CIFRADO DE TEXTO MEDIANTE EL MÉTODO AFÍN

Laura Vanessa Méndez Rivera - 2191951

César Luis Hurtado Rodriguez - 2191957

Daniel Eduardo Cobos Ayala - 2191954

CIFRAR O ENCRIPTAR

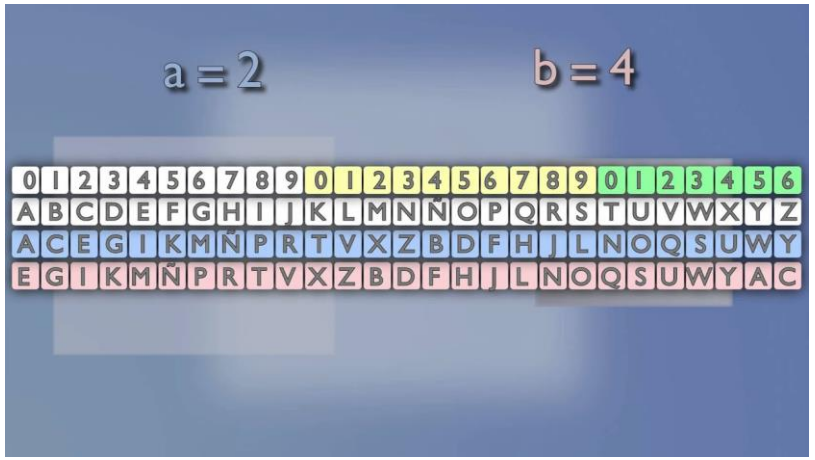
- Cifrar una información significa **ocultar el contenido de un mensaje a simple vista**, de manera que haga falta una interacción concreta para poder desvelar ese contenido.

¿PARA QUE SIRVE?

- El cifrado de mensajes sirve para hacer las comunicaciones más seguras, el cifrado es la base principal de la seguridad de datos. Es la forma más sencilla e importante para garantizar que la información de un mensaje o una computadora no sea leída ni robada por alguien que desee utilizarla con fines maliciosos.

