NAME: BOSAN RIYASAI JOY

MATRIC. ON: 15/ENG02/012

COMPUTER ENGINEERING

COE522 ASSIGNMENT 3

Question one: Explain the Auto key cipher

An autokey cipher is a cipher that incorporates the message (the plaintext) into the key. 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.

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.

There are two forms of autokey cipher: key-autokey and text-autokey ciphers. A key-autokey cipher uses previous members of the keystream to determine the next element in the keystream. A text-autokey uses the previous message text to determine the next element in the keystream.

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
```

Question two: Discuss computer crimes

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. Computer crime describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like hacking, are uniquely related to computers. Alternatively referred to as cyber-crime, e-crime, electronic crime, or hi-tech crime.

Examples of computer crimes

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

- 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;
- 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.
- **Cyberbully or Cyberstalking** - Harassing or stalking others online. Cyberbullying is aggressive harassment that occurs using electronic technology, including cell phones, tablets, and computers

using social media sites and chat-sites. Cyberbullying includes the sending of unwanted, abusive text messages, photographs, personal information, defamatory and libelous allegations and rumors, and the creation of fake profiles intended to harm victims.

- **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.
- **Child pornography** - Making or distributing child pornography. Child pornographers and child molesters have unfortunately found the Internet to be a useful tool to prey on children as well. The Department of Justice (DOJ) has a special task force devoted to catching these predators, and if your child has been targeted, you should contact law enforcement right away. The DOJ has published a Citizen's Guide to U.S. Federal Law on Child Pornography to outline the applicable federal laws. The Department of Justice also provides additional resources on Internet safety for children and the rights of child victims.
- **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.
- **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.
- **Social Network, Cybercrime and Internet Sex Crimes** - While bullying, sexual harassment, and child pornography are long standing crimes and societal problems, the Internet and social network sites have introduced a whole new arena for predators to practice their trade.

Protecting Yourself: Losing a computer or a web account due to cybercrime can be very damaging, especially as we continue to rely more and more on these networks to conduct business. There are, however, certain things you can do to help protect yourself.

First, much of cybercrime is fraud involving the use of a computer. Learn the warning signs of fraudulent behavior and wire fraud. Be extremely careful when giving out sensitive personal information such as social security numbers and bank account access codes over the Internet. Otherwise, take basic precautions for keeping your data private. Use passwords that are difficult to hack and change them frequently. Don't conduct financial transactions on public computers or over unprotected networks. You should also install a good anti-virus program on your computer and keep it updated. Finally, be careful about downloading software from disreputable websites as it can contain spyware, viruses, or other malware.