

Actividad 1.- Cifrador Afín

Considera el alfabeto en Inglés (26 caracteres)

| | |
|-----------------------|---|
| Factor multiplicativo | 7 |
|-----------------------|---|

| | |
|-----------------------|---|
| Corrimiento (aditivo) | 1 |
| | 7 |

| 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 1

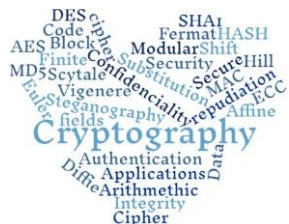
| | |
|-----------------------|---|
| Factor multiplicativo | 3 |
|-----------------------|---|

| | |
|-----------------------|---|
| 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 |

M. en C. Nidia A. Cortez Duarte



Actividad 1.- Cifrador Afín

Ejercicio 2

| | |
|-----------------------|---|
| Factor multiplicativo | 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 | D |

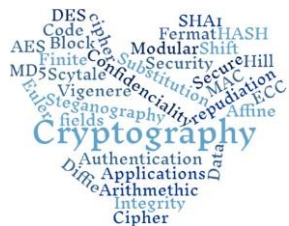
| Message . | c | r | y | p | t | o | g | r | a | p | h | y | c | l | a | s | s |
|------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | J | N | B | J | T | H | R | N | F | J | T | B | J | B | F | P | P |

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



Actividad 1.- Cifrador Afín

Procedimientos:

-Chacón Inostrosa Jaime Enrique:

| Actividad #1: Cifrador Afín | | | |
|-----------------------------|--------------------|-----------|-------|
| Ejercicio #1: | | | |
| | | Mod 26 | Letra |
| A | $0 \times 3 = 0$ | $+2 = 2$ | C |
| B | $1 \times 3 = 3$ | $+2 = 5$ | F |
| C | $2 \times 3 = 6$ | $+2 = 8$ | I |
| D | $3 \times 3 = 9$ | $+2 = 11$ | L |
| E | $4 \times 3 = 12$ | $+2 = 14$ | O |
| F | $5 \times 3 = 15$ | $+2 = 17$ | R |
| G | $6 \times 3 = 18$ | $+2 = 20$ | U |
| H | $7 \times 3 = 21$ | $+2 = 23$ | X |
| I | $8 \times 3 = 24$ | $+2 = 26$ | A |
| J | $9 \times 3 = 27$ | $+2 = 29$ | D |
| K | $10 \times 3 = 30$ | $+2 = 32$ | G |
| L | $11 \times 3 = 33$ | $+2 = 35$ | J |
| M | $12 \times 3 = 36$ | $+2 = 38$ | M |
| N | $13 \times 3 = 39$ | $+2 = 41$ | P |
| O | $14 \times 3 = 42$ | $+2 = 44$ | S |
| P | $15 \times 3 = 45$ | $+2 = 47$ | V |
| Q | $16 \times 3 = 48$ | $+2 = 50$ | Y |
| R | $17 \times 3 = 51$ | $+2 = 53$ | B |
| S | $18 \times 3 = 54$ | $+2 = 56$ | E |
| T | $19 \times 3 = 57$ | $+2 = 59$ | H |
| U | $20 \times 3 = 60$ | $+2 = 62$ | K |
| V | $21 \times 3 = 63$ | $+2 = 65$ | N |
| W | $22 \times 3 = 66$ | $+2 = 68$ | Q |
| X | $23 \times 3 = 69$ | $+2 = 71$ | T |
| Y | $24 \times 3 = 72$ | $+2 = 74$ | W |
| Z | $25 \times 3 = 75$ | $+2 = 77$ | Z |

