# Loyalist College

In Class Assignment 1

**WINP2003 - Wireless Communication and Mobile Security 01 (M05 Group 1)**

## Group –G3


Submitted by:

Manish Shrestha (500229247)

Nabin Shrestha (500219496)

Pratap Shrestha (500233537)

Seema Seema (500231780)

Clinton Kenechukwu Ogboji (500233188)

Submitted to:

Nawaz Mohamudally

# PART 1

The following message has been encrypted using the Vigenère cipher:

**GGIATVWGQIR**

Review the cipher keyword.

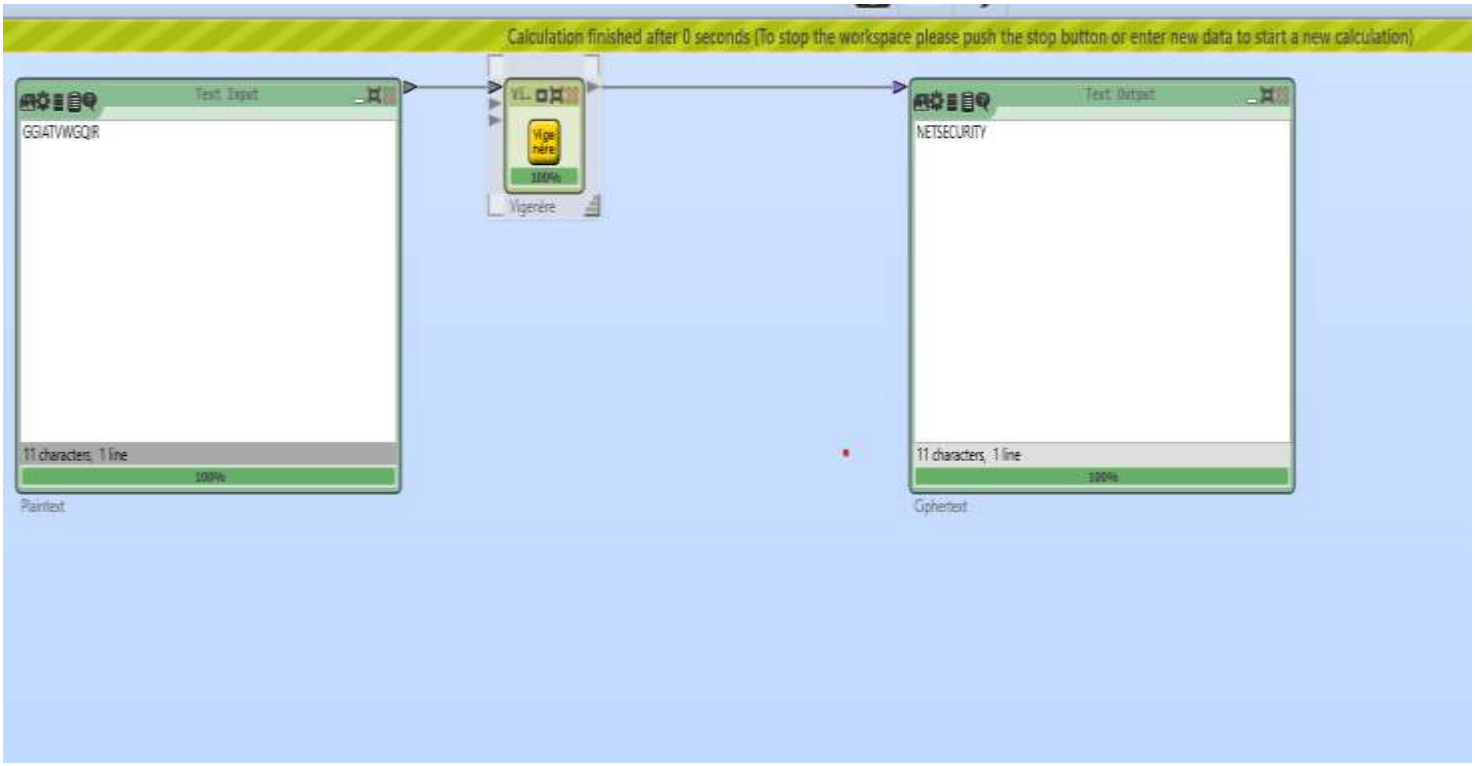
The cipher keyword **TCPIP** was used to encrypt the message. The same keyword will be used to decrypt or decipher the message.

Review the structure of the Vigenère square.

A standard Vigenère square or table is used with the keyword to decipher the message.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher Keyword | T | C | P | I | P | T | C | P | I | P | T |
| Encrypted Message | G | G | I | A | T | V | W | G | Q | I | R |
| Decrypted Message | N | E | T | S | E | C | U | R | I | T | Y |

The following example uses Cryptool to decrypt the encrypted message.




