**SAMUEL IBITOGBE**

**15/eng02/029**

**Auto key Cipher**

**Introduction** §

The Auto Key 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** [§](http://practicalcryptography.com/ciphers/autokey-cipher/#the-algorithm)

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

The Auto key 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 cipher text character, 'I'.

So, the cipher text for the above plaintext is:k

FORTIFICATIONDEFENDTHEEASTWA

DEFENDTHEEASTWALLOFTHECASTLE

ISWXVIBJEXIGGZEQPBIMOIGAKMHE

# Computer crime

Alternatively referred to as **cybercrime**, **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. Clicking on any of the links below gives further information about each crime.

* **Child pornography** - Making or distributing child pornography.
* **Copyright violation** - Stealing or using another person's Copyrighted material without permission.
* **Cracking** - Breaking or deciphering codes designed to protect data.
* **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
* **Cyberbully or Cyberstalking** - Harassing or stalking others online.
* **Cybersquatting** - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
* **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)
* **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
* **Doxing** - Releasing another person's personal information without their permission.
* **Espionage** - Spying on a person or business.
* **Fraud** - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud
* **Harvesting**- Collect account or account-related information on other people.
* **Human trafficking** - Participating in the illegal act of buying or selling other humans.
* **Identity theft** - Pretending to be someone you are not.
* **Illegal sales** - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
* **Intellectual property theft** - Stealing practical or conceptual information developed by another person or company.
* **IPR violation** - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.
* **Phishing**- Deceiving individuals to gain private or personal information about that person.
* **Salami slicing**- Stealing tiny amounts of money from each transaction.
* **Scam** - Tricking people into believing something that is not true.
* **Slander** - Posting libel or slander against another person or company.
* **Software piracy** - Copying, distributing, or using software that was not purchased by the user of the software.
* **Spamming**- Distributed unsolicited e-mail to dozens or hundreds of different addresses.
* **Spoofing** - Deceiving a system into thinking you're someone you are not.
* **Typo squatting** - Setting up a domain that is a misspelling of another domain.
* **Unauthorized access**- Gaining access to systems you have no permission to access.
* **Wiretapping** - Connecting a device to a phone line to listen to conversations.