| Ejercicio #2 | | | |
|--------------|--------------------|------------|-------|
| | | Mod 26 | Letra |
| A | $0 \times 2 = 0$ | $+12 = 12$ | M |
| B | $1 \times 2 = 2$ | $+12 = 14$ | O |
| C | $2 \times 2 = 4$ | $+12 = 16$ | Q |
| D | $3 \times 2 = 6$ | $+12 = 18$ | S |
| E | $4 \times 2 = 8$ | $+12 = 20$ | U |
| F | $5 \times 2 = 10$ | $+12 = 22$ | W |
| G | $6 \times 2 = 12$ | $+12 = 24$ | Y |
| H | $7 \times 2 = 14$ | $+12 = 26$ | A |
| I | $8 \times 2 = 16$ | $+12 = 28$ | C |
| J | $9 \times 2 = 18$ | $+12 = 30$ | E |
| K | $10 \times 2 = 20$ | $+12 = 32$ | G |
| L | $11 \times 2 = 22$ | $+12 = 34$ | I |
| M | $12 \times 2 = 24$ | $+12 = 36$ | K |
| N | $13 \times 2 = 26$ | $+12 = 38$ | M |
| O | $14 \times 2 = 28$ | $+12 = 40$ | O |
| P | $15 \times 2 = 30$ | $+12 = 42$ | Q |
| Q | $16 \times 2 = 32$ | $+12 = 44$ | S |
| R | $17 \times 2 = 34$ | $+12 = 46$ | U |
| S | $18 \times 2 = 36$ | $+12 = 48$ | W |
| T | $19 \times 2 = 38$ | $+12 = 50$ | Y |
| U | $20 \times 2 = 40$ | $+12 = 52$ | A |
| V | $21 \times 2 = 42$ | $+12 = 54$ | C |
| W | $22 \times 2 = 44$ | $+12 = 56$ | E |
| X | $23 \times 2 = 46$ | $+12 = 58$ | G |
| Y | $24 \times 2 = 48$ | $+12 = 60$ | I |
| Z | $25 \times 2 = 50$ | $+12 = 62$ | K |

NOTA: El mensaje no se puede decifrar porque de repiten valores



M. en C. Nidia A. Cortez Duarte

Actividad 1.- Cifrador Afín

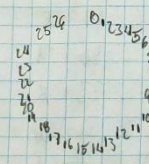
-Sánchez Méndez Edmundo Josué:

Ejercicio 1

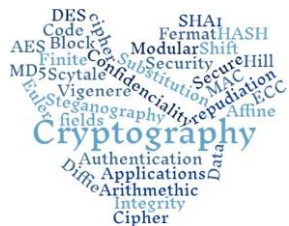
Factor multiplicativo: 3 Corrimiento aditivo: 2

$a \rightarrow [(0 \times 3) + 2] \bmod 26 = 2 \bmod 26 = 2 \rightarrow C$
 $b \rightarrow [(1 \times 3) + 2] \bmod 26 = 5 \bmod 26 = 5 \rightarrow F$
 $c \rightarrow [(2 \times 3) + 2] \bmod 26 = 8 \bmod 26 = 8 \rightarrow I$
 $d \rightarrow [(3 \times 3) + 2] \bmod 26 = 11 \bmod 26 = 11 \rightarrow L$
 $e \rightarrow [(4 \times 3) + 2] \bmod 26 = 14 \bmod 26 = 14 \rightarrow O$
 $f \rightarrow [(5 \times 3) + 2] \bmod 26 = 17 \bmod 26 = 17 \rightarrow R$
 $g \rightarrow [(6 \times 3) + 2] \bmod 26 = 20 \bmod 26 = 20 \rightarrow U$
 $h \rightarrow [(7 \times 3) + 2] \bmod 26 = 23 \bmod 26 = 23 \rightarrow X$
 $i \rightarrow [(8 \times 3) + 2] \bmod 26 = 26 \bmod 26 = 0 \rightarrow A$
 $j \rightarrow [(9 \times 3) + 2] \bmod 26 = 29 \bmod 26 = 3 \rightarrow D$
 $k \rightarrow [(10 \times 3) + 2] \bmod 26 = 32 \bmod 26 = 6 \rightarrow G$
 $l \rightarrow [(11 \times 3) + 2] \bmod 26 = 35 \bmod 26 = 9 \rightarrow J$
 $m \rightarrow [(12 \times 3) + 2] \bmod 26 = 38 \bmod 26 = 12 \rightarrow M$
 $n \rightarrow [(13 \times 3) + 2] \bmod 26 = 41 \bmod 26 = 15 \rightarrow P$
 $o \rightarrow [(14 \times 3) + 2] \bmod 26 = 44 \bmod 26 = 18 \rightarrow S$
 $p \rightarrow [(15 \times 3) + 2] \bmod 26 = 47 \bmod 26 = 21 \rightarrow V$
 $q \rightarrow [(16 \times 3) + 2] \bmod 26 = 50 \bmod 26 = 24 \rightarrow Y$
 $r \rightarrow [(17 \times 3) + 2] \bmod 26 = 53 \bmod 26 = 1 \rightarrow B$
 $s \rightarrow [(18 \times 3) + 2] \bmod 26 = 56 \bmod 26 = 4 \rightarrow E$

