# **OJO OLAOLUWA JOEL**

# **COMPUTER ENGINEERING**

# **15/ENG02/041**

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

## The Algorithm

The 'key' for the Autokey cipher is a key word. e.g. 'FORTIFICATION'

The Autokey cipher uses the following tableau (the 'tabula recta') to encipher the plaintext:

 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

 ---------------------------------------------------

A A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

B B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

C C D E F G H I J K L M N O P Q R S T U V W X Y Z A B

D D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

E E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

F F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

G G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G

I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H

J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J

L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K

M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L

N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

O O P Q R S T U V W X Y Z A B C D E F G H I J K L M N

P P Q R S T U V W X Y Z A B C D E F G H I J K L M N O

Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P

R R S T U V W X Y Z A B C D E F G H I J K L M N O P Q

S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R

T T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

U U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

V V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

W W X Y Z A B C D E F G H I J K L M N O P Q R S T U V

X X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

Y Y Z A B C D E F G H I J K L M N O P Q R S T U V W X

Z Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

To encipher a message, place the keyword above the plaintext. Once all of the key characters have been written, start writing the plaintext as the key:

FORTIFICATIONDEFENDTHEEASTWA

DEFENDTHEEASTWALLOFTHECASTLE

Now we take the letter we will be encoding, 'D', and find it on the first column on the tableau. Then, we move along the 'D' row of the tableau until we come to the column with the 'F' at the top (The 'F' is the keyword letter for the first 'D'), the intersection is our ciphertext character, 'I'.

So, the ciphertext for the above plaintext is:

FORTIFICATIONDEFENDTHEEASTWA

DEFENDTHEEASTWALLOFTHECASTLE

ISWXVIBJEXIGGZEQPBIMOIGAKMHE

2. Computer Crimes

Alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech 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.

Examples of computer crimes

Below is a listing of the different types of computer crimes today.

* **Child pornography** - Making or distributing child pornography.
* **Copyright violation** - Stealing or using another person's [Copyrighted](https://www.computerhope.com/jargon/c/copyrigh.htm) material without permission.
* [**Cracking**](https://www.computerhope.com/jargon/c/cracker.htm) - Breaking or deciphering codes designed to protect data.
* **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
* [**Cyberbully or Cyberstalking**](https://www.computerhope.com/jargon/c/cyberbul.htm) - Harassing or stalking others online.
* [**Cybersquatting**](https://www.computerhope.com/jargon/c/cybersqu.htm) - Setting up a [domain](https://www.computerhope.com/jargon/d/domain.htm) of another person or company with the sole intention of selling it to them later at a premium price.
* [**Creating Malware**](https://www.computerhope.com/jargon/m/malware.htm) - Writing, creating, or distributing malware (e.g., [viruses](https://www.computerhope.com/jargon/v/virus.htm) and [spyware](https://www.computerhope.com/jargon/s/spyware.htm).)
* [**Denial of Service attack**](https://www.computerhope.com/jargon/d/dos.htm) - Overloading a system with so many requests it cannot serve normal requests.
* [**Doxing**](https://www.computerhope.com/jargon/d/doxing.htm) - Releasing another person's personal information without their permission.
* **Espionage** - Spying on a person or business.
* [**Fraud**](https://www.computerhope.com/jargon/c/computer-fraud.htm) - Manipulating data, e.g., changing banking records to transfer money to an account or participating in [credit card fraud](https://www.computerhope.com/jargon/c/creditca.htm).
* [**Harvesting**](https://www.computerhope.com/jargon/h/harvest.htm) - Collect account or account-related information on other people.
* **Human trafficking** - Participating in the illegal act of buying or selling other humans.
* [**Identity theft**](https://www.computerhope.com/jargon/i/identhef.htm) - Pretending to be someone you are not.