

Soluție Provocare-Decriptare



Provocare:

dpplo6++renpqwh)wywzaiu*nk+Ynulpk+aq*ljc

De unde să începem?

Provocare

dpplo6++renpqwh)wywzaiu*nk+Ynulpk+aq*ljc

100-44 BC

🕒 100-44 BC



Rezultate căutare



Wikipedia

https://ro.wikipedia.org/wiki/Lulius_Cezar ⋮

Lulius Cezar ✓

Cezar a ieșit învingător într-un război civil, devenind dictator al lumii romane, și a inițiat o vastă acțiune de reformare a societății romane și a guvernării ...



Wikipedia

https://en.wikipedia.org/wiki/Julius_Caesar · Traducerea acestei pagini ⋮

Julius Caesar ✓


Gaius Julius Caesar (12 July 100 **BC** – 15 March 44 **BC**) was a Roman general and statesman. A member of the First Triumvirate, Caesar led the Roman armies in ...



Cifru lui Cezar sau Cifrul cu deplasare

Cifrul lui Cezar

Acesta constă în deplasarea fiecărui caracter cu un număr N de caractere mai la dreapta dintr-un alfabet specificat (abcdefghijklmnopqrstuvwxyz).

 <https://cryptii.com/pipes/caesar-cipher>

Site cu un code translator

Code Translator/Decryptor

VIEW **Ciphertext** ▾

dpplo6++renpqwh)wywzaiu*nk+Ynulpk+aq*ljc

ENCODE **DECODE**

Caesar cipher ▾

SHIFT **22 a→w** +

ALPHABET
abcdefghijklmnopqrstuvwxyz

CASE STRATEGY: **Maintain case** ▾ FOREIGN CHARS: **Include Ignore**

→ Decoded 40 chars

VIEW **Plaintext** ▾

https6++virtual)academy*ro+Crypto+eu*png

Am incrementat pe rand numarul de “shiftări”, până am ajuns la numarul **22**. Unde am văzut ca mesajul decriptat are o forma rezonabilă.

Decriptarea caracterelor din afara alfabetului

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	\$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	+	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	,	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	;	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	=	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

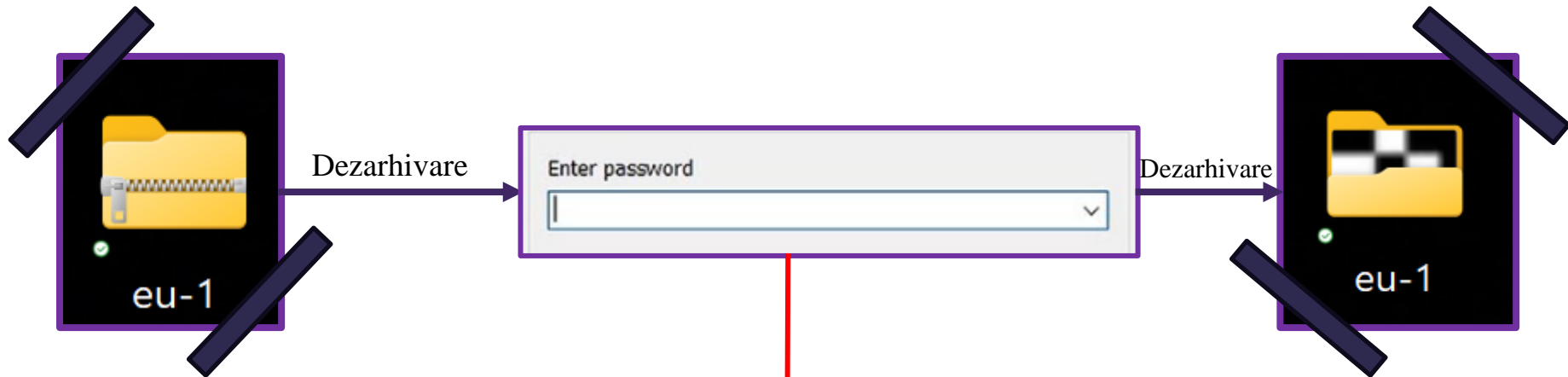
Observăm că fiecare caracter nemodificat, “shiftat” (incrementat) cu 4 în tabelul ASCII reprezintă câte un caracter valid dintr-o adresă URL (:, /, ,, -).

<https://virtual-academy.ro/Crypto/eu.png>

Ce se afla la acel link?