$t \rightarrow [(19 \times 3) + 2] \bmod 26 = 59 \bmod 26 = 7 \rightarrow H$
 $u \rightarrow [(20 \times 3) + 2] \bmod 26 = 62 \bmod 26 = 10 \rightarrow K$
 $v \rightarrow [(21 \times 3) + 2] \bmod 26 = 65 \bmod 26 = 13 \rightarrow N$
 $w \rightarrow [(22 \times 3) + 2] \bmod 26 = 68 \bmod 26 = 16 \rightarrow Q$
 $x \rightarrow [(23 \times 3) + 2] \bmod 26 = 71 \bmod 26 = 19 \rightarrow T$
 $y \rightarrow [(24 \times 3) + 2] \bmod 26 = 74 \bmod 26 = 22 \rightarrow W$
 $z \rightarrow [(25 \times 3) + 2] \bmod 26 = 77 \bmod 26 = 25 \rightarrow Z$



M. en C. Nidia A. Cortez Duarte



Actividad 1.- Cifrador Afín

Ejercicio 2
Factor multiplicativo: 2 Corrimiento Aditivo: 5

$$a \rightarrow [(0 \times 2) + 5] \bmod 26 = 5 \bmod 26 = 5 \rightarrow F$$

$$b \rightarrow [(1 \times 2) + 5] \bmod 26 = 7 \bmod 26 = 7 \rightarrow H$$

$$c \rightarrow [(2 \times 2) + 5] \bmod 26 = 9 \bmod 26 = 9 \rightarrow J$$

$$d \rightarrow [(3 \times 2) + 5] \bmod 26 = 11 \bmod 26 = 11 \rightarrow L$$

$$e \rightarrow [(4 \times 2) + 5] \bmod 26 = 13 \bmod 26 = 13 \rightarrow M$$

$$f \rightarrow [(5 \times 2) + 5] \bmod 26 = 15 \bmod 26 = 15 \rightarrow P$$

$$g \rightarrow [(6 \times 2) + 5] \bmod 26 = 17 \bmod 26 = 17 \rightarrow Q$$

$$h \rightarrow [(7 \times 2) + 5] \bmod 26 = 19 \bmod 26 = 19 \rightarrow T$$

$$i \rightarrow [(8 \times 2) + 5] \bmod 26 = 21 \bmod 26 = 21 \rightarrow V$$

$$j \rightarrow [(9 \times 2) + 5] \bmod 26 = 23 \bmod 26 = 23 \rightarrow X$$

$$k \rightarrow [(10 \times 2) + 5] \bmod 26 = 25 \bmod 26 = 25 \rightarrow Z$$

$$l \rightarrow [(11 \times 2) + 5] \bmod 26 = 27 \bmod 26 = 1 \rightarrow B$$

$$m \rightarrow [(12 \times 2) + 5] \bmod 26 = 29 \bmod 26 = 3 \rightarrow D$$

$$n \rightarrow [(13 \times 2) + 5] \bmod 26 = 31 \bmod 26 = 5 \rightarrow F$$

$$o \rightarrow [(14 \times 2) + 5] \bmod 26 = 33 \bmod 26 = 7 \rightarrow H$$

$$p \rightarrow [(15 \times 2) + 5] \bmod 26 = 35 \bmod 26 = 9 \rightarrow J$$

$$q \rightarrow [(16 \times 2) + 5] \bmod 26 = 37 \bmod 26 = 11 \rightarrow L$$

$$r \rightarrow [(17 \times 2) + 5] \bmod 26 = 39 \bmod 26 = 13 \rightarrow N$$

$$s \rightarrow [(18 \times 2) + 5] \bmod 26 = 41 \bmod 26 = 15 \rightarrow P$$

$$t \rightarrow [(19 \times 2) + 5] \bmod 26 = 43 \bmod 26 = 17 \rightarrow Q$$

$$u \rightarrow [(20 \times 2) + 5] \bmod 26 = 45 \bmod 26 = 19 \rightarrow T$$

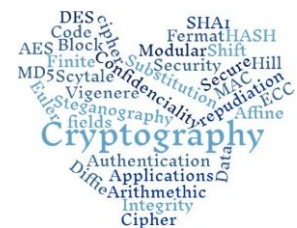
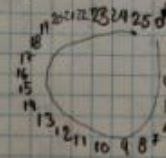
$$v \rightarrow [(21 \times 2) + 5] \bmod 26 = 47 \bmod 26 = 21 \rightarrow V$$

