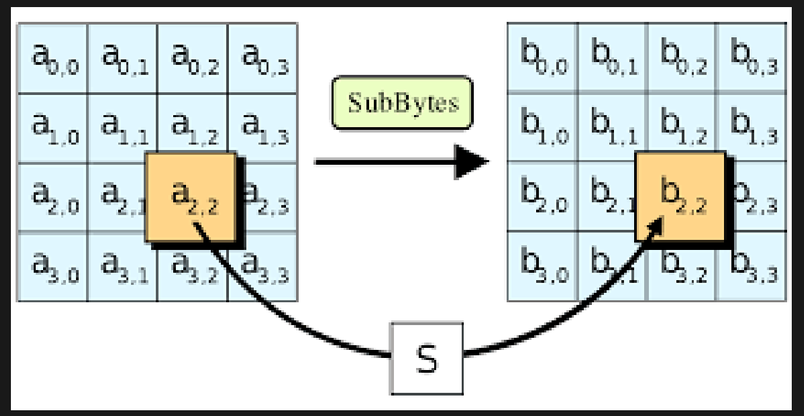
SIMULACIÓN Y ESTUDIO DEL ALGORITMO DE ENCRIPTACIÓN AES

~Gian Sebastián Mier Bello - 2210073
~Luis Sebastián Mora Cañas - 2211554
~Jesús David Ramírez Celis - 2211593

Universidad Industrial de Santander



Resumen

Se diseñó un autómata capaz de encriptar palabras ajustado al algoritmo AES (Rijndael).

Introducción

El autómata recibe palabras en el sistema decimal, luego las convierte a hexadecimal y las devuelve encriptadas en AES.

Restricciones

Se admiten los caracteres ASCII imprimibles. Además, solo se tiene en cuenta desde el 20 hasta el 7F en hexadecimal.

Conceptos utilizados

Se utilizó principalmente el concepto de máquina de Turing.

Estado del arte

Se encontró similitud con tres proyectos.

(link) 2019-2

2019-2 (link)

(link) 2020-2

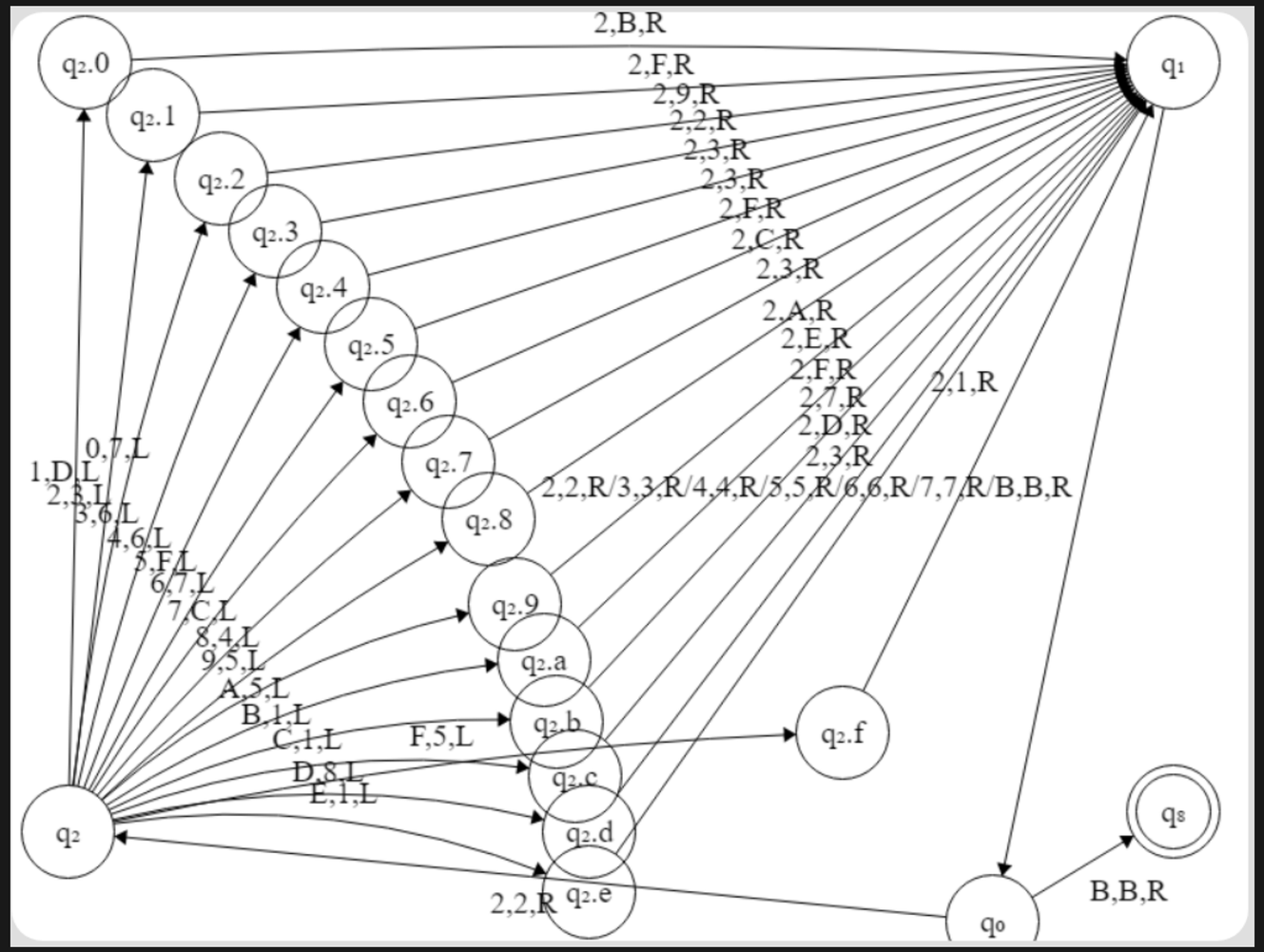
Método propuesto

Caracteres ASCII imprimibles

32	espacio	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

		Y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Diagrama de transiciones (simplificado)



MT = (q0, q1, q2, q3, q4, q5, q6, q7, q8, q2.0... q2.e, q3.0... q3.e, q4.0... q4.e, q5.0... q5.e, q6.0... q6.e,q7.0...q7.e, (q0), (q8), (0,1,2,3,4,5,6,7,8,9,A,B, C,D,E), (.))

Conclusiones

Se evidencio el nivel de capacidad de la máquina de Turing a la hora de procesar caracteres y transformar el resultado segun la operación deseada.

Pero también la limitación a nivel general de los automatas y lenguajes a la hora de realizar operaciones un poco mas complejas.

GRACIAS POR SU ATENCIÓN