INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre: Mora Ayala José Antonio

# Actividad 1.- Cifrador Afín

Considera el alfabeto en Inglés (26 caracteres)

| Factor múltiplicativo | 7 |
|---|---|

| Corrimiento (aditivo) | 17 |
|---|---|

| Alfabeto | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Número | 0 | 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 |
| Resultado de la transformación | 17 | 24 | 5 | 12 | 19 | 0 | 7 | 14 | 21 | 2 | 9 | 16 | 23 | 4 | 11 | 18 | 25 | 6 | 13 | 20 | 1 | 8 | 15 | 22 | 3 | 10 |
| Letra correspondiente | R | Y | F | M | T | A | H | O | V | C | J | Q | X | E | L | S | Z | G | N | U | B | I | P | W | D | K |

| Message . | c | r | y | p | t | o | g | r | a | p | h | y | c | l | a | s | s |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | **F** | **G** | **D** | **S** | **U** | **L** | **H** | **G** | **R** | **S** | **O** | **D** | **F** | **Q** | **R** | **N** | **N** |

Ejercicio 0

Suppose someone uses the Shift 19 cipher and sends the message **LHXTLR** to you, find the original message.

**C=p+19 mod 26**

**m=**


M. en C. Nidia A. Cortez Duarte

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre: Mora Ayala José Antonio

# Actividad 1.- Cifrador Afín

## Ejercicio 1

| Factor múltiplicativo | 3 |
|---|---|

| Corrimiento (aditivo) | 2 |
|---|---|

| Alfabeto | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Número | 0 | 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 |
| Resultado de la transformación | 2 | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 1 | 4 | 7 | 10 | 13 | 16 | 19 | 22 | 25 |
| Letra correspondiente | **C** | **F** | **I** | **L** | **O** | **R** | **U** | **X** | **A** | **D** | **G** | **J** | **M** | **P** | **S** | **V** | **Y** | **B** | **E** | **H** | **K** | **N** | **Q** | **T** | **W** | **Z** |

| Message . | c | r | y | p | t | o | g | r | a | p | h | y | c | l | a | s | s |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | **I** | **B** | **W** | **V** | **H** | **S** | **U** | **B** | **C** | **V** | **X** | **W** | **I** | **J** | **C** | **E** | **E** |

## Ejercicio 2

| Factor múltiplicativo | 2 |
|---|---|

| Corrimiento (aditivo) | 5 |
|---|---|

| Alfabeto | **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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Número | **0** | **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 |
| Resultado de la transformación | **5** | **7** | **9** | **11** | **13** | **15** | **17** | **19** | **21** | **23** | **25** | **1** | 3 | **5** | **7** | **9** | **11** | **13** | **15** | **17** | **19** | **21** | **23** | **25** | **1** | 3 |
| Letra correspondiente | **F** | **H** | **J** | **L** | **N** | **P** | **R** | **T** | **V** | **X** | **Z** | **B** | D | **F** | **H** | **J** | **L** | **N** | **P** | **R** | **T** | **V** | **X** | **Z** | **B** | C |

| Message . | c | r | y | p | t | o | g | r | a | p | h | y | c | l | a | s | s |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | **J** | **N** | **B** | **J** | **R** | **H** | **R** | **N** | **F** | **J** | **T** | **B** | **J** | **B** | **F** | **P** | **P** |


M. en C. Nidia A. Cortez Duarte

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre: Mora Ayala José Antonio

# Actividad 1.- Cifrador Afín

Nota: Los procedimientos deben realizarse a mano, debes escanear tus notas o tomar una foto e incluirla como imagen al final de este archivo.

Trabajos sin procedimientos a mano valen 0 puntos.

Al finalizar guarda tu archivo como PDF para subirlo a Classroom.


