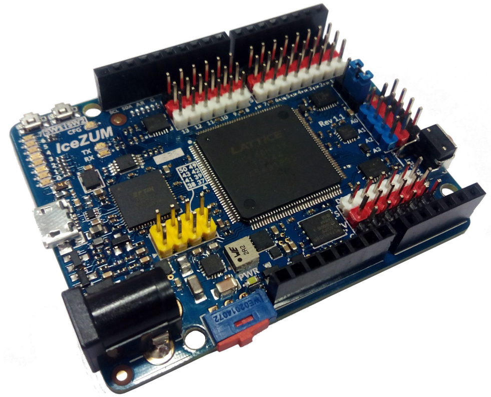
The enigma project

FPGA WARS



Creating an Enigma Machine inside an Open Source FGPA

Julián Caro Linares

jcarolinares@gmail.com
@jcarolinares

Cryptography

Greek kryptos “hidden” + graphia “to write”

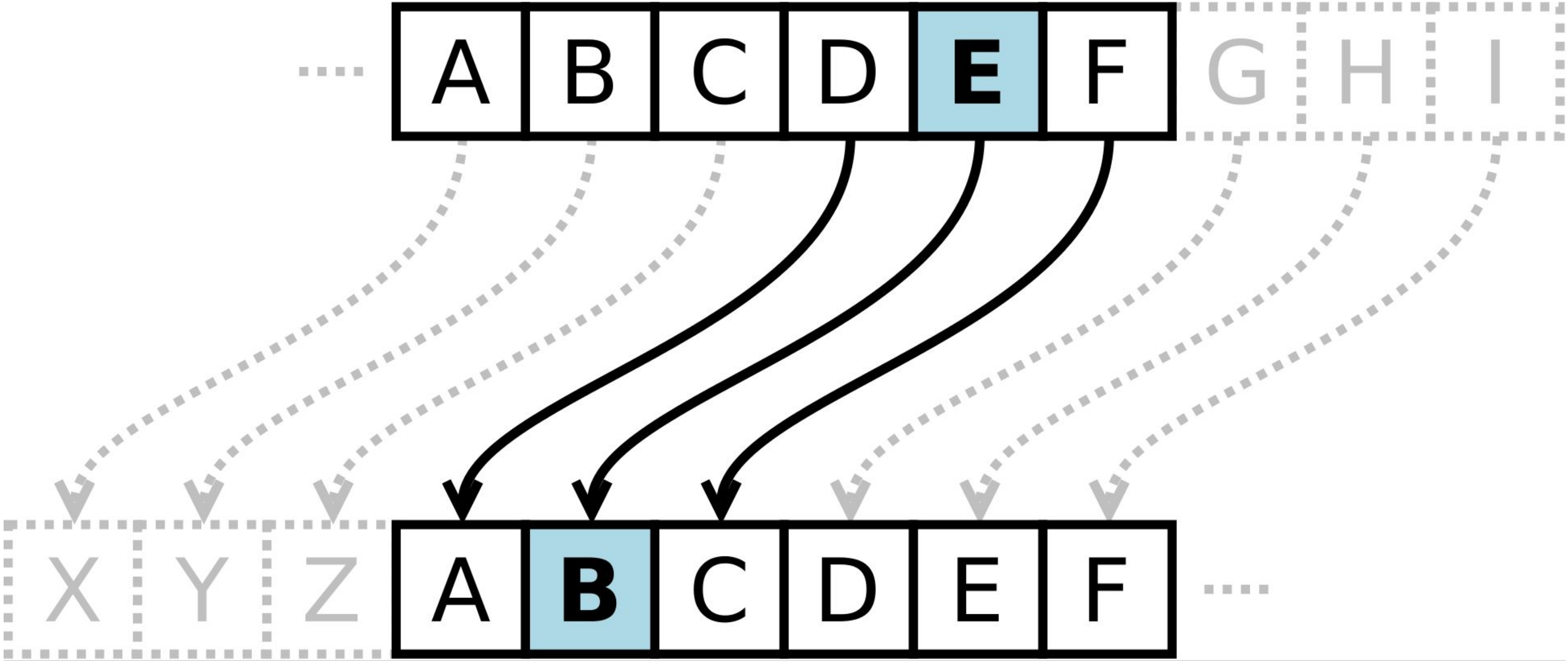
“A secret message”

WHEN WE WERE JUST CHILDS...

- **Hidden messages with family and friends**
- **Secret languages**
- **Invisible ink**
- **Invisible friends**

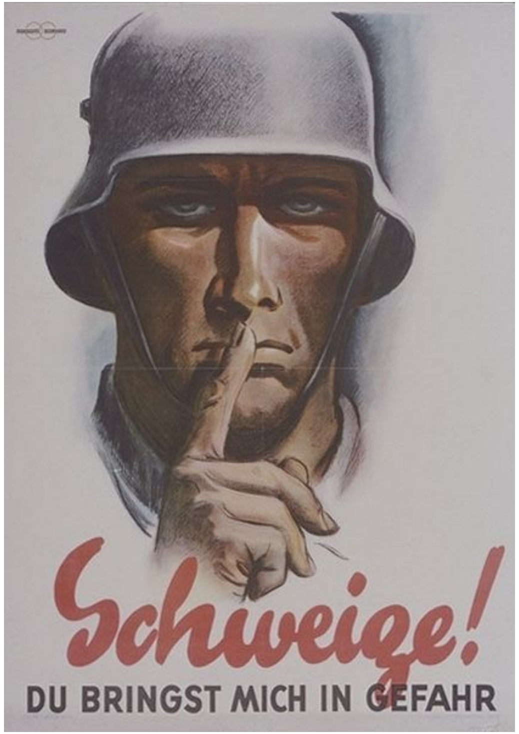
Humans need secrets, because they have feelings that can be harmed, but need to be said

