# Homework #5 – Vigenère cipher

**Due**: 12/05/2017 by 11:59pm

You may submit the homework up to 24 hours late for a 20% penalty.

**Deliverables:**

Submit the source file (.asm) to Canvas before the due date. This should be the only file you submit to Canvas.

The file should be named {USERNAME}-HW{NUMBER}.asm

E.g. abc0003-HW5.asm

**Specifications:**

This program has two objectives. The first objective is to create a procedure that will take plaintext and an encryption key, use the Vigenère cipher, and encrypt the plaintext. The second objective is to create a procedure that will take cyphertext, an encryption key, use the Vigenère cipher, and decrypt the cyphertext.

Assume that all characters will be uppercase letters, no spaces, symbols, etc.

All "high level" directives are not allowed on this homework. (e.g. .IF .ENDIF .REPEAT, etc.)

**Design:**

Create a BYTE array with the label 'pt'. This array may be of any length between 2 and 20. This will hold the plaintext.

Create a BYTE array with the label 'key'. This array will have length between 1 and (LENGHTOF pt - 1). Meaning the lower bound for 'key' is one character and the upper bound is one less than the number of characters in 'pt'.

Create a BYTE array with the label 'ct'. This array will have length equal to LENGTHOF pt. This will hold the cyphertext. The cyphertext will always have as many characters as the plaintext.

You may create any other values you deem necessary.

You must have two procedures for this homework. One procedure to handle the encryption, the other to handle the decryption. You may create other procedures if you wish.

**Example of encryption / decryption:**

For more information check the Wiki link: (https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher)

Link to the full cypher grid (https://upload.wikimedia.org/wikipedia/commons/9/9a/Vigen%C3%A8re_square_shading.svg)

The example below will use the plaintext word MEMORY and the key BAD.

First you "line up" your plaintext word with your key by writing the key directly beneath the plaintext word. Continue to repeat the key under each plaintext character:

MEMORY

BADBAD

In the above example MEMORY is longer than BAD, therefore, BAD was repeated.

Next choose each character in the plaintext word, starting with the first and encrypt it.

To encrypt a character, you first find the column on the chart corresponding to the character in the plaintext, e.g. the character M (circled in blue). Next, find the row starting with the key character, e.g. the character B (circled in red). Finally, find where the plaintext column and the key row intersect, e.g. the character N (circled in yellow). Continue this for each character.

MEMORY

BADBAD

N

| | 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 |

MEMORY

BADBAD

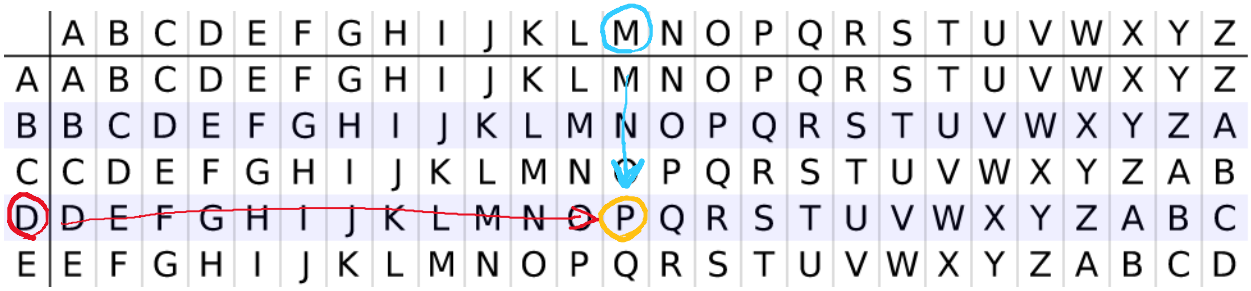
NE

| | 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 |

MEMORY

BADBAD

NEP



Continue until all characters have been encrypted:

MEMORY (plaintext)

BADBAD (key)

NEPPRB (cyphertext)

Decrypting is the opposite of encrypting. To decrypt NEPPRB first write the key under the cyphertext. Then find the row starting with the key character. Next, move across that row until you find the cyphertext character. The cyphertext character's column is the plaintext column.

NEPPRB

BADBAD

M

NEPPRB

BADBAD

ME

| | 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 |

NEPPRB

BADBAD

MEM

| | 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 |

Continue until the cyphertext has been decrypted:

NEPPRB

BADBAD

MEMORY