Universidad Francisco Marroquín

Matemática Discreta

Freddy Arévalo García

Oscar Enrique Acuña Rodríguez

WS3

Yara Maldonado 20160038

Sergio García 20160267

Gabriel Estrada 20160021

a) Encryption FSM (Es igual de válida para Gödel(Extra), como para Fibonacci)

M = M(A, S, Z, S_0, *f, g*)

(1) A finite set A of input symbols.

α = {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}

β = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

ϕ = {!, “, #, $, %, &, /, (, |, =, ¡}

A = {α ,β , ϕ}

(2) A finite set S of “internal” states.

S = {S_0, S_1, S_2, S_3, S_4, S_5, S_6}

(3) A finite set Z of output symbols.

α = {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}

β = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

ϕ = {!, “, #, $, %, &, /, (, |, =, ¡}

Z = { α, β, ϕ}

(4) An initial state S_0 in S.

Initial state S_0

(5) A next-state function f from S × A into S.

$F(S_0, x\in\alpha) = S_1$, $F(S_1, x\in\alpha) = S_1$, $F(S_2, x\in\alpha) = S_2$, $F(S_3, x\in\alpha) = S_3$,
$F(S_4, x\in\alpha) = S_4$, $F(S_5, x\in\alpha) = S_6$, $F(S_6, x\in\alpha)$ = SINK

$F(S_0, x\in\beta) = S_0$, $F(S_1, x\in\beta) = S_2$, $F(S_2, x\in\beta) = S_2$, $F(S_3, x\in\beta) = S_4$,
$F(S_4, x\in\beta) = S_4$, $F(S_5, x\in\beta) = S_5$, $F(S_6, x\in\beta)$ = SINK

$F(S_0, x\in\phi) = S_0$, $F(S_1, x\in\phi) = S_1$, $F(S_2, x\in\phi) = S_3$, $F(S_3, x\in\phi) = S_3$,
$F(S_4, x\in\phi) = S_5$, $F(S_5, x\in\phi) = S_5$, $F(S_6, x\in\phi)$ = SINK

(6) An output function g from S × A into Z.

$G(S_0, x\in\alpha) = x\in\alpha$, $G(S_1, x\in\alpha)$ = SINK , $G(S_2, x\in\alpha)$ = SINK , $G(S_3, x\in\alpha)$ = SINK
,$G(S_4, x\in\alpha)$ = SINK, $G(S_5, x\in\alpha) = x\in\alpha$, $G(S_6, x\in\alpha)$ = SINK

$G(S_0, x\in\beta)$ = SINK , $G(S_1, x\in\beta) = x\in\beta$, $G(S_2, x\in\beta)$ = SINK , $G(S_3, x\in\beta) = x\in\beta$,
$G(S_4, x\in\beta)$ = SINK, $G(S_5, x\in\beta)$ = SINK , $G(S_6, x\in\beta)$ = SINK

$G(S_0, x \in \phi) = SINK$, $G(S_1, x \in \phi) = SINK$, $G(S_2, x \in \phi) = x \in \phi$, $G(S_3, x \in \phi) = SINK$, $G(S_4, x \in \phi) = x \in \phi$, $G(S_5, x \in \phi) = SINK$, $G(S_6, x \in \phi) = SINK$

b) Decryption FSM (Fibonacci)

M = M(A, S, Z, S_0, *f, g*)

(1) A finite set A of input symbols.