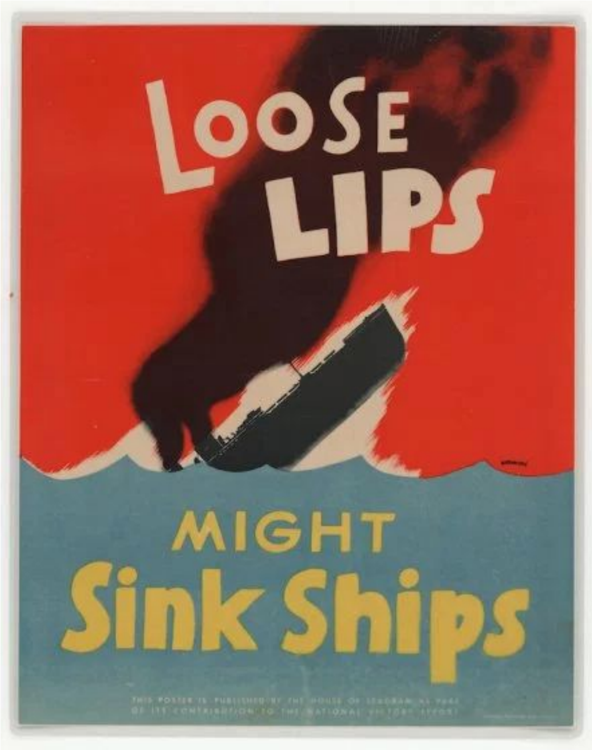
The Caesar Cipher

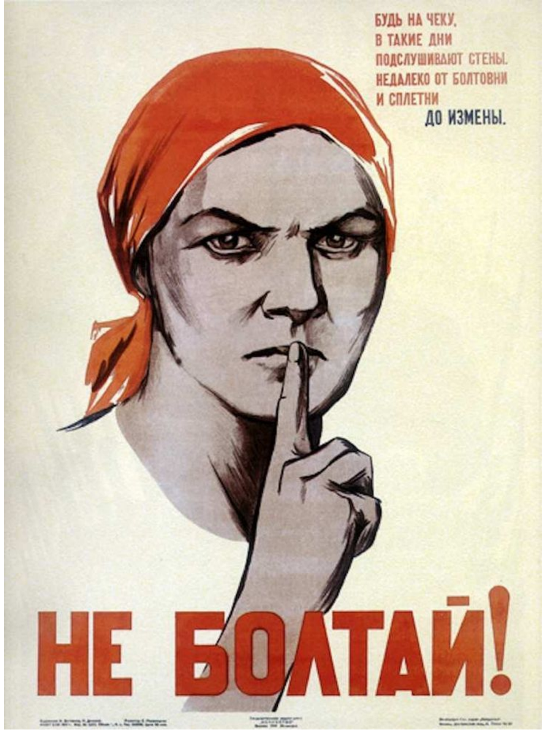


INFORMATION IS POWER

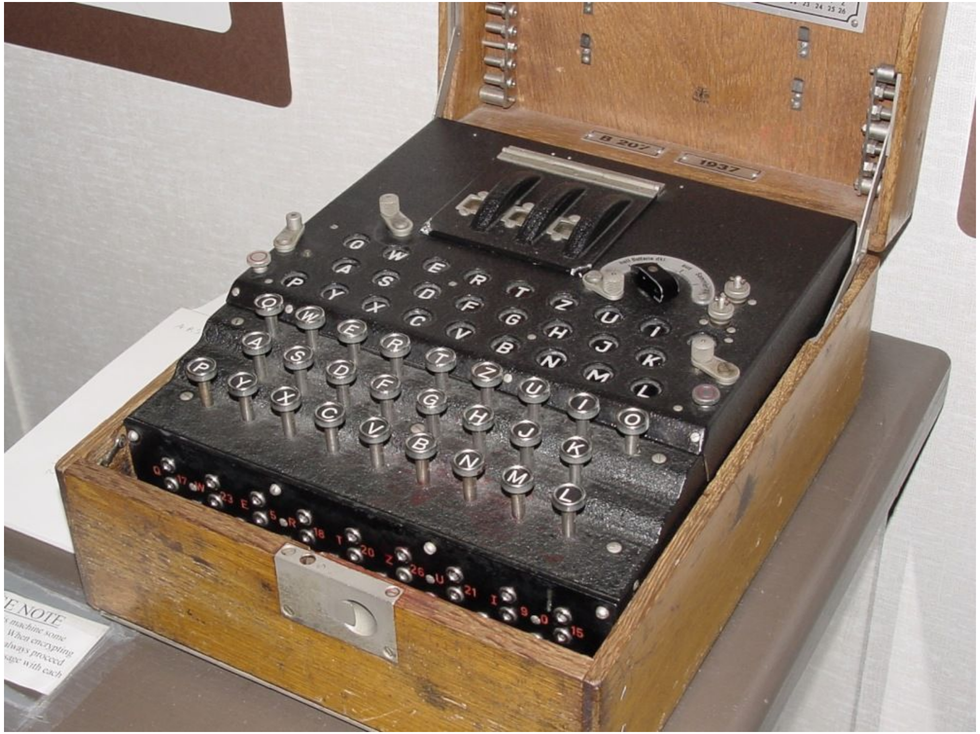
World War II


Schweige!
DU BRINGST MICH IN GEFAHR

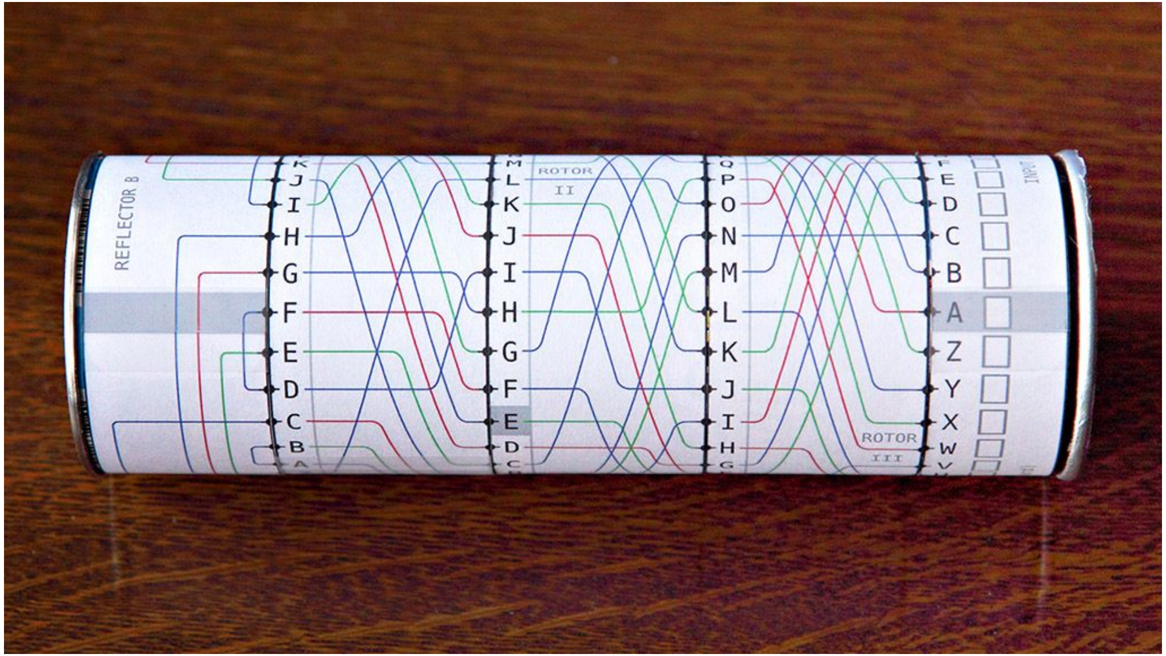

LOOSE
LIPS
MIGHT
Sink Ships
THIS POSTER IS PUBLISHED BY THE HOUSE OF SEAGRAM AS PART