**Using Excel to show the decryption**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher Keyword | T | C | P | I | P | T | C | P | I | P | T |
| Plainteet | G | G | I | A | T | Y | V | G | Q | I | R |
| Encrypted Message | N | E | T | S | E | C | U | R | I | T | Y |
| CO-ORDINATES POINTS | 20,14 | 3,5 | 16,20 | 9,19 | 16,5 | 20,3 | 3,21 | 16,18 | 9,9 | 16,20 | 20,25 |

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 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 |
| 1 | A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | Y | W | X | Y | Z |
| 2 | 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 |
| 3 | 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 |
| 4 | D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | Y | W | X | Y | Z | A | B | C |
| 5 | E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | Y | W | X | Y | Z | A | B | C | D |
| 6 | 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 |
| 7 | 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 |
| 8 | H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | Y | W | X | Y | Z | A | B | C | D | E | F | G |
| 9 | 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 |
| 10 | 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 |
| 11 | K | K | L | M | N | O | P | Q | R | S | T | U | Y | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| 12 | L | L | M | N | O | P | Q | R | S | T | U | Y | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| 13 | 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 |
| 14 | 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 |
| 15 | O | O | P | Q | R | S | T | U | Y | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 16 | P | P | Q | R | S | T | U | Y | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 17 | 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 |
| 18 | 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 |
| 19 | S | S | T | U | Y | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| 20 | 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 |
| 21 | 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 |
| 22 | V | Y | 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 |
| 23 | 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 | Y |
| 24 | 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 |
| 25 | 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 |
| 26 | Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | Y | W | X | Y |

# PART 2

For the part 2 we are taking following key and plain text for the encryption:

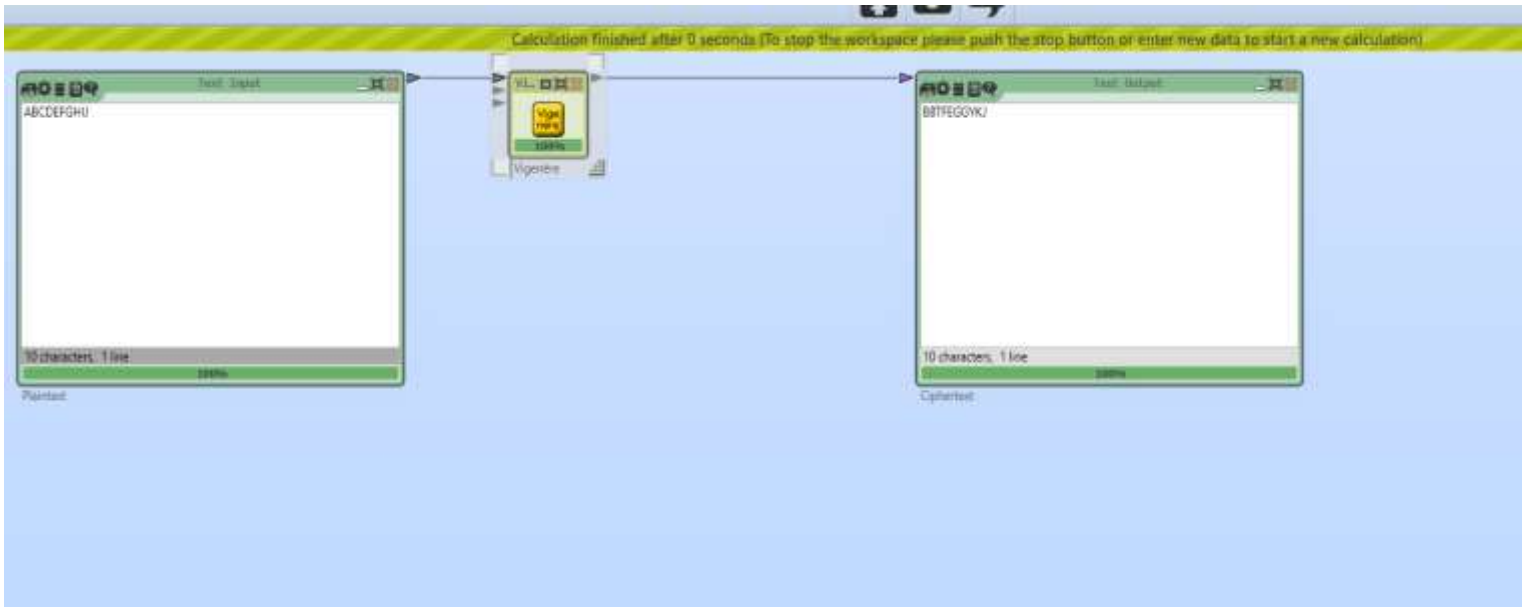
Key: **BARCA**

Plain text: **ABCDEFGHIJ**

For encryption we are taking standard Vigenère square table:

| Cipher Keyword | B | A | R | C | A | B | A | R | C | A |
|---|---|---|---|---|---|---|---|---|---|---|
| PlainText | A | B | C | D | E | F | G | H | I | J |
| Encrypted Message | B | B | T | F | E | G | G | Y | K | J |

In this step, we generated our own cipher keyword, which was “BARCA”, and plaintext was “ABCDEFGHIJ”. We used the mentioned keyword to encrypt the plaintext. With using the Vigenere square the message send was “BBTFEGGYKJ”. The receiver would receive this message.



