The story of the "Uncrackable" Lockbox, and Why Hackers Need to Work Alongside Developers

Matthew Ruffell Chcon 2019

Challenge #1

Posted by u/cryptocomicon 20 hours ago

³² Hand off your digital assets, even if you are no longer around.

Over the years I've seen many people wondering how they can transfer ownership of their digital assets in the future. They don't want to give a loved one a copy of their wallet seed, but they do want to make sure that no matter what, those assets are made available at a date in the future.

TimeLock is a tool which I have developed to solve this problem, and probably many other problems which I am not aware of. The free version allows you to protect a file of up to 10KB with an un-hackable time lock, synced to the Bitcoin Network.

I'm so confident in this technology that I've created a challenge LockBox file which holds the private key to an address with 0.02 BTC.

Please give it a try.

More information at algomachines.com

Link to the challenge: challenge

Information and Scope

- We are given:
 - Password "TimeLock".
 - Answers to questions "0.02".
 - Time range Start and end, both UTC.
- This limits scope to time lock mechanism only.

Reconnaissance



about download tutorial

orial contact

about

Securely lock your data until a time you choose.

Create LockBoxes up to 10KB.

Un-crackable TimeLock synced to the Bitcoin Network.

Retain privacy. Your data stays on your computer an nowhere else.

Distribute your time locked LockBox to whomever you wish.

technical information

Project files are encrypted using a hash of the project password and the contents of a random file generated on install.

LockBox files contain encrypted:

- Questions
- Delay and TimeLock information
- Data file

Encryption algorithm requires a 1 GB memory buffer.

CPU clock is continuously checked against BTC Network time.

Files are encrypted with:

- Hash of password
- Random generated file
- No mention of Time?

Running TimeLock

. . .

TimeLock Control Panel	×	LockBox Creator ? LockBox Name ? Data File ? Password ? Questions and Answers
Create or Edit a LockBox Open a LockBox		Q1 A1 Q2 A2 Q3 A3 Q4 A4 Q5 A5
Connected to BTC Network		40 ? Make available on or after date 01/18/2019 (MM/DD/YYYY) ? Make available on or after time on above date 00:00:00 (HH:MM::SS) ? Revoke availability on or after date 01/18/2020 (MM/DD/YYYY) ? Revoke availability on or after date 01/18/2020 (MM/DD/YYYY) ? Revoke availability on or after time on above date 00:00:00 (HH:MM::SS) Info Open Test Save Generate LockBox Quit

Unlocking a LockBox

Password		
	Videor	
OK Cancel	TimeLock	able
Answer Question 4 Private key unlocks how many BTC?	N OF	<
t Next Cancel		

Analysing Strings

Ad	dress	Length	Туре	String
's'	.rdata:0000	000000D	С	ControlPanel
's'	.rdata:0000	00000021	С	BTC Network %ld of 8 connections
's'	.rdata:0000	00000057	С	Clock on this computer does not match BTC Network time, must be within +/- 10 minutes.
's'	.rdata:0000	00000019	С	Connected to BTC Network
's'	.rdata:0000	A0000000	С	LockBoxes
's'	.rdata:0000	0000001C	С	Select a LockBox file (*.x)
's'	.rdata:0000	0000001E	С	Unable to open LockBox file:
's'	.rdata:0000	00000022	С	Problem #1 reading LockBox file:
's'	.rdata:0000	0000002A	С	Incorrect password or invalid LockBox #1.
's'	.rdata:0000	0000002A	С	Incorrect password or invalid LockBox #2.
's'	.rdata:0000	00000022	С	Problem #2 reading LockBox file:
's'	.rdata:0000	0000001A	С	Corrupt LockBox file #1:
's'	.rdata:0000	A0000000	С	Canceled.
's'	.rdata:0000	0000022	С	Problem #3 reading LockBox file:
's'	.rdata:0000	00000013	С	Incorrect answers.
's'	.rdata:0000	0000001E	С	No connection to BTC Network.
's'	.rdata:0000	0000004B	С	Number of required connections to BTC Network=%ld, connections we have=%ld
's'	.rdata:0000	00000057	С	Clock on this computer is off by more than 10 minutes with respect to the BTC Network.
's'	.rdata:0000	00000033	С	%ld days %ld hours %ld sec until data is available
's'	.rdata:0000	0000002A	С	%ld hours %ld sec until data is available
's'	.rdata:0000	00000020	С	%ld sec until data is available
's'	.rdata:0000	00000021	С	This data is no longer available
's'	.rdata:0000	00000022	С	Problem #4 reading LockBox file:
's'	.rdata:0000	00000036	С	Can't allocate enough memory to load file to memory:
's'	.rdata:0000	00000022	С	Problem #5 reading LockBox file:
's'	.rdata:0000	00000028	С	Select folder where %s will be created.
's'	.rdata:0000	00000021	С	You elected not to save file: %s
's'	.rdata:0000	00000014	С	Can't create file:
's'	.rdata:0000	00000024	С	Reveal file %s in Windows Explorer?
's'	.rdata:0000	000000D	С	/select, \"%s\"
's'	.rdata:0000	000000D	С	explorer.exe
's'	.rdata:0000	0000005	С	open
's'	.rdata:0000	000000C	С	DelaySecDig
's'	.rdata:0000	80000008	С	%ld sec
's'	.rdata:0000	00000013	С	disable-timesync
's'	.rdata:0000	000000D	С	AlgoMachines
's'	.rdata:0000	0000001D	С	Unable to create directory:
's'	.rdata:0000	0000009	С	TimeLock
's'	.rdata:0000	0000006	С	e.bin
's'	.rdata:0000	0000001E	С	Can't open file for reading:
's'	.rdata:0000	00000012	С	File is invalid:
's'	.rdata:0000	00000017	С	Problem reading file:
's'	.rdata:0000	00000012	С	BTC_peer_list.bin