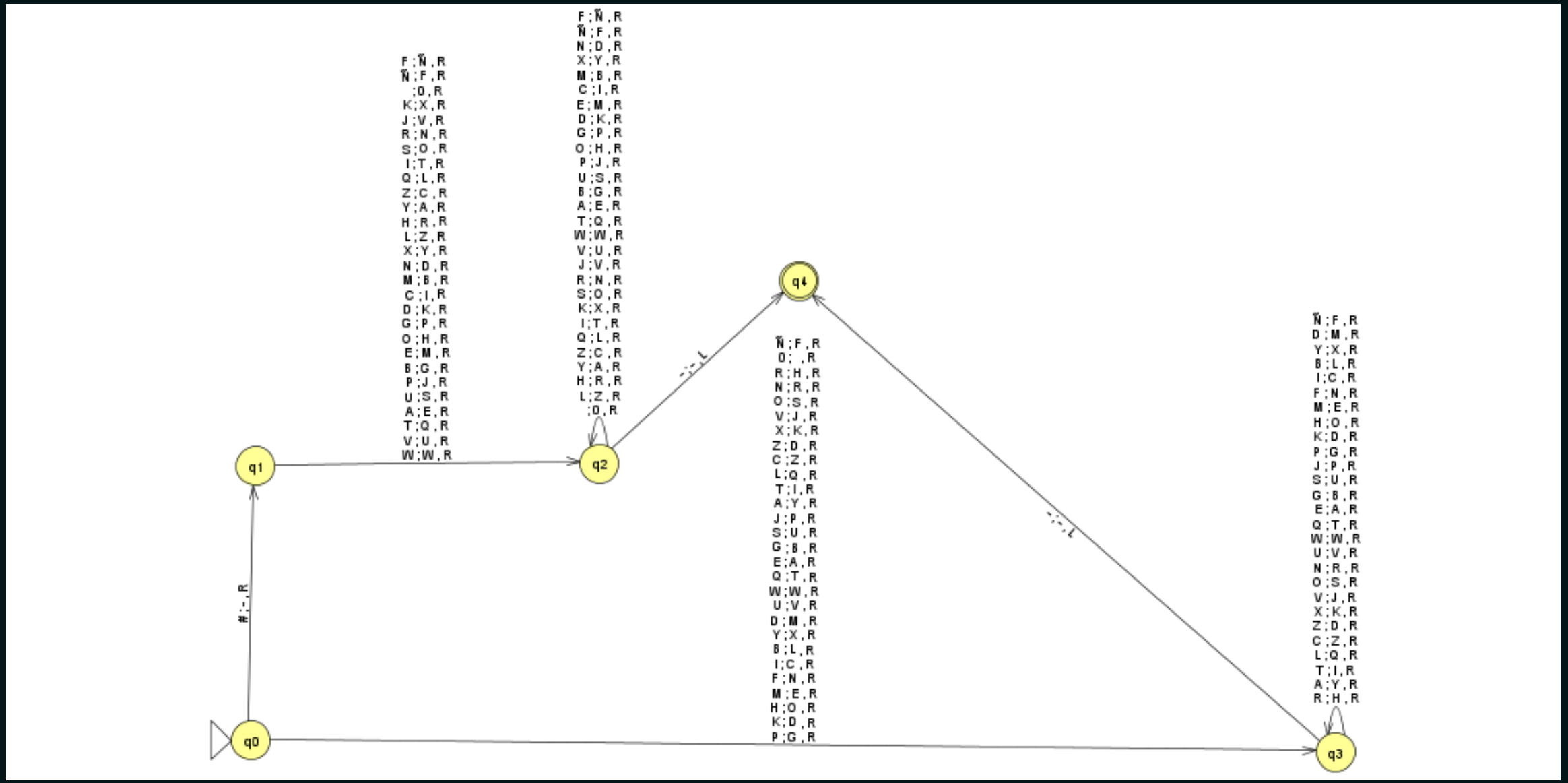
CIFRADO AFÍN

- El cifrado afín también se le llama cifrado de transformación afín o cifrado mono alfabético genérico. Es un tipo de cifrado por sustitución en el que cada símbolo del alfabeto en claro es sustituido por un símbolo del alfabeto cifrado siendo el número de símbolos del alfabeto en claro igual que el número de símbolos del alfabeto cifrado.



MAQUINA DE TURING

- Una máquina de Turing es un dispositivo que manipula símbolos sobre una tira de cinta de acuerdo con una tabla de reglas. A pesar de su simplicidad, una máquina de Turing puede ser adaptada para simular la lógica de cualquier algoritmo de computador.


q0
q1
q2
q3
q4
#;-,R
F;Ñ,R
Ñ;F,R
;D,R
K;X,R
J;V,R
R;N,R
S;O,R
I;T,R
Q;L,R
Z;C,R
Y;A,R
H;R,R
L;Z,R
X;Y,R
N;D,R
M;B,R
C;I,R
D;K,R
G;P,R
O;H,R
E;M,R
B;G,R
P;J,R
U;S,R
A;E,R
T;Q,R
V;U,R
W;W,R
F;Ñ,R
Ñ;F,R
N;D,R
X;Y,R
M;B,R
C;I,R
E;M,R
D;K,R
G;P,R
O;H,R
P;J,R
U;S,R
B;G,R
A;E,R
T;Q,R
W;W,R
V;U,R
J;V,R
R;N,R
S;O,R
K;X,R
I;T,R
Q;L,R
Z;C,R
Y;A,R
H;R,R
L;Z,R
;D,R
-;-,L
Ñ;F,R
O; ,R
R;H,R
N;R,R
O;S,R
V;J,R
X;K,R
Z;D,R
C;Z,R
L;Q,R
T;I,R
A;Y,R
J;P,R
S;U,R
G;B,R
E;A,R
Q;T,R
W;W,R
U;V,R
D;M,R
Y;X,R
B;L,R
I;C,R
F;N,R
M;E,R
H;O,R
K;D,R
P;G,R
-;-,L
Ñ;F,R
D;M,R
Y;X,R
B;L,R
I;C,R
F;N,R
M;E,R
H;O,R
K;D,R
P;G,R
J;P,R
S;U,R
G;B,R
E;A,R
Q;T,R
W;W,R
U;V,R
N;R,R
O;S,R
V;J,R
X;K,R
Z;D,R
C;Z,R
L;Q,R
T;I,R
A;Y,R
R;H,R