OF ITS CONTRIBUTION TO THE NATIONAL VICTORY EFFORT


БУДЬ НА ЧЕКУ,
В ТАКИЕ ДНИ
ПОДСЛУШИВАЮТ СТЕНЫ.
НЕДАЛЕКО ОТ БОЛТОВНИ
И СПЛЕТНИ
ДО ИЗМЕНЫ.
НЕ БОЛТАЙ!

The Enigma Machine



LET'S WRITE "HELLO"



NAZIS IMPROVED ENIGMA

- Additional rotors for the Nazi’s Marine Army
- Plugboard

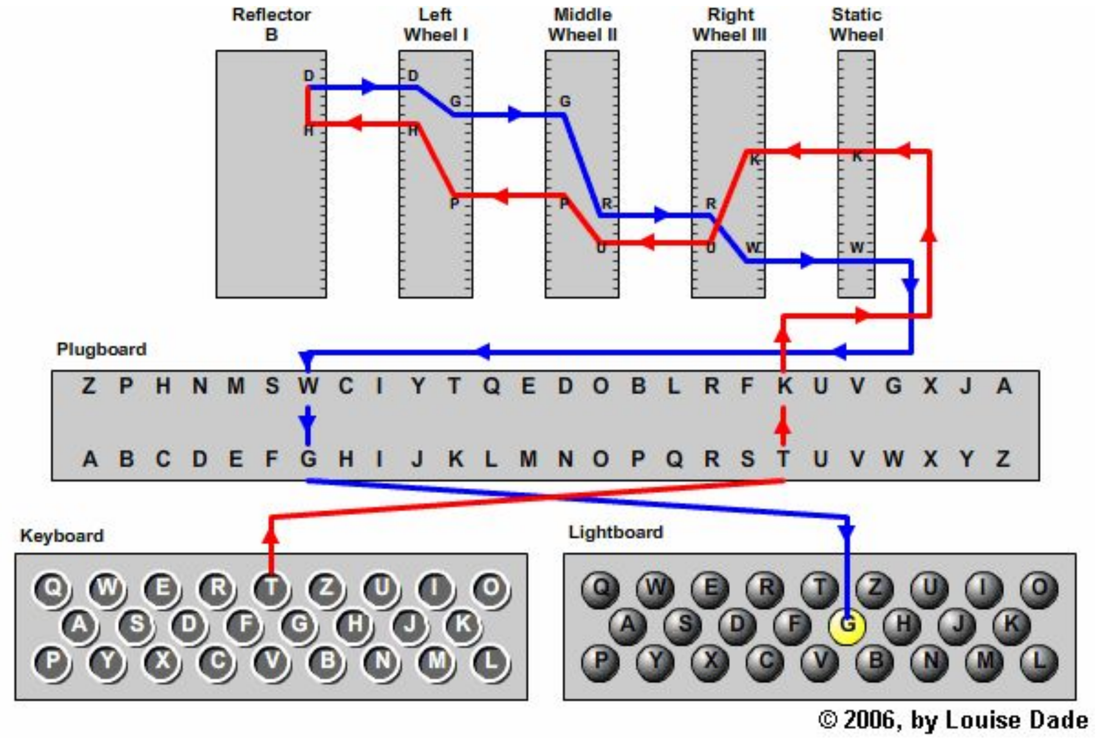
Three rotors -> 26 × 26 × 26 = 17,576 combinations.