- "Incorrect answers"
- "%ld days %ld hours %ld sec until data is available"
- "Select folder where %s will be created"
- "Reveal file %s in Windows Explorer?"

Xref Strings – Hackers Best Friend

.rdata:00000001402374F0 .rdata:0000000140237547	al dDavid d	db 't to the BTC align 8	Network.',0	until data is available! A
.rdata:0000000140237548		Rename	N	REF: sub_14000BCD0+FA5to
.rdata:000000014023757B .rdata:0000000140237580	aLdHou 🖕	lump to operand	Enter	is available'.0
.rdata:0000000140237580		Jump in a new window	Alt+Enter	REF: sub_14000BCD0+FC2↑o
.rdata:00000001402375AA .rdata:00000001402375B0	aLdSec 😼	Jump in a new hex window		ble',0
.rdata:00000001402375B0	aThicD	Jump to xref to operand	х	REF: sub_14000BCD0+FDCto
.rdata:00000001402375D0	amisu	List cross references to	Ctrl+X	REF: sub_14000BCD0+105Eto
.rdata:00000001402375F1	a			

mov dwor mov r9d, mov r8d, lea rdx, lea rcx, call sub_ jmp shor	d ptr [rsp+11400h+lpDirectory], edi esi aldDaysLdHoursL ; "%ld ays %1 [rbp+11300h+var_11320] 140008680 t loc_14000CCBC	ebx .d hours %10	d sec until data i	" [0] [1] [1] [2] [2] [2]
+8]] loc_140 mov call xor mov call xor mov call nop	<pre>@ @@CCBC: ; Memory rcx, r13 j_free rcx, [rsp+11400h+File]; File fclose r8d, r8d edx, edx rdi, [rbp+11300h+var_11320] rcx, rdi sub_14002C484</pre>	mov mov call jmp	rcx, [rdx] rax, [rcx] qword ptr [rax+8] loc_14000D17D	loc lea cal nop



The "true" Path Leads to File Writing





TimeLock Mechanism == If Statements



What Happens If We Patch It Out?



Patch jbe -> jmp

Patched Logic



Looks Promising...

, Do	wnloads 🖈 🕞 🕂 👘 🖓	
D	Browse For Folder	×
] P N	Select folder where BTCPrivateKey.txt will be created.	
Т	🔜 Desktop	ר
V	> 🐔 OneDrive	
On	 Analysis This PC 	
Thi	> 🐂 Libraries	
Ne	> 💣 Network > 📴 Control Panel	
	👩 Recycle Bin	
	> PS_Transcripts	
	TimeLock	
	Folder: Analysis	
	Make New Folder OK Cancel	

Videor	I ImeLock - Copy.til	
TimeLock - Copy	/	×
Reveal	file BTCPrivateKey.txt in Window	ws Explorer?
	Yes	No

Loot #1

can samp ocaren nen options minuons neip
BTCPrivateKey.txt - Notepad
File Edit Format View Help
brar Here's the private key:
nctio L1VhgihJF21ovrW2D5VXYuwYaXDjs6rQrNXigdrQ9MkB6mzMW8y2
<pre>b_1 Please send me a message at (https://www.algomachines.com/contact) which includes: b_1</pre>
^{b_1} 1) 90FF12E5-8F68-432F-8518-BEC252CA8076
b_1 2) Sufficient instructions on how you did this so that I can plug the hole.
^{b_1} After receiving the message and verifying the vulnerability, I'll send you another 0.02 BTC.
1b_1; 1b_1
ib_1

Lessons Learned:

Vulnerability:

- Checks placed after decryption is too late. How to Fix:
 - Time is a secret, and needs to be involved in the encryption process.
 - Executables cannot be a root of trust.
 - Key derivation should be handled by a third party.