DEFINICIÓN

$$MT = (Q, q_0, \mathrm{F}, \Sigma, \Gamma, B, \delta)$$

↓

$Q = \{q_0, q_1, q_2, q_3, q_4\}$

$q_0 = 'q_0'$

$F = 'q_4'$

$\Sigma = (A - Z), '\#', '0',$

$\Gamma = (A - Z), '\#, ' ' - ', '0' ,$

$\mathrm{B} = ' - '$

DEFINICIÓN

$\delta(q_0, \#) = (q_1, \#, R)$
$\delta(q_0, A) = (q_3, Y, R)$
$\delta(q_0, B) = (q_3, L, R)$
$\delta(q_0, C) = (q_3, Z, R)$
$\delta(q_0, D) = (q_3, M, R)$
$\delta(q_0, E) = (q_3, A, R)$
$\delta(q_0, F) = (q_3, N, R)$
$\delta(q_0, G) = (q_3, B, R)$
$\delta(q_0, H) = (q_3, O, R)$
$\delta(q_0, I) = (q_3, C, R)$
$\delta(q_0, J) = (q_3, P, R)$
$\delta(q_0, K) = (q_3, D, R)$
$\delta(q_0, L) = (q_3, Q, R)$
$\delta(q_0, M) = (q_3, E, R)$
$\delta(q_0, N) = (q_3, R, R)$
$\delta(q_0, \tilde{N}) = (q_3, F, R)$
$\delta(q_0, O) = (q_3, S, R)$
$\delta(q_0, P) = (q_3, G, R)$
$\delta(q_0, Q) = (q_3, T, R)$
$\delta(q_0, R) = (q_3, H, R)$
$\delta(q_0, S) = (q_3, U, R)$
$\delta(q_0, T) = (q_3, I, R)$
$\delta(q_0, U) = (q_3, V, R)$
$\delta(q_0, V) = (q_3, J, R)$
$\delta(q_0, W) = (q_3, W, R)$
$\delta(q_0, X) = (q_3, K, R)$
$\delta(q_0, Y) = (q_3, X, R)$
$\delta(q_0, Z) = (q_3, D, R)$
$\delta(q_0, 0) = (q_3, \quad, R)$
$\delta(q_1, A) = (q_2, E, R)$
$\delta(q_1, B) = (q_2, G, R)$
$\delta(q_1, C) = (q_2, I, R)$
$\delta(q_1, D) = (q_2, K, R)$
$\delta(q_1, E) = (q_2, M, R)$
$\delta(q_1, F) = (q_2, \tilde{N}, R)$
$\delta(q_1, G) = (q_2, P, R)$
$\delta(q_1, H) = (q_2, R, R)$
$\delta(q_1, I) = (q_2, T, R)$
$\delta(q_1, J) = (q_2, V, R)$
$\delta(q_1, K) = (q_2, X, R)$
$\delta(q_1, L) = (q_2, Z, R)$
$\delta(q_1, M) = (q_2, B, R)$
$\delta(q_1, N) = (q_2, F, R)$
$\delta(q_1, \tilde{N}) = (q_2, F, R)$
$\delta(q_1, O) = (q_2, H, R)$
$\delta(q_1, P) = (q_2, J, R)$
$\delta(q_1, Q) = (q_2, L, R)$
$\delta(q_1, R) = (q_2, N, R)$
$\delta(q_1, S) = (q_2, O, R)$
$\delta(q_1, T) = (q_2, Q, R)$
$\delta(q_1, U) = (q_2, S, R)$
$\delta(q_1, V) = (q_2, U, R)$
$\delta(q_1, W) = (q_2, W, R)$
$\delta(q_1, X) = (q_2, Y, R)$
$\delta(q_1, Y) = (q_2, A, R)$
$\delta(q_1, Z) = (q_2, C, R)$
$\delta(q_1, \quad) = (q_2, 0, R)$
$\delta(q_1, V) = (q_2, U, R)$
$\delta(q_2, A) = (q_2, E, R)$
$\delta(q_2, B) = (q_2, G, R)$
$\delta(q_2, C) = (q_2, I, R)$
$\delta(q_2, D) = (q_2, K, R)$
$\delta(q_2, E) = (q_2, M, R)$
$\delta(q_2, F) = (q_2, \tilde{N}, R)$
$\delta(q_2, G) = (q_2, P, R)$
$\delta(q_2, H) = (q_2, R, R)$
$\delta(q_2, I) = (q_2, T, R)$
$\delta(q_2, J) = (q_2, V, R)$
$\delta(q_2, K) = (q_2, X, R)$
$\delta(q_2, L) = (q_2, Z, R)$
$\delta(q_2, M) = (q_2, B, R)$
$\delta(q_2, N) = (q_2, F, R)$
$\delta(q_2, \tilde{N}) = (q_2, F, R)$
$\delta(q_2, O) = (q_2, H, R)$
$\delta(q_2, P) = (q_2, J, R)$
$\delta(q_2, Q) = (q_2, L, R)$