M. en C. Nidia A. Cortez Duarte

**INSTITUTO POLITÉCNICO NACIONAL**
**ESCUELA SUPERIOR DE CÓMPUTO**
**Nombre: Mora Ayala José Antonio**

# Actividad 1.- Cifrador Afín

## Ejercicio 1

Ejercicio Cifrando los mensajes

Alfabeto 1 Factor multiplicativo 3 Corrimiento (aditivo) 2
$\alpha$ $\beta$

$C = \alpha p + \beta \bmod 26$ 26 Considerando alfabeto en inglés

$C = 3(Q) + 2 \bmod 26$
$C = 3(0) + 2 \bmod 26$
$C = 2 \longrightarrow C$

$C = 3(K) + 2 \bmod 26$
$C = 3(10) + 2 \bmod 26$
$C = 6 \quad G$

$C = 3(U) + 2 \bmod 26$
$C = 3(20) + 2 \bmod 26$
$C = 10 \quad K$

$C = 3(b) + 2 \bmod 26$
$C = 3(1) + 2 \bmod 26$
$C = 5 \quad F$

$C = 3(I) + 2 \bmod 26$
$C = 3(11) + 2 \bmod 26$
$C = 9 \quad J$

$C = 3(V) + 2 \bmod 26$
$C = 3(21) + 2 \bmod 26$
$C = 13 \quad N$

$C = 3(C) + 2 \bmod 26$
$C = 3(2) + 2 \bmod 26$
$C = 8 \quad i$

$C = 3(m) + 2 \bmod 26$
$C = 3(12) + 2 \bmod 26$
$C = 12 \quad M$

$C = 3(W) + 2 \bmod 26$
$C = 3(22) + 2 \bmod 26$
$C = 16 \quad Q$

$C = 3(d) + 2 \bmod 26$
$C = 3(3) + 2 \bmod 26$
$C = 11 \quad L$

$C = 3(n) + 2 \bmod 26$
$C = 3(13) + 2 \bmod 26$
$C = 15 \quad P$

$C = 3(X) + 2 \bmod 26$
$C = 3(23) + 2 \bmod 26$
$C = 19 \quad T$

$C = 3(e) + 2 \bmod 26$
$C = 3(4) + 2 \bmod 26$
$C = 14 \quad O$

$C = 3(O) + 2 \bmod 26$
$C = 3(19) + 2 \bmod 26$
$C = 18 \quad S$

$C = 3(Y) + 2 \bmod 26$
$C = 3(24) + 2 \bmod 26$
$C = 22 \quad W$

$C = 3(f) + 2 \bmod 26$
$C = 3(5) + 2 \bmod 26$
$C = 17 \quad R$

$C = 3(p) + 2 \bmod 26$
$C = 3(15) + 2 \bmod 26$
$C = 21 \quad V$

$C = 3(Z) + 2 \bmod 26$
$C = 3(25) + 2 \bmod 26$
$C = 25 \quad z$

$C = 3(g) + 2 \bmod 26$
$C = 3(6) + 2 \bmod 26$
$C = 20 \quad U$

$C = 3(q) + 2 \bmod 26$
$C = 3(16) + 2 \bmod 26$
$C = 29 \quad Y$

$C = 3(h) + 2 \bmod 26$
$C = 3(7) + 2 \bmod 26$
$C = 23 \quad X$

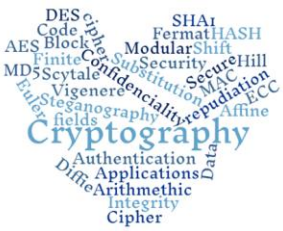
$C = 3(r) + 2 \bmod 26$
$C = 3(17) + 2 \bmod 26$
$C = 1 \quad B$