17,576 by six possible wheel orders gives 105,456 combinations

Plus a fourth rotor and a plugboard the number of combinations are:

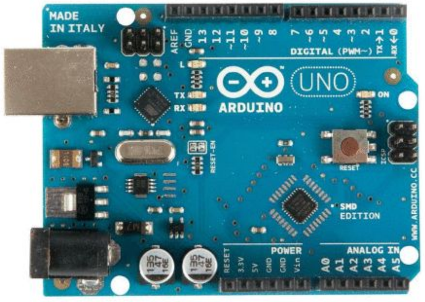
3×10^{114} (~380 bits)

NAZIS IMPROVED ENIGMA



A letter is never encrypted as itself

STOP!

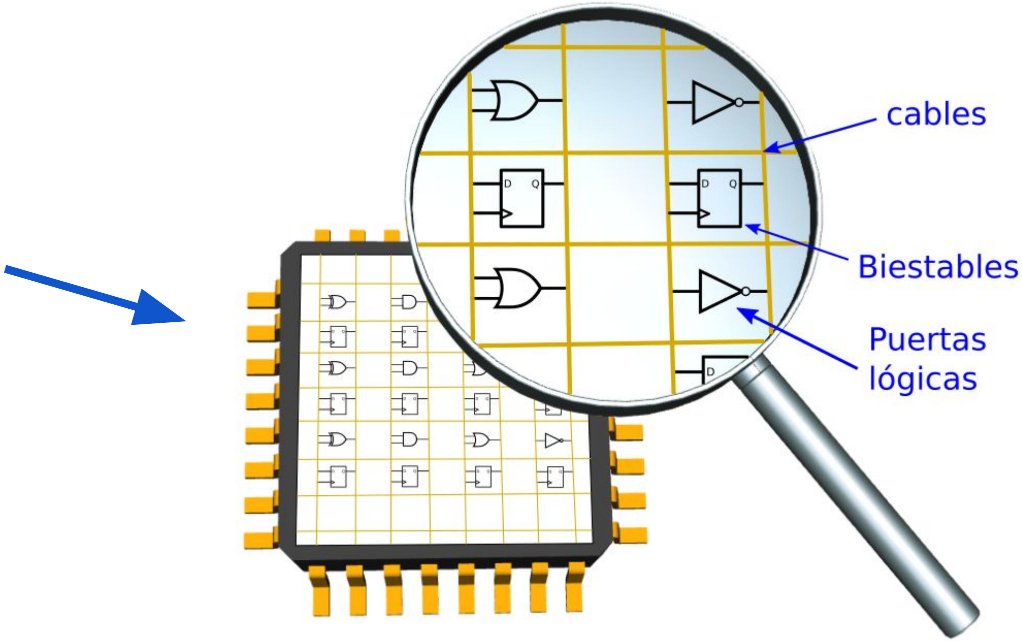


INSTRUCCIÓN 1

INSTRUCCIÓN 2

INSTRUCCIÓN 3

INSTRUCCIÓN 4



Field Programmable Gate Array

WHAT IS AN FPGA?

Juan Gonzalez Gomez:
https://github.com/Obijuan/digital-electronics-with-open-FPGAs-tutorial

FPGAS ARE...

- We are creating REAL circuits inside the FPGA. NO PROGRAMS HERE. JUST HARDWARE.

- Each circuit is INDEPENDENT and all the circuits work in PARALLEL, just like real circuits because THEY ARE REAL.

- If the circuit is well designed, it’s faster than its equivalent implementation in software. If not, probably it’s also faster.

- You can make new circuits without the need of manufacture again the new circuit all the times that you want, in a matter of seconds.

OPEN SOURCE FPGAS

Clifford Wolf
“The fucking master of the universe”