A = { X | ∀ X ∈ { 5918793878, 2.3675E+10, 5.3269E+10, 1.4797E+11, 3.78803E+11, 1.00028E+12, 2.61019E+12, 6.84213E+12, 1.79044E+13, 4.68828E+13, 1.22732E+14, 3.21325E+14, 8.41232E+14, 2.20238E+15, 5.76591E+15, 1.50953E+16, 3.95201E+16, 1.03465E+17, 2.70875E+17, 7.0916E+17, 1.8566E+18, 4.86065E+18, 1.27254E+19, 3.33154E+19, 8.72209E+19, 2.28347E+20, 5.97821E+20, 1.56512E+21, 4.09753E+21, 1.07275E+22, 2.80849E+22, 7.35271E+22, 1.92496E+23, 5.03962E+23, 1.31939E+24, 3.45421E+24, 9.04324E+24, 2.36755E+25, 6.19833E+25, 1.62274E+26, 4.2484E+26, 1.11224E+27, 2.91189E+27, 7.62344E+27, 1.99584E+28, 5.22518E+28, 1.36797E+29}}

(2) A finite set S of "internal" states.

S = {S_0, S_1, S_2, S_3, S_4, S_5, S_6}

(3) A finite set Z of output symbols.

Z = { X | ∀ X ∈ { 5918793878, 2.3675E+10, 5.3269E+10, 1.4797E+11, 3.78803E+11, 1.00028E+12, 2.61019E+12, 6.84213E+12, 1.79044E+13, 4.68828E+13, 1.22732E+14, 3.21325E+14, 8.41232E+14, 2.20238E+15, 5.76591E+15, 1.50953E+16, 3.95201E+16, 1.03465E+17, 2.70875E+17, 7.0916E+17, 1.8566E+18, 4.86065E+18, 1.27254E+19, 3.33154E+19, 8.72209E+19, 2.28347E+20, 5.97821E+20, 1.56512E+21, 4.09753E+21, 1.07275E+22, 2.80849E+22, 7.35271E+22, 1.92496E+23, 5.03962E+23, 1.31939E+24, 3.45421E+24, 9.04324E+24, 2.36755E+25, 6.19833E+25, 1.62274E+26, 4.2484E+26, 1.11224E+27, 2.91189E+27, 7.62344E+27, 1.99584E+28, 5.22518E+28, 1.36797E+29}}

(4) An initial state S_0 in S.

Initial state S_0

(5) A next-state function f from S × A into S.

$F(S_0, X \in A) = S_1$, $F(S_1, X \in A) = S_2$, $F(S_2, X \in A) = S_3$, $F(S_3, X \in A) = S_4$, $F(S_4, X \in A) = S_5$, $F(S_5, X \in A) = S_6$, $F(S_6, X \in A) = SINK$

(6) An output function g from S × A into Z.

$G(S_0, X \in A) = X \in A$, $G(S_1, X \in A) = X \in A$, $G(S_2, X \in A) = X \in A$,
$G(S_3, X \in A) = X \in A$, $G(S_4, X \in A) = X \in A$, $G(S_5, X \in A) = X \in A$,
$G(S_6, X \in A)$ = SINK

c.) Encryption function

α = {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}

β = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

ϕ = {!, “, #, $, %, &, /, (, |, =, ¡}

A = {α ,β , ϕ}

a. Gödel (Extra)

fe : X $\rightarrow$ Y

X = { X_1, X_2, X_3, X_4, X_5, X_6 | $\forall_i$, $X_i \in A$ }

Y = { Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 | $\forall_i$, $Y_i \in \{ \mathbb{N} \}$}

b. Fibonacci y F(x)= $\frac{(x*1703)^2}{0.00049}$

NOTA: Se uso Fibonacci para crear el índice, y después el número del índice se ingresó en la formula anteriormente mencionada.