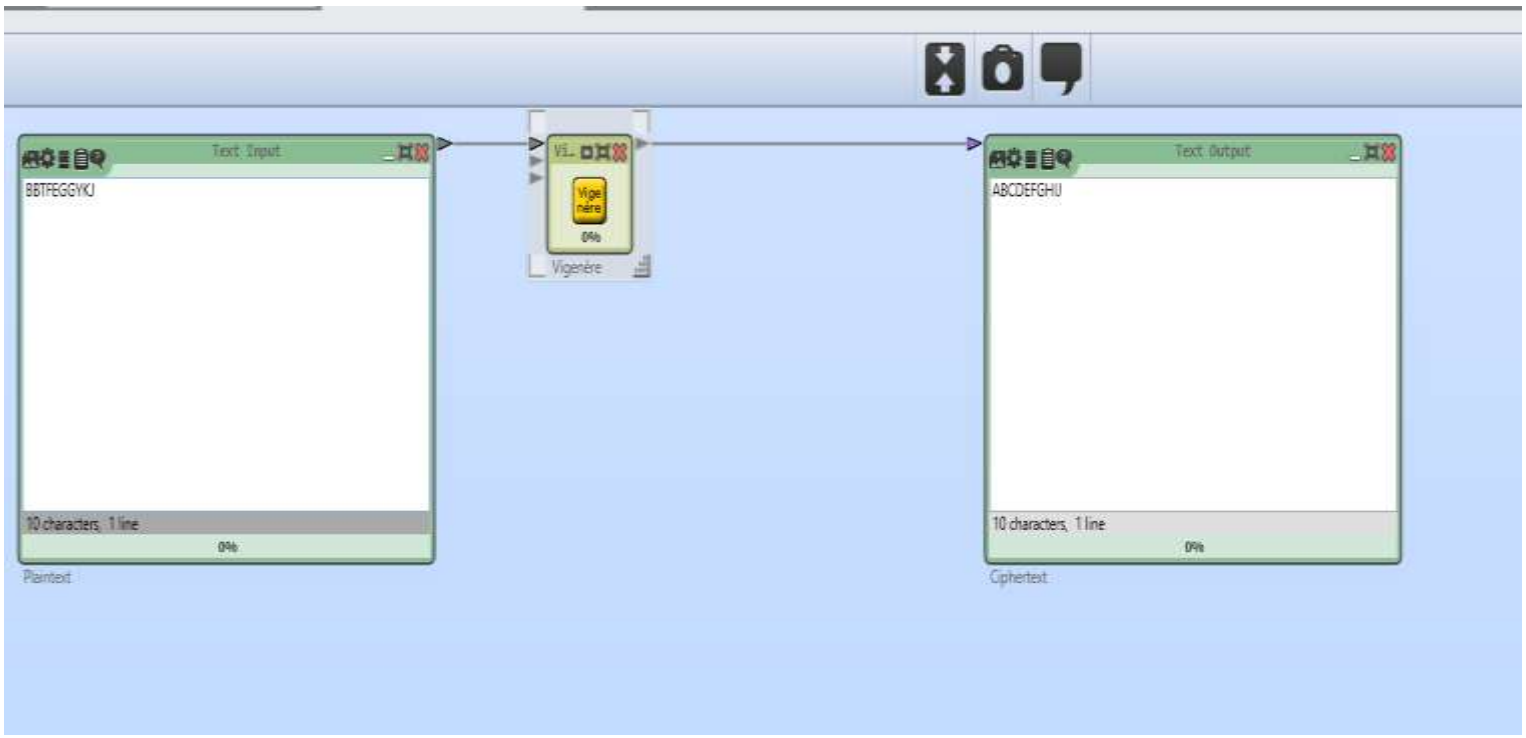

## PART 3

For decryption on other side, we use Vigenère square table.

| Cipher Keyword | B | A | R | C | A | B | A | R | C | A |
|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Encrypted Message | B | B | T | F | E | F | G | H | I | J |
| Decrypted Message | A | B | C | D | E | F | G | H | I | J |

Now at the receiver end to receive the encrypted message which was “BBTFEGGYKJ” we again used the Vigenere square to decrypt the message. Using it the receiver would get the answer as “ABCDEFGHIJ”




# REFLECTION

1. Could the Vigenère cipher be used to decode messages in the field without a computer?

- Yes, we could use the Vigenère cipher to decode messages in the field without a computer because with a key and a Vigenère square, we can manually decode communications in the field without the use of a computer using the Vigenère cipher. It requires careful attention to detail, but it can be used to reverse

encryption by matching the square with the ciphertext and the key.

2. Search the internet for Vigenère cipher cracking tools. Is the Vignere cipher considered a strong encryption system that is difficult to crack?

- No, it is not considered a strong encryption system because it is vulnerable to several attacks. The repeating patterns in this cipher and the short and resued keys makes it easy to crack the length of the key and the plaintext.