Project IceStorm

FPGA WARS

THE ENIGMA INSIDE AN FPGA

Setup of icestudio and ScriptCommunicator

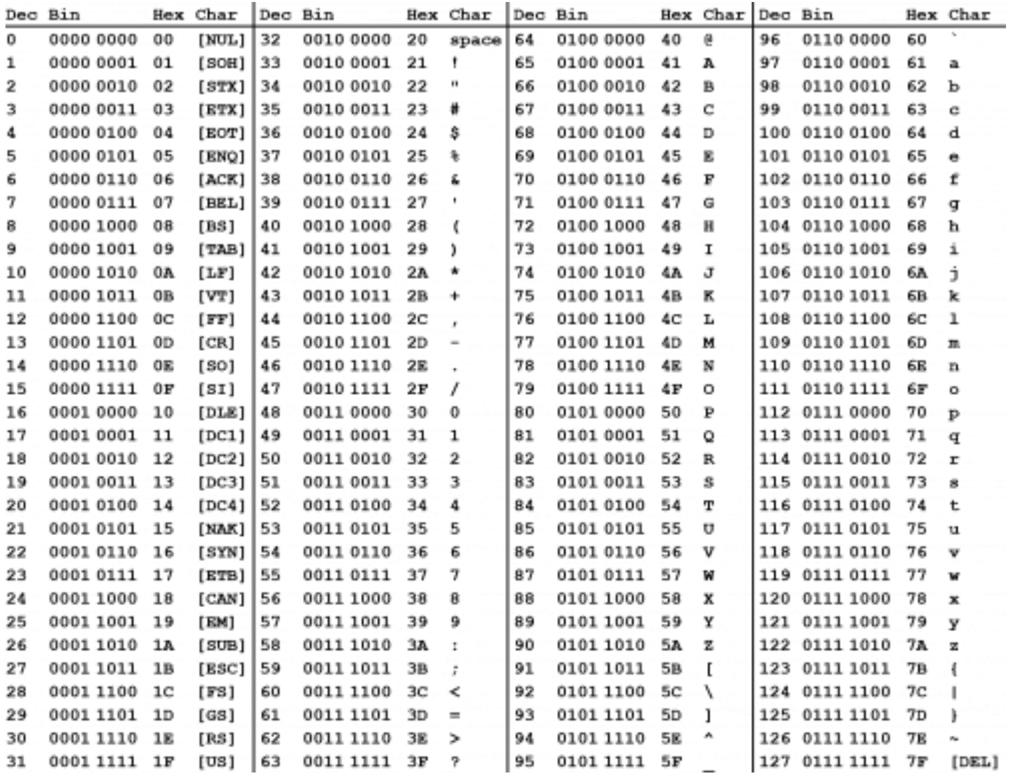
https://github.com/FPGAwars/icestudio

https://github.com/szieke/ScriptCommunicator_serial-terminal

https://github.com/FPGAwars/Collection-Jedi

LET'S PLAY WITH ICESTUDIO

WHAT IS ASCII

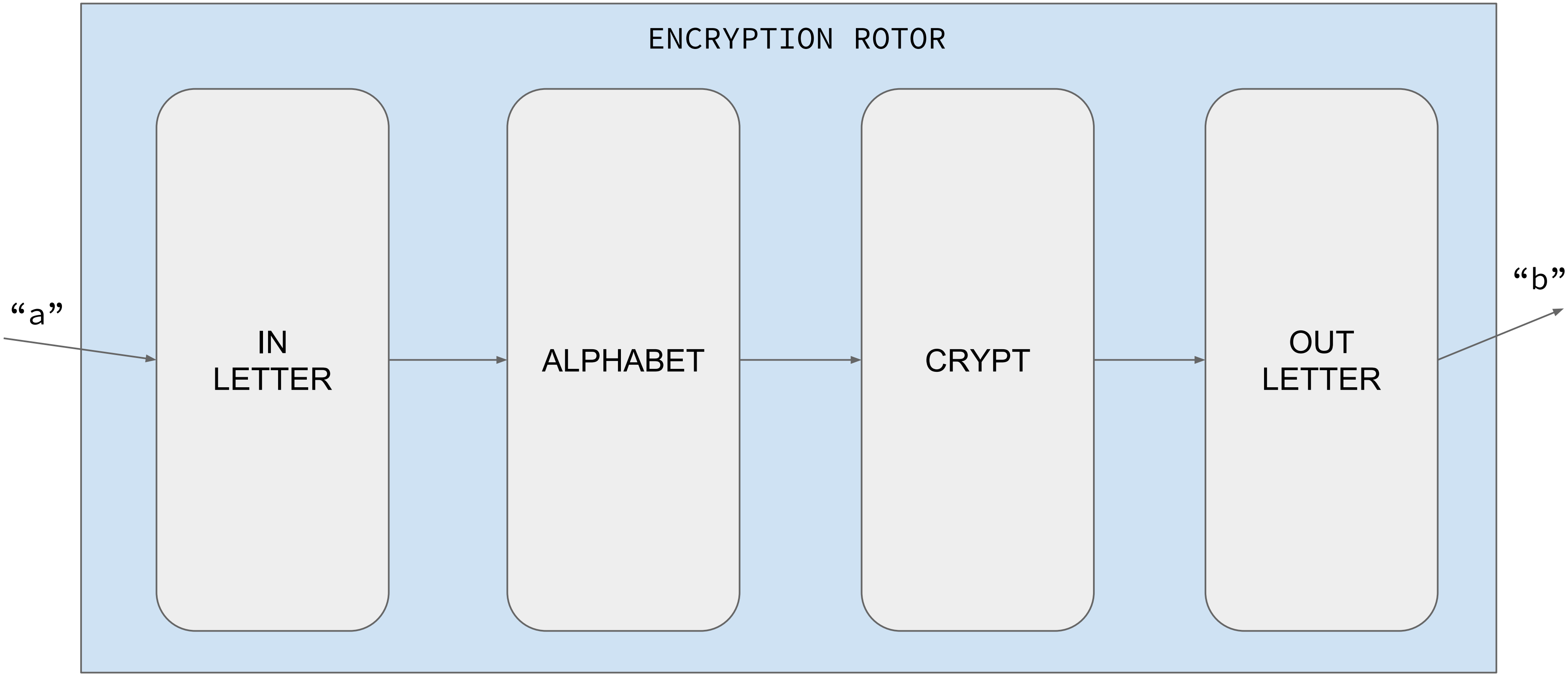


Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char
0	0000 0000	00	[NUL]	32	0010 0000	20	space	64	0100 0000	40	@	96	0110 0000	60	`
1	0000 0001	01	[SOH]	33	0010 0001	21	!	65	0100 0001	41	A	97	0110 0001	61	a
2	0000 0010	02	[STX]	34	0010 0010	22	"	66	0100 0010	42	B	98	0110 0010	62	b
3	0000 0011	03	[ETX]	35	0010 0011	23	#	67	0100 0011	43	C	99	0110 0011	63	c
4	0000 0100	04	[EOT]	36	0010 0100	24	$	68	0100 0100	44	D	100	0110 0100	64	d
5	0000 0101	05	[ENQ]	37	0010 0101	25	%	69	0100 0101	45	E	101	0110 0101	65	e
6	0000 0110	06	[ACK]	38	0010 0110	26	&	70	0100 0110	46	F	102	0110 0110	66	f
7	0000 0111	07	[BEL]	39	0010 0111	27	'	71	0100 0111	47	G	103	0110 0111	67	g
8	0000 1000	08	[BS]	40	0010 1000	28	(	72	0100 1000	48	H	104	0110 1000	68	h
9	0000 1001	09	[TAB]	41	0010 1001	29	)	73	0100 1001	49	I	105	0110 1001	69	i
10	0000 1010	0A	[LF]	42	0010 1010	2A	*	74	0100 1010	4A	J	106	0110 1010	6A	j
11	0000 1011	0B	[VT]	43	0010 1011	2B	+	75	0100 1011	4B	K	107	0110 1011	6B	k
12	0000 1100	0C	[FF]	44	0010 1100	2C	,	76	0100 1100	4C	L	108	0110 1100	6C	l