DEFINICIÓN

$\delta(q_2, R) = (q_2, N, R)$
$\delta(q_2, S) = (q_2, O, R)$
$\delta(q_2, T) = (q_2, Q, R)$
$\delta(q_2, U) = (q_2, S, R)$
$\delta(q_2, V) = (q_2, U, R)$
$\delta(q_2, W) = (q_2, W, R)$
$\delta(q_2, X) = (q_2, Y, R)$
$\delta(q_2, Y) = (q_2, A, R)$
$\delta(q_2, Z) = (q_2, C, R)$
$\delta(q_2, \quad) = (q_2, 0, R)$
$\delta(q_2, -) = (q_4, -, L)$

$\delta(q_3, -) = (q_4, -, L)$
$\delta(q_3, A) = (q_3, Y, R)$
$\delta(q_3, B) = (q_3, L, R)$
$\delta(q_3, C) = (q_3, Z, R)$
$\delta(q_3, D) = (q_3, M, R)$
$\delta(q_3, E) = (q_3, A, R)$
$\delta(q_3, F) = (q_3, N, R)$
$\delta(q_3, G) = (q_3, B, R)$
$\delta(q_3, H) = (q_3, O, R)$
$\delta(q_3, I) = (q_3, C, R)$
$\delta(q_3, J) = (q_3, P, R)$
$\delta(q_3, K) = (q_3, D, R)$
$\delta(q_3, L) = (q_3, Q, R)$
$\delta(q_3, M) = (q_3, E, R)$

$\delta(q_3, N) = (q_3, R, R)$
$\delta(q_3, \tilde{N}) = (q_3, F, R)$
$\delta(q_3, O) = (q_3, S, R)$
$\delta(q_3, P) = (q_3, G, R)$
$\delta(q_3, Q) = (q_3, T, R)$
$\delta(q_3, R) = (q_3, H, R)$
$\delta(q_3, S) = (q_3, U, R)$
$\delta(q_3, T) = (q_3, I, R)$
$\delta(q_3, U) = (q_3, V, R)$
$\delta(q_3, V) = (q_3, J, R)$
$\delta(q_3, W) = (q_3, W, R)$
$\delta(q_3, X) = (q_3, K, R)$
$\delta(q_3, Y) = (q_3, X, R)$
$\delta(q_3, Z) = (q_3, D, R)$

¿CÓMO FUNCIÓNA?

```
print("Bienvenido al cifrador por el metodo AFIN\n"
     "Para encriptar una cadena de texto por favor ingresela a contunuación: \n")
mensaje = input()
mensaje = mensaje.upper()
mensaje = "#"+ mensaje
try:
    print(d.validate_input(mensaje))
except Exception as e:
        print("Por favor ingrese una cadena de texto valida.\n")
```

```
Bienvenido al cifrador por el metodo AFIN
Para encriptar una cadena de texto por favor ingresela a contunuación:

Hola mundo
('q4', TMTape('-RHZE0BSDKH-'))
```

CONCLUSIÓN

- El uso de la maquina de Turing es un método viable para desarrollar el cifrado de afin.En el proceso de creación del proyecto nos dimos cuenta que haciendo uso de la maquina de turing también se pueden llevar a cabo otros métodos de cifrados como por ejemplo cifrado cesar, monomio-binomio, ROT13 y Atbash.

GRACIAS POR SU ATENCIÓN