$$w \rightarrow [(22 \times 2) + 5] \bmod 26 = 49 \bmod 26 = 23 \rightarrow X$$

$$x \rightarrow [(23 \times 2) + 5] \bmod 26 = 51 \bmod 26 = 25 \rightarrow Z$$

$$y \rightarrow [(24 \times 2) + 5] \bmod 26 = 53 \bmod 26 = 1 \rightarrow B$$

$$z \rightarrow [(25 \times 2) + 5] \bmod 26 = 55 \bmod 26 = 3 \rightarrow D$$



M. en C. Nidia A. Cortez Duarte

Actividad 1.- Cifrador Afín

-Ramírez Olvera Guillermo:

Ejercicio 1

| Factor: mltiplicativo: 3 | Corrección (aditivo): 2 |
|--|--|
| $a \Rightarrow 0 \times 3 \Rightarrow 0 + 2 = 2 = c$ | $u \Rightarrow 21 \times 3 \Rightarrow 66 \mid 26 = 14 + 2 = 16 = q$ |
| $b \Rightarrow 1 \times 3 \Rightarrow 3 + 2 = 5 = f$ | $x \Rightarrow 23 \times 3 \Rightarrow 69 \mid 26 = 17 + 2 = 19 = t$ |
| $c \Rightarrow 2 \times 3 \Rightarrow 6 + 2 = 8 = i$ | $y \Rightarrow 24 \times 3 \Rightarrow 72 \mid 26 = 20 + 2 = 22 = v$ |
| $d \Rightarrow 3 \times 3 \Rightarrow 9 + 2 = 11 = l$ | $z \Rightarrow 25 \times 3 \Rightarrow 75 \mid 26 = 23 + 2 = 25 = z$ |
| $e \Rightarrow 4 \times 3 \Rightarrow 12 + 2 = 14 = o$ | |
| $f \Rightarrow 5 \times 3 \Rightarrow 15 + 2 = 17 = r$ | |
| $g \Rightarrow 6 \times 3 \Rightarrow 18 + 2 = 20 = u$ | |
| $h \Rightarrow 7 \times 3 \Rightarrow 21 + 2 = 23 = x$ | |
| $i \Rightarrow 8 \times 3 \Rightarrow 24 + 2 = 26 = a$ | |
| $j \Rightarrow 9 \times 3 \Rightarrow 27 \mid 26 \Rightarrow 1 + 2 = 3 = d$ | |
| $k \Rightarrow 10 \times 3 \Rightarrow 30 \mid 26 \Rightarrow 4 + 2 = 6 = g$ | |
| $l \Rightarrow 11 \times 3 \Rightarrow 33 \mid 26 \Rightarrow 7 + 2 = 9 = j$ | |
| $m \Rightarrow 12 \times 3 \Rightarrow 36 \mid 26 \Rightarrow 10 + 2 = 12 = m$ | |
| $n \Rightarrow 13 \times 3 \Rightarrow 39 \mid 26 = 13 + 2 = 15 = p$ | |
| $o \Rightarrow 14 \times 3 \Rightarrow 42 \mid 26 = 16 + 2 = 18 = s$ | |
| $p \Rightarrow 15 \times 3 \Rightarrow 45 \mid 26 = 19 + 2 = 21 = v$ | |
| $q \Rightarrow 16 \times 3 \Rightarrow 48 \mid 26 = 22 + 2 = 24 = y$ | |
| $r \Rightarrow 17 \times 3 \Rightarrow 51 \mid 26 = 25 + 2 = 27 = b$ | |
| $s \Rightarrow 18 \times 3 \Rightarrow 54 \mid 26 = 28 + 2 = 30 = e$ | |
| $t \Rightarrow 19 \times 3 \Rightarrow 57 \mid 26 = 31 + 2 = 33 = h$ | |
| $u \Rightarrow 20 \times 3 \Rightarrow 60 \mid 26 = 34 + 2 = 36 = k$ | |
| $v \Rightarrow 21 \times 3 \Rightarrow 63 \mid 26 = 37 + 2 = 39 = n$ | |

M. en C. Nidia A. Cortez Duarte