13	0000 1101	0D	[CR]	45	0010 1101	2D	-	77	0100 1101	4D	M	109	0110 1101	6D	m
14	0000 1110	0E	[SO]	46	0010 1110	2E	.	78	0100 1110	4E	N	110	0110 1110	6E	n
15	0000 1111	0F	[SI]	47	0010 1111	2F	/	79	0100 1111	4F	O	111	0110 1111	6F	o
16	0001 0000	10	[DLE]	48	0011 0000	30	0	80	0101 0000	50	P	112	0111 0000	70	p
17	0001 0001	11	[DC1]	49	0011 0001	31	1	81	0101 0001	51	Q	113	0111 0001	71	q
18	0001 0010	12	[DC2]	50	0011 0010	32	2	82	0101 0010	52	R	114	0111 0010	72	r
19	0001 0011	13	[DC3]	51	0011 0011	33	3	83	0101 0011	53	S	115	0111 0011	73	s
20	0001 0100	14	[DC4]	52	0011 0100	34	4	84	0101 0100	54	T	116	0111 0100	74	t
21	0001 0101	15	[NAK]	53	0011 0101	35	5	85	0101 0101	55	U	117	0111 0101	75	u
22	0001 0110	16	[SYN]	54	0011 0110	36	6	86	0101 0110	56	V	118	0111 0110	76	v
23	0001 0111	17	[ETB]	55	0011 0111	37	7	87	0101 0111	57	W	119	0111 0111	77	w
24	0001 1000	18	[CAN]	56	0011 1000	38	8	88	0101 1000	58	X	120	0111 1000	78	x
25	0001 1001	19	[EM]	57	0011 1001	39	9	89	0101 1001	59	Y	121	0111 1001	79	y
26	0001 1010	1A	[SUB]	58	0011 1010	3A	:	90	0101 1010	5A	Z	122	0111 1010	7A	z
27	0001 1011	1B	[ESC]	59	0011 1011	3B	;	91	0101 1011	5B	[	123	0111 1011	7B	{
28	0001 1100	1C	[FS]	60	0011 1100	3C	<	92	0101 1100	5C	\	124	0111 1100	7C	|
29	0001 1101	1D	[GS]	61	0011 1101	3D	=	93	0101 1101	5D	]	125	0111 1101	7D	}
30	0001 1110	1E	[RS]	62	0011 1110	3E	>	94	0101 1110	5E	^	126	0111 1110	7E	~
31	0001 1111	1F	[US]	63	0011 1111	3F	?	95	0101 1111	5F	_	127	0111 1111	7F	[DEL]

