NAME: JADESOLA KAREEM ‘TANWA

15/ENG02/033

COE 522

CRYPTOGRAPHY PRINCIPLES AND APPLICATIONS.

1. 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. An **autokey cipher** is a [cipher](https://en.wikipedia.org/wiki/Cipher) that incorporates the message (the [plaintext](https://en.wikipedia.org/wiki/Plaintext)) into the [key](https://en.wikipedia.org/wiki/Key_%28cryptography%29). 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*: A key-autokey cipher uses previous members of the [keystream](https://en.wikipedia.org/wiki/Keystream) to determine the next element in the keystream.
* *text-autokey*: A text-autokey uses the previous message text to determine the next element in the keystream.

Methodology

The Autokey cipher uses the 'tabula recta' to encipher a plaintext. 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.

Example: The Autokey cipher key word is 'FORTIFICATION'. Plain text is “defend the east wall of the castle”.

**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:

 Key: FORTIFICATIONDEFENDTHEEASTWA

Plaintext: DEFENDTHEEASTWALLOFTHECASTLE

 ISWXVIBJEXIGGZEQPBIMOIGAKMHE

1. Computer Crimes.

A 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. Computer crime is a crime that involves a computer and a network.

Examples of computer crimes.

* Cracking - Breaking or deciphering codes designed to protect data. A cracker is an individual who can decipher codes and passwords being able to break security systems for illegal reasons. Often this person uses a program or script known as a crack that was written to do what they're hoping to achieve.
* Cyberbully or Cyberstalking - Harassing or stalking others online. A cyberbully is someone who posts inappropriate or unwanted things about another person, or otherwise harasses them in e-mails, IMs, or SMS. A cyberbully may try to ruin another person's reputation by posting false information, or they may post information the other person does not want others to know. Online social media platforms, like Facebook and Twitter, are common places for a cyberbully to harass other people.
* Cybersquatting - Cybersquatting is a term used to describe an individual or company who intentionally purchases a domain and holds it until they can sell it at a premium price. Cybersquatting is sometimes referred to as domain squatting and typo squatting.
* Denial of Service attack - Overloading a system with so many requests it cannot serve normal requests.
* Fraud - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
* 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. 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. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
* 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. Spamming is the use of messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same website.
* Spoofing - Deceiving a system into thinking you're someone you are not.
* Typosquatting - 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.