Alamin Mohammed Nabil

15/ENG02/006

Autokey Ciphers

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. This cipher incorporates a keyword in the creation of the keystream as well as the plaintext.

Encryption

The keystream is made by starting with the keyword itself then appending the plaintext to its end. Tabula recta is used to encode by taking the point of the first plaintext and tracing on its row to intersect with the corresponding key stream value.

Below is an example:

Keyword: boy

Plaintext: inthedistance

Keystream: boyintheddist

```
    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
```

Now we take the letter we will be encoding, 'I', and find it on the first column on the tableau.

Then, we move along the 'I' row of the tableau until we come to the column with the 'B' at the top (The 'B' is the keyword letter for the first 'I'), the intersection is our ciphertext character, 'J'.

So the ciphertext for the above plaintext is:

Plaintext: inthedistance

Keystream: boyintheddist

Cyphertext: jbrprwpwwifve

Decryption

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, 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.

Computer Crimes

Cybercrimes are criminal offenses committed via the Internet or otherwise aided by various forms of computer technology, such as the use of online social networks to bully others or sending sexually explicit digital photos with a smart phone. But while cybercrime is a relatively new phenomenon, many of the same offenses that can be committed with a computer or smart phone, including theft or child pornography, were committed in person prior to the computer age. This sub-section includes articles on cyber bullying, sexting, and a whole host of other crimes commonly committed online or with the help of computer networking technology.

Cybercrimes include:

1. Cryptocurrency theft
2. Hacking
3. Phishing
4. Fraud
5. Dark Web Crimes