CASE SENSITIVE

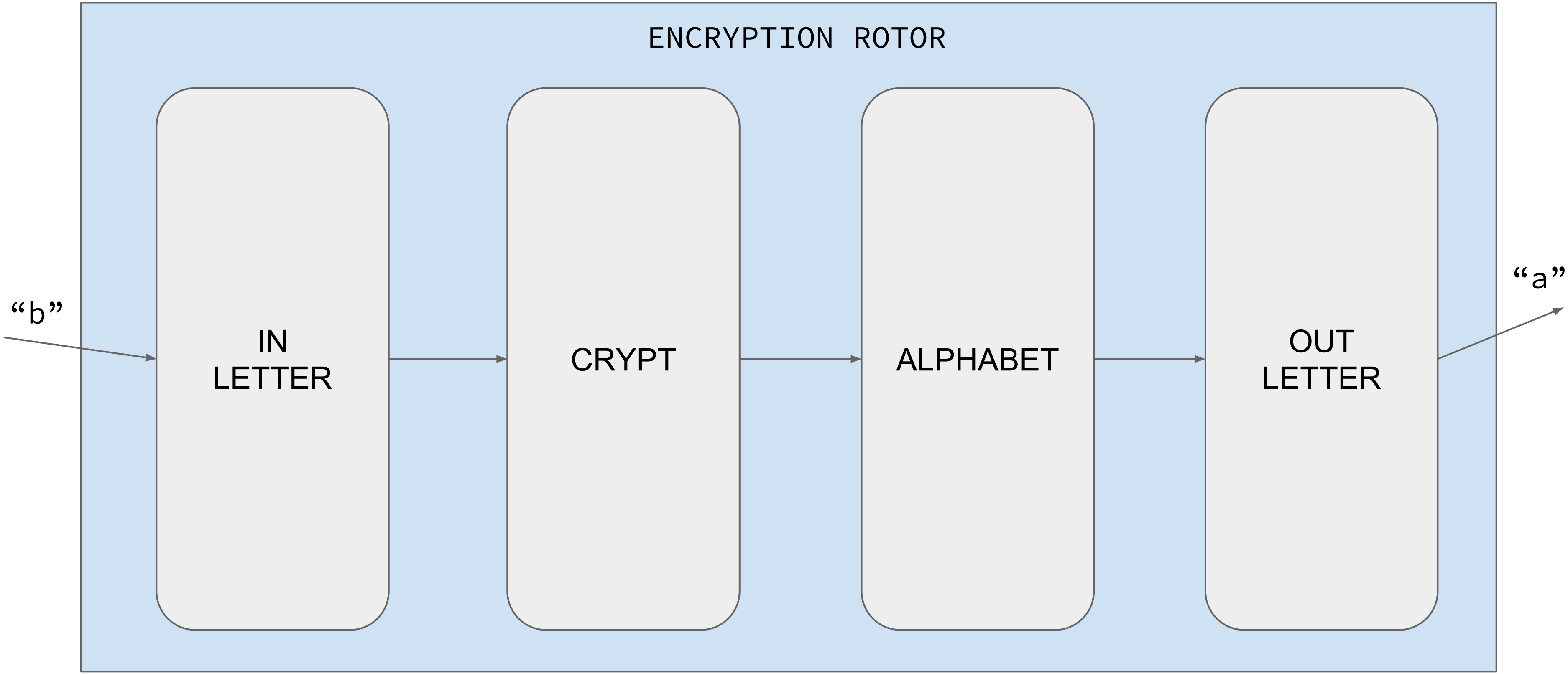
VERILOG: DESCRIBING HARDWARE

THE CAESAR CIRCUIT



Alphabet and crypt change position depending of the Encryption/Decryption mode

THE CAESAR CIRCUIT



Alphabet and crypt change position depending of the Encryption/Decryption mode

OUR FIRST ENIGMA WITH ONE ROTOR

ENIGMA WITH THREE MOTORS

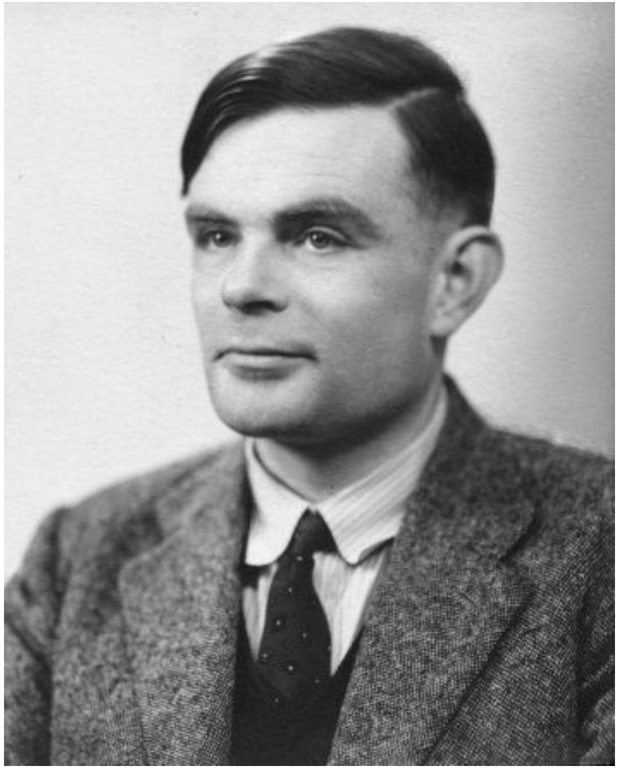
THERE'S MORE...

ALAN TURING

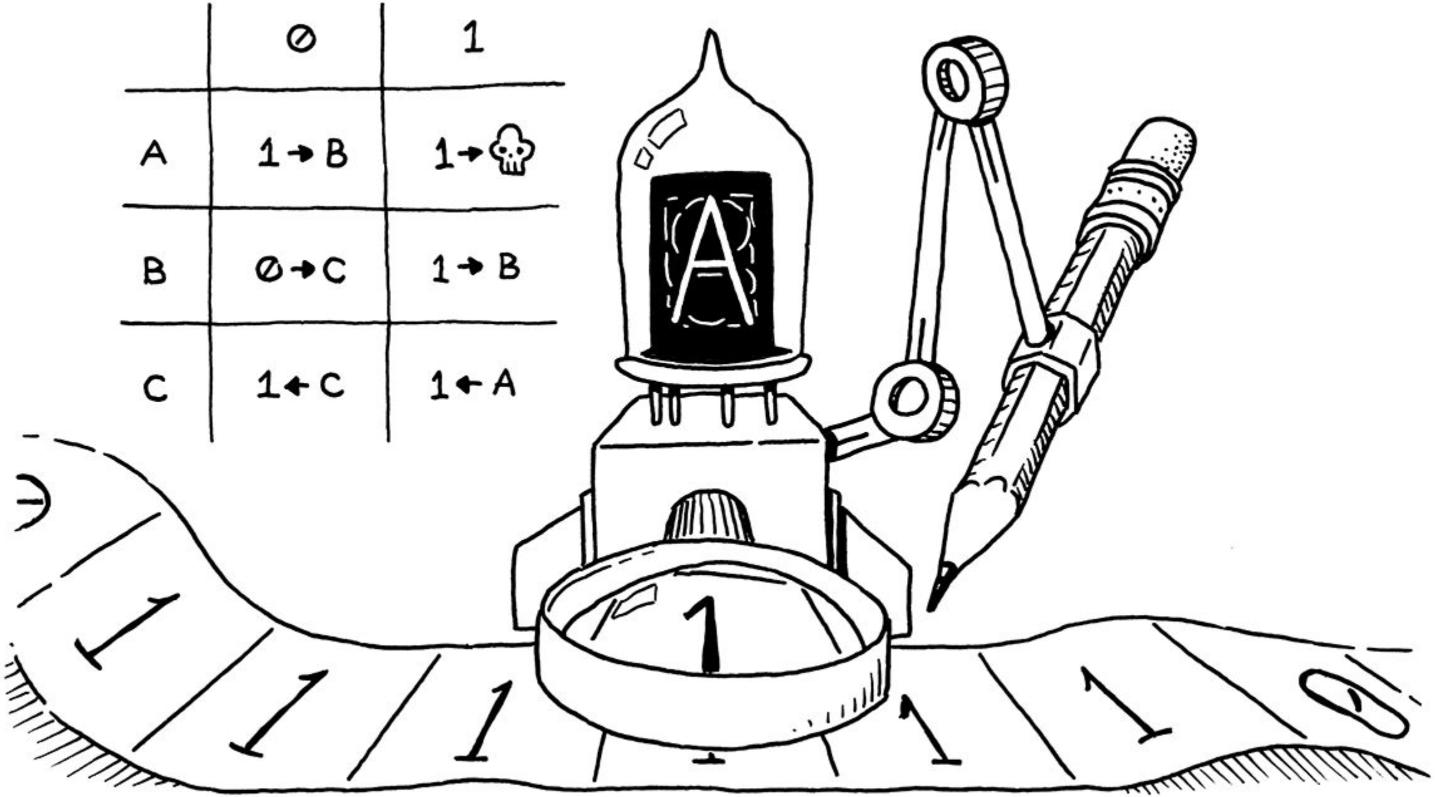
- He demonstrates that “The Entscheidungsproblem (decision problem)” cannot be resolve.