fe : X $\rightarrow$ Y

X = { X_1, X_2, X_3, X_4, X_5, X_6 | $\forall_i$, $X_i \in$ {α ,β , ϕ}}

Y = { Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 | $\forall_i$, Yi ∈ { 5918793878, 2.3675E+10, 5.3269E+10, 1.4797E+11, 3.78803E+11, 1.00028E+12, 2.61019E+12, 6.84213E+12, 1.79044E+13, 4.68828E+13, 1.22732E+14, 3.21325E+14, 8.41232E+14, 2.20238E+15, 5.76591E+15, 1.50953E+16, 3.95201E+16, 1.03465E+17, 2.70875E+17, 7.0916E+17, 1.8566E+18, 4.86065E+18, 1.27254E+19, 3.33154E+19, 8.72209E+19, 2.28347E+20, 5.97821E+20, 1.56512E+21, 4.09753E+21, 1.07275E+22, 2.80849E+22, 7.35271E+22, 1.92496E+23, 5.03962E+23, 1.31939E+24, 3.45421E+24, 9.04324E+24, 2.36755E+25, 6.19833E+25, 1.62274E+26, 4.2484E+26, 1.11224E+27, 2.91189E+27, 7.62344E+27, 1.99584E+28, 5.22518E+28, 1.36797E+29}

d.) Decryption function

NOTA: En ambos casos, la función de "Decryption" no nos devuelve las letras como tal, sino que nos devuelve el índice, y ya con el índice, se puede ver que letra, signo, o número que es. Ver anexo para más detalles.

a. Gödel (Extra)

Fe : Y $\rightarrow$ X

Y = { Y1, Y2, Y3, Y4, Y5, Y6 | ∀i, Yi ∈ { ℕ }}

$X=\{X_1,X_2,X_3,X_4,X_5,X_6|\forall_i,X_i\in=\{\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47\}\}$

b. Fibonacci

NOTA: para pasar los valores encriptados al índice se usó la inversa de la función anteriormente mencionada la cual seria: $F'(x) = \frac{\sqrt{x*0.00049}}{1703}$

Fe : Y $\rightarrow$ X

Y = { Y1, Y2, Y3, Y4, Y5, Y6 | ∀i, Yi ∈ { 5918793878, 2.3675E+10, 5.3269E+10, 1.4797E+11, 3.78803E+11, 1.00028E+12, 2.61019E+12, 6.84213E+12, 1.79044E+13, 4.68828E+13, 1.22732E+14, 3.21325E+14, 8.41232E+14, 2.20238E+15, 5.76591E+15, 1.50953E+16, 3.95201E+16, 1.03465E+17, 2.70875E+17, 7.0916E+17, 1.8566E+18, 4.86065E+18, 1.27254E+19, 3.33154E+19, 8.72209E+19, 2.28347E+20, 5.97821E+20, 1.56512E+21, 4.09753E+21, 1.07275E+22, 2.80849E+22, 7.35271E+22, 1.92496E+23, 5.03962E+23, 1.31939E+24, 3.45421E+24, 9.04324E+24, 2.36755E+25, 6.19833E+25, 1.62274E+26, 4.2484E+26, 1.11224E+27, 2.91189E+27, 7.62344E+27, 1.99584E+28, 5.22518E+28, 1.36797E+29}

X = { X1, X2, X3, X4, X5, X6 |∀i , Xi ∈ { 1, 2 , 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393, 196418, 317811, 514229, 832040, 1346269, 2178309, 3524578, 5702887, 9227465, 14930352, 24157817, 39088169, 63245986, 102334155, 165580141, 267914296, 433494437, 701408733, 1134903170, 1836311903, 2971215073, 4807526976}

e. Step by Step explanation of a working sample, encryption and decryption functions

Fibonacci

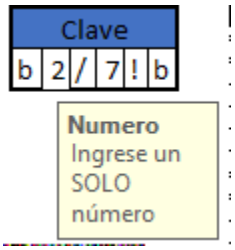
(1) Como primer paso, el programa a utilizar fue Excel. En el cual se hizo una secuencia de Fibonacci empezando en 1, para crear el índice.

Encryption	
Indice Fibonacci	Teclado
1	a
2	b
3	c
5	d
8	e
13	f
21	g
34	h
55	i
89	j
144	k
233	l
377	m
610	n
987	ñ
1597	o
2584	p
4181	q

(2) Seguido de eso al índice se le aplico la siguiente formula **F(x)**= $\frac{(x*1703)^2}{0.00049}$ con lo cual cada posible valor del teclado queda encriptado.

