AGOYI ISAAC OTUOZE

15/ENG02/002

COE 522 ASSIGNMENT 3

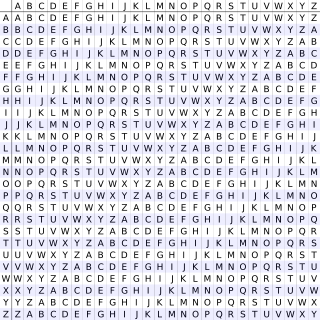
1. **EXPLAIN AUTOKEY CIPHER**

The autokey cipher was presented in 1586 by a French diplomat and alchemist Blaise de Vigenère. The autokey cipher was used in Europe until the 20th century. Currently it is considered to be easy to break. However, the idea to create key letters based on plaintext letters is used in many modern ciphers.

**Algorithm:** similarly 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* and looks like the one below:

 *Fig:Tabula Recta*

Unlike in other similar ciphers, after using all of secret key letters, the algorithm doesn't go back to its first letter but starts to take plaintext letters as new key letters. For example, after encryption two words *Opinio communis* using the secret key *Ab ovo* one receives:

|  |  |
| --- | --- |
| Plaintext: | OPINIOCOMMUNIS |
| Key: | ABOVO**OPINIOCOM** |
| Ciphertext: | OQWIWCRWZUIPWE |

### Security of the autokey cipher

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. However its weakness is that all key characters create words and sentences which in addition are the same as in plaintext.

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.

1. **Discuss 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

* **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](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** - 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](https://www.computerhope.com/jargon/s/software.htm) that was not purchased by the user of the software.
* **Spamming** - Distributed unsolicited [e-mail](https://www.computerhope.com/jargon/e/email.htm) 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.