crossover letter as the ciphertext letter.

**Decryption**
To decrypt a ciphertext using the Autokey Cipher, we start just as we did for the Vigenère Cipher, and find the first letter of the key across the top, find the ciphertext letter down that column, and take the plaintext letter at the far left of this row. As well as being the plaintext letter, we now need to add this letter to the end of the keystream as we shall need it later. Continuing to decode each letter, we add them to the end of the keystream each time.

**QUESTION TWO**

**Discuss computer crimes**

**SOLUTION**

Cybercrime, also called computer crime, the use of a [computer](https://www.britannica.com/technology/computer) as an instrument to further illegal ends, such as committing [fraud](https://www.britannica.com/topic/fraud), trafficking in child pornography and [intellectual](https://www.merriam-webster.com/dictionary/intellectual) property, [stealing identities](https://www.britannica.com/topic/identity-theft), or violating privacy. Cybercrime, especially through the [Internet](https://www.britannica.com/technology/Internet), has grown in importance as the computer has become central to commerce, entertainment, and government.

**Examples of Computer Crimes**

Computer crime laws in [many states](https://statelaws.findlaw.com/criminal-laws/computer-crimes.html) prohibit a person from performing certain acts without authorization, including:

* 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](https://criminal.findlaw.com/criminal-charges/fraud.html);

Interfering with someone else's computer access or use;

* Using encryption in aid of a crime;
* Falsifying email source information; and
* Stealing an information service from a provider.