Encryption		
Indice Fibonacci	Teclado	Encriptado
1	a	5918793878
2	b	2.3675E+10
3	c	5.3269E+10
5	d	1.4797E+11
8	e	3.788E+11

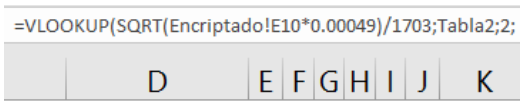
(3) Después le aplicamos nuestra FSM, para validar las entradas que se quieren encriptar, en este caso son solo 6 entradas, pero pusimos la restricción de que solo se puedan poner letras en la primera casilla, números en la segundo, símbolos en la tercera, números en la cuarta, símbolos en la quinta y finalmente letras en la sexta. Aplicamos una validación de celda para que se cumplieran estos requisitos.



(4) Después se aplica la función Vlookup para que busque el valor de cada casilla en la tabla anteriormente mostrada, y así lo encripte.

Encriptado					
23675175510	1565115332765240000000	291189394637382000000000000	1924964605737520000000	9043236121828950000000000	23675175510

(5) Seguido de esto, ya que tenemos el código encriptado, para hacer el proceso inverso y poder leerlo primero aplicamos al número encriptado la función inversa $F'(x) = \frac{\sqrt{x*0.00049}}{1703}$, y ya que después de esto obtenemos el número de Fibonacci que se usó para crear el índice, vamos al índice a buscar que significa cada valor y usamos la función Vlookup para agilizar el proceso.

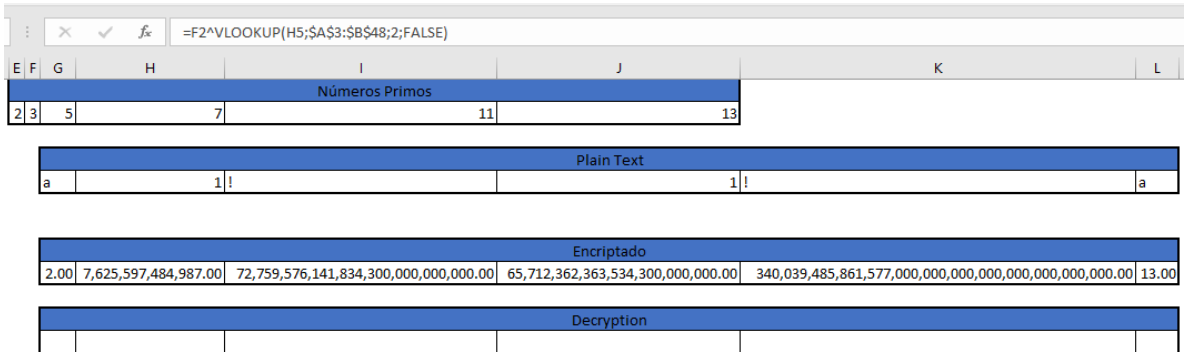


Clave					
b	2	/	7	!	b

Gödel

(1) Para aplicar Gödel se cambia un poco el proceso, el índice ahora solo va de 1:47, se usan solo los primeros 6 números primos, que corresponden a las 6 casillas que se deben de llenar. Se sigue aplicando la validación de celda, para que la FSM siga siendo funcional en la encripción.

(2) Para encriptar se toma el valor de la casilla y se busca en la tabla que se creó el índice correspondiente a dicho valor, y después el número primo correspondiente se eleva a la potencia que el índice indique.



(3) Después, ya con todos los números primos elevados a la respectiva potencia, se multiplican entre ellos y se obtiene le número de Gödel. Y se termina el proceso de encriptar el código.