- One of the founders of the Science of computation. He creates “The Turing Machine”. One of the first theoretical general purpose computer.

- He broke the encryption of “The Enigma Machine” thanks to his talent and vision. He saves (and provoke) thousands of lives and reduce the WWII in more than two years.



THE TURING MACHINE

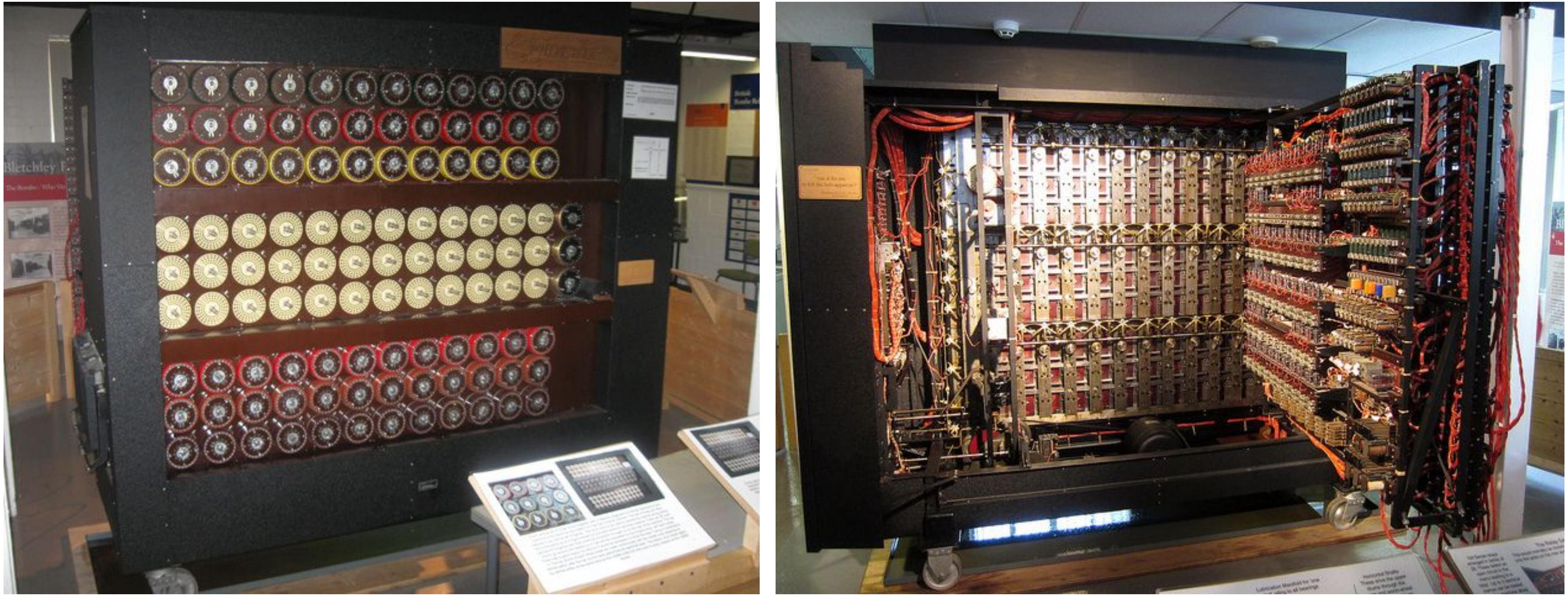


	Ø	1
A	1 → B	1 → ☠
B	Ø → C	1 → B
C	1 ← C	1 ← A

BLETCHEY PARK

CROWN COPYRIGHT, USED WITH KIND PERMISSION, DIRECTOR GCHQ

"THE BOMB"



Equivalent to 36 Enigma machines of three rotors

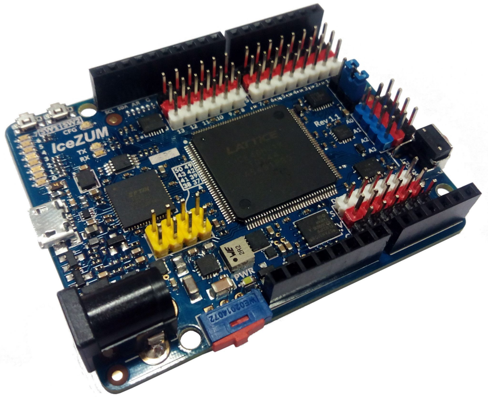
First version created by the Polish mathematician Marian Rejewski

ALAN TURING

8 June 1954

The enigma project

FPGA WARS



Creating an Enigma Machine inside an Open Source FGPA

Julián Caro Linares

jcarolinares@gmail.com
@jcarolinares