15/ENG02/028

IBINAIYE SEUN JOHN

COE 522 ASSIGNMENT SOLUTION

NUMBER 1

Autokey Cipher

The term autokey refers to any cipher where the key is based on the original plaintext. In its simplest form, it was first described by Girolamo Cardano, and consisted of using the plaintext itself as the keystream. The Autokey cipher is very similar to the vignere cipher.

Encryption using Autokey cipher

Encryption using the Autokey Cipher is very similar to the Vigenère Cipher, except in the creation of the keystream. The keystream is made by starting with the keyword or key phrase, and then appending to the end of this the plaintext itself. We then use a Tabula Recta to find the keystream letter across the top, and the plaintext letter down the left, and use the crossover letter as the ciphertext letter.

As an example we shall encode the plaintext "meet me at the corner" using the keyword **king**. First we must generate the keystream, which starts with the keyword, and then continues with the plaintext itself, getting kingmeetmeattheco as seen below.

PLAINTEXT - MEETMEATTHECORNER

KEY STREAM –KINGMEETMEATTHECO

KEYWORD – KING

The keystream in the Autokey CIpher starts with the keyword, and is then followed by the plaintext itself.

With the keystream generated, we use the Tabula Recta, just like for the Vigenère Cipher. We find K across the top, and M down the left side. The ciphertext letter is "W".

For the second letter, "e", we go to I across the top, and E down the left to get the ciphertext letter "M".

Continuing in this way we get the cipher text "WMRZYIEMFLEVHYRGF".

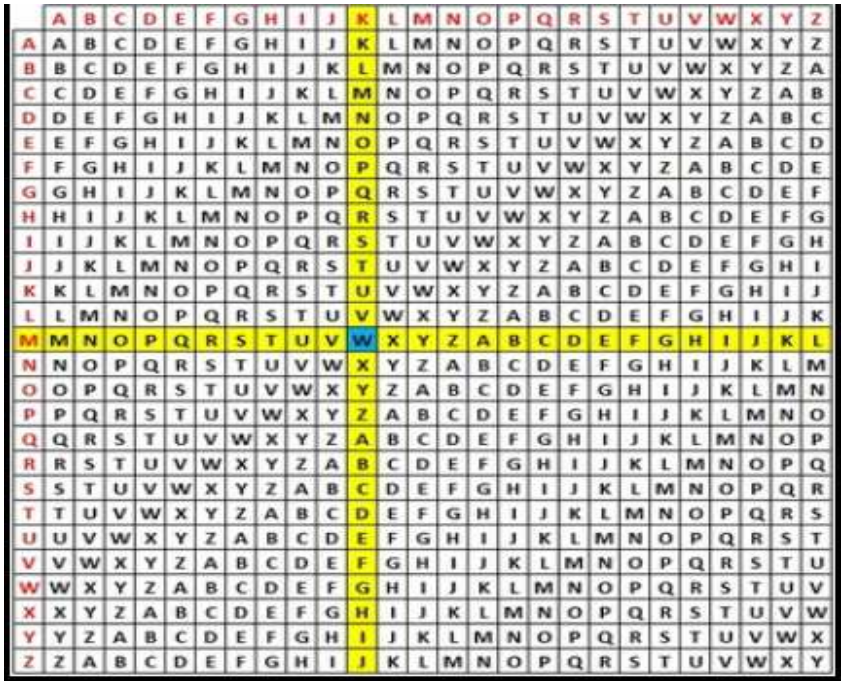

Figure 1: The Tabula Recta

Therefore, the plaintext, key stream and cipher text using the Autokey cipher is shown below

PLAINTEXT - MEETMEATTHECORNER

KEY STREAM- KINGMEETMEATTHECO

Cipher text - WMRZYIEMFLEVHYRG

Decryption of Autokey cipher

To decrypt a ciphertext using the Autokey Cipher, we start just as we did for the Vigenère Cipher, and find the first letter of the key across the top of the tabula reacta as seen in figure 1, find the ciphertext letter down that column, and take the plaintext letter at the far left of this row. As well as being the plaintext letter, we now need to add this letter to the end of the keystream as we shall need it later. Continuing to decode each letter, we add them to the end of the keystream each time.

We shall decrypt the cipher text " WMRZYIEMFLEVHYRG " which has been encrypted using the keyword king as seen from the previous example on encryption.

We start with the data shown below.

KEY STREAM- KING

Cipher text - WMRZYIEMFLEVHYRG

PLAINTEXT-

Solution

First we look along the top row of the tabula recta in figure 1 to find the first letter from the keystream, which is “K”. We look down this column and find the cipher text letter "W".

We then go along this row to the left hand edge, and the letter there is the plaintext letter which we can see as letter “A".

We now add this to the end of the keystream, as well as to the plaintext row.

KEY STREAM- KINGM

Cipher text - WMRZYIEMFLEVHYRG

PLAINTEXT- M

We have added the first letter from the plaintext, and appended this to the end of the keystream as well.

In the same way as the previous step, we find the keystream letter “I”, and find the cipher text letter "M" in this column. We then follow this row to find the plaintext letter "E".

Again we add this plaintext letter to the end of the keystream.

KEY STREAM- KINGME

Cipher text - WMRZYIEMFLEVHYRG

PLAINTEXT- ME

We have added the first letter from the plaintext, and appended this to the end of the keystream as well.

We repeat the same steps and at the end retrieve the plaintext " **MEETMEATTHECORNER** ".

NUMBER 2

Computer crimes

Computer crime is often referred to as cybercrime. Computer crime is an act performed by a knowledgeable computer user (hacker) that illegally browses or steals a company's or individual's private information (sensitive). 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

Briefly we would discuss different types of computer crimes today;

1. **Cracking** - Breaking or deciphering codes designed to protect data.
2. **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
3. **Cyberbully or Cyberstalking** - Harassing or stalking others online.
4. **Cybersquatting** - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
5. **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)
6. **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
7. **Espionage** - Spying on a person or business.
8. **Fraud** - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
9. **Phishing** - Deceiving individuals to gain private or personal information about that person.

10. **Salami slicing** - Stealing tiny amounts of money from each transaction.
11. **Software piracy** - Copying, distributing, or using software that was not purchased by the user of the software.
12. **Spamming** - Distributed unsolicited e-mail to dozens or hundreds of different addresses.
13. **Spoofing** - Deceiving a system into thinking you're someone you are not.
14. **Unauthorized access** - Gaining access to systems you have no permission to access.
15. **Wiretapping** - Connecting a device to a phone line to listen to conversations.