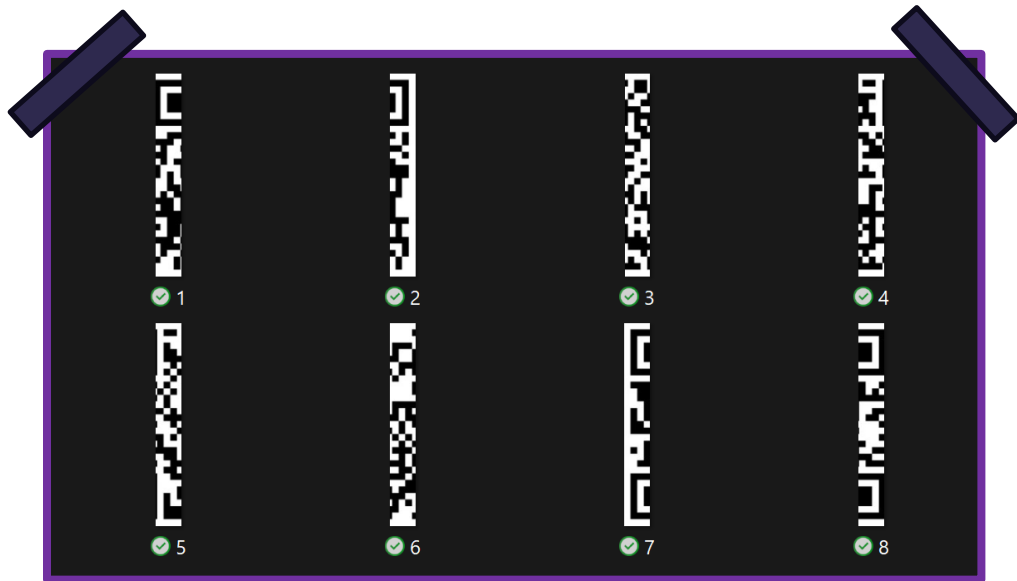


Arhiva descărcată



După câteva încercări eșuate (și puțin john the ripper), ne-a atras atenția numele arhivei “**eu-1**”, și ne-am gândit la numele domnului profesor care a lansat provocarea: **Dorin Iordache** → **doriniordache** (eu este scris cu lowercase), care era defapt și parola arhivei.

Interiorul folderului

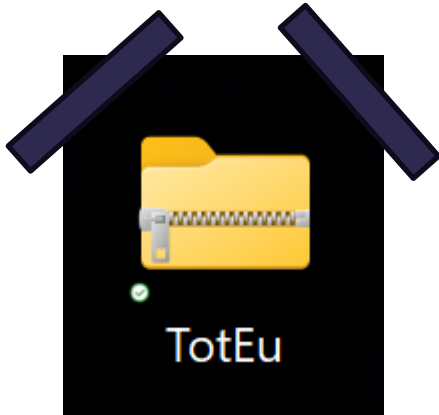


În interior am găsit 8 bucăți tăiate și dezaranjate dintr-un cod QR. Am folosit Paint-ul pentru a da insert la imagini și pentru a le reordona într-o singură imagine cu un cod QR valid.

Al doilea cod QR



A doua arhivă descărcată



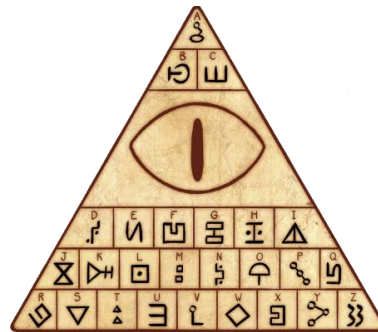
Bazându-ne tot pe numele arhivei și observând că aceasta are formatul **Capitalize Each Word**, ne-am gândit că noua parolă se referă tot la numele domnului profesor, doar că în formatul menționat mai sus → **DorinIordache**

Interiorul celei de-a doua arhive



Alfabetul folosit în cărțile din desen.

Referință la desenul animat Gravity Falls



Decriptare text in limbajul lui Bill Cipher

După ce am luat simbol cu simbol si l-am tradus cu ajutorul dicționarului din piramida (Bill Cipher) de pe slide-ul anterior, am determinat mesajul ascuns.



TRIMITE EMAIL CATRE DORIN IORDACHE CU SUBIECTUL BILL CIPHER



Mulțumesc pentru atenție!

Membrii echipă: Manole Cristiana
Moroianu Adrian-Ștefan