Numero de Gödel
3223397146164820000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(4) La lógica para lograr descomponer un número de Gödel reside en empezar a dividirlo por el primer número primero. Ósea 2. Y seguir dividiéndolo hasta que en la división ya quedé un residuo. Si la división ejecutada retorna un residuo o un número con decimal, entonces ahí se deja de dividir. Y se divide el número ahora dentro del siguiente número primo hasta que ya no se pueda dividir. Entonces contamos cuantas veces se pudo dividir dentro de cada número. Por el ejemplo si 2 se pudo usar 5 veces, entonces 2 se elevó a la 5 potencia, y ese 5 sería el número que buscaríamos en nuestro índice para decodificar el número de Gödel. Y así con las 6 casillas, lo que conlleva a hacer la división con los 6 números primos para lograr decodificar el número de Gödel.

```
> library(gmp)

Attaching package: ‘gmp’

The following objects are masked from ‘packa

    %*%, apply, crossprod, matrix, tcrosspro

> factorize(270270)
Big Integer ('bigz') object of length 8:
[1] 2  3  3  3  5  7  11 13
>
```

En este ejemplo, según nuestro índice entonces el mensaje oculta seria “acaaaa” contando el número de veces que se elevó cada primo, nos damos cuenta de que solo 3 se elevó 3 veces, por lo que nuestro índice nos indica que 3 = c, y 1=a, que fue en todos los demás casos que solo se elevó el número primo una vez.

Algoritmo en Python Determina divisibilidad del número de Gödel, almacena el valor de la variable y repite el proceso hasta que ya no sea divisible.

```python
Index_List = [(1,'a'),(2,'b'),(3,'c'),(4,'d'),(5,'e'),(6,'f'),(7,'g'),(8,'h'),(9,'i'),(10,'j'),
Index_Dict = dict(Index_List)
Prime_List = [2,3,5,7,11,13]

def Determine_Divisibility(number):
    factors = []
    for i in Prime_List:
        result = number % i
        while result == 0 :
            factors.append(i)
            number = number/i
            result = number % i
    return factors
```

ANEXO

Índice usado para Gödel

Encryption	
Teclado	#
a	1
b	2
c	3
d	4
e	5
f	6
g	7
h	8
i	9
j	10
k	11
l	12
m	13
n	14
o	16
p	17
q	18
r	19
s	20
t	21
u	22
v	23
x	24
y	25
z	26
1	27
2	28
3	29
4	30
5	31
6	32
7	33
8	34
9	35
0	36
!	37
"	38
#	39
$	40
%	41
&	42
/	43
(	44
)	45
=	46
¡	47

Índice usado para Fibonacci

Encryption		
Indice Fibonacci	Teclado	Encriptado
1	a	5918793878
2	b	2.3675E+10
3	c	5.3269E+10
5	d	1.4797E+11
8	e	3.788E+11
13	f	1.0003E+12
21	g	2.6102E+12
34	h	6.8421E+12
55	i	1.7904E+13
89	j	4.6883E+13
144	k	1.2273E+14
233	l	3.2133E+14
377	m	8.4123E+14
610	n	2.2024E+15
987	ñ	5.7659E+15
1597	o	1.5095E+16
2584	p	3.952E+16
4181	q	1.0347E+17
6765	r	2.7087E+17
10946	s	7.0916E+17
17711	t	1.8566E+18
28657	u	4.8607E+18
46368	v	1.2725E+19
75025	x	3.3315E+19
121393	y	8.7221E+19
196418	z	2.2835E+20
317811	1	5.9782E+20
514229	2	1.5651E+21
832040	3	4.0975E+21
1346269	4	1.0727E+22
2178309	5	2.8085E+22
3524578	6	7.3527E+22
5702887	7	1.925E+23
9227465	8	5.0396E+23
14930352	9	1.3194E+24
24157817	0	3.4542E+24
39088169	!	9.0432E+24
63245986	"	2.3675E+25
102334155	#	6.1983E+25
165580141	$	1.6227E+26
267914296	%	4.2484E+26
433494437	&	1.1122E+27
701408733	/	2.9119E+27
1134903170	(	7.6234E+27
1836311903	)	1.9958E+28
2971215073	=	5.2252E+28
4807526976	¡	1.368E+29