$C = 3(i) + 2 \bmod 26$
$C = 3(8) + 2 \bmod 26$
$C = 0 \quad A$

$C = 3(s) + 2 \bmod 26$
$C = 3(18) + 2 \bmod 26$
$C = 4 \quad E$

$C = 3(j) + 2 \bmod 26$
$C = 3(9) + 2 \bmod 26$
$C = 3 \quad D$

$C = 3(t) + 2 \bmod 26$
$C = 3(19) + 2 \bmod 26$
$C = 7 \quad H$




M. en C. Nidia A. Cortez Duarte

**INSTITUTO POLITÉCNICO NACIONAL**
**ESCUELA SUPERIOR DE CÓMPUTO**
**Nombre: Mora Ayala José Antonio**

# Actividad 1.- Cifrador Afín

## Ejercicio 2

Ejercicio Cifrando los mensajes

Actividad 1 Factor multiplicativo 2 Corrimiento (aditivo) 5
$\alpha$ $\beta$

$C = 2p + 8 \bmod 26$ 26 Considerando alfabeto en inglés

$C = 2(Q) + 5 \bmod 26$
$C = 2(0) + 5 \bmod 26$
$C = 5$ F

$C = 2(b) + 5 \bmod 26$
$C = 2(1) + 5 \bmod 26$
$C = 7$ H

$C = 2(C) + 5 \bmod 26$
$C = 2(2) + 5 \bmod 26$
$C = 9$ J

$C = 2(d) + 5 \bmod 26$
$C = 2(3) + 5 \bmod 26$
$C = 11$ L

$C = 2(e) + 5 \bmod 26$
$C = 2(4) + 5 \bmod 26$
$C = 13$ N

$C = 2(f) + 5 \bmod 26$
$C = 2(5) + 5 \bmod 26$
$C = 15$ P

$C = 2(g) + 5 \bmod 26$
$C = 2(6) + 5 \bmod 26$
$C = 17$ R

$C = 2(h) + 5 \bmod 26$
$C = 2(7) + 5 \bmod 26$
$C = 19$ T

$C = 2(i) + 5 \bmod 26$
$C = 2(8) + 5 \bmod 26$
$C = 21$ V

$C = 2(j) + 5 \bmod 26$
$C = 2(9) + 5 \bmod 26$
$C = 23$ X

$C = 2(K) + 5 \bmod 26$
$C = 2(10) + 5 \bmod 26$
$C = 25$ Z

$C = 2(l) + 5 \bmod 26$
$C = 2(11) + 5 \bmod 26$
$C = 1$ B

$C = 2(m) + 5 \bmod 26$
$C = 2(12) + 5 \bmod 26$
$C = 3$ D

$C = 2(n) + 5 \bmod 26$
$C = 2(13) + 5 \bmod 26$
$C = 5$ F

$C = 2(O) + 5 \bmod 26$
$C = 2(14) + 5 \bmod 26$
$C = 7$ H

$C = 2(p) + 5 \bmod 26$
$C = 2(15) + 5 \bmod 26$
$C = 9$ J

$C = 2(9) + 5 \bmod 26$
$C = 2(16) + 5 \bmod 26$
$C = 11$ L

$C = 2(r) + 5 \bmod 26$
$C = 2(17) + 5 \bmod 26$
$C = 13$ N

$C = 2(s) + 5 \bmod 26$
$C = 2(18) + 5 \bmod 26$
$C = 15$ P

$C = 2(t) + 5 \bmod 26$
$C = 2(19) + 5 \bmod 26$
$C = 17$ R

$C = 2(U) + 5 \bmod 26$
$C = 2(20) + 5 \bmod 26$
$C = 19$ T

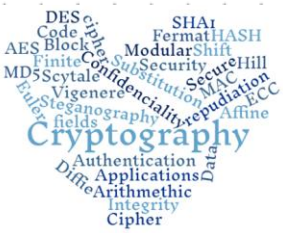
$C = 2(V) + 5 \bmod 26$
$C = 2(21) + 5 \bmod 26$
$C = 21$ V

$C = 2(W) + 5 \bmod 26$
$C = 2(22) + 5 \bmod 26$
$C = 23$ X

$C = 2(X) + 5 \bmod 26$
$C = 2(23) + 5 \bmod 26$
$C = 25$ Z

$C = 2(Y) + 5 \bmod 26$
$C = 2(24) + 5 \bmod 26$
$C = 1$ B

$C = 2(Z) + 5 \bmod 26$
$C = 2(25) + 5 \bmod 26$
$C = 3$ C




M. en C. Nidia A. Cortez Duarte