Challenge #2

Posted by u/cryptocomicon 6 days ago

² Hand off your digital assets, even if you are no longer around (TimeLock V1.2 challenge)

Over the years I've seen many people wondering how they can transfer ownership of their digital assets in the future. They don't want to give a loved one a copy of their wallet seed, but they do want to make sure that no matter what, those assets are made available at a date in the future.

TimeLock is a tool which I have developed to solve this problem, and probably many other problems which I am not aware of. The free version allows you to protect a file of up to 10KB with an un-hackable time lock, synced to the Bitcoin Network.

I'm so confident in this technology that I've created a challenge LockBox file which holds the private key to an address with 0.02 BTC.

Please give it a try.

NOTE: This is going to be much harder than last time.

More information at algomachines.com

Link to the challenge: challenge

Here's a link to the Creator screen for this lock box: <u>Creator</u>. This shows you the available time period for the lock box. I'm also giving you the password and the answer to the one question... much more information than you would have if you stumbled upon this file and wanted to crack it.

Here's a link to the TimeLock V1.0 challenge thread: Challenge #1

What Changed?

- + security_researcher redditor for 1 week 1 point 5 days ago
- I'm looking forward to seeing what has changed. I'll give it a go tonight, and I'll let you know how I get on. Can I ask what you changed or is this meant to be a surprise?

Reply Share Save Edit …

🔶 cryptocomicon 🎤 1 point · 5 days ago · edited 5 days ago

This can't be cracked by stepping over some logic. The data file is encrypted with the time lock data, not just the password and answer.

The following data are required in order to crack the LockBox: Password, Answers, Available time range. However, none of these items are stored in the LockBox. (BTW I'm giving you all of this data for Challenge2.x)

The only way that the program knows that you have entered the right password and answers is if decrypted data is validated. The only way that the program knows if the BTC network time is inside of the required interval is if the data file decryption (using current BTC network time) is validated.

Data file decryption workload is programmable, can be made quite costly. Even if you have the source code for the program, the password and the answers, choosing a very high encryption cycle count for your lock box (and a narrow available time interval) can make cracking a lock box very costly.

Encryption cycle count of 10 for Challenge2.x means that about 20 seconds of CPU time will be required to decrypt.

- "...encrypted with time lock data, not just password and [question] answer"
- Decrypted data must now be "validated".
- Validation implies correct BTC network time.

Plan of Attack

- Locate where the time is passed into decryption function, set it to future.
- We know what the times are. Keep an eye out for:
 - 22/02/2019 00:00 UTC becomes 1550793600. Hex:
 0x5C6F3B80
 - 23/02/2019 00:00 UTC becomes 1550880000. Hex:
 0x5C708D00

Opening Lockboxes





Address	Length	Туре	String
's' .rdata:0000	00000012	С	Answer Question Dlg
's' .rdata:0000	00000013	С	Incorrect <mark>answer</mark> s.
😒 .rdata:0000	00000047	С	Incorrect answer(s) or current time is not within the TimeLock window.
's'.rdata:0000	000000E2	C	The project may include one data file, which will be revealed\nwhen a user answers all qu
's' .rdata:0000	000000A9	С	The project may include between one and five questions and <mark>answer</mark> s. \n\nIn order to acc

17FF6D6A4758A 17FF6D6A4758A 17FF6D6A47590 17FF6D6A47590	aIncorrectAnswe	align 10h <mark>e_0</mark> db 'Incorrect	; answer(s) ;	DATA XREF: or current DATA XREF:	<pre>sub_/FF6D6818</pre> time is not w sub_7FF6D6818	ithin the Time D00:loc_7FF6D0	Lock wi	•
7FF6D	to alncorrectAnswe	≊_0 ⊳				_		×
7FF6D Directio	Ty; Address	Text						
7FF6D 🖼 Up	o sub_7FF6D681E	3D00:loc_7 lea rdx	, aIncorrectAns	we_0; "Incorrec	t answer(s) or curre	nt time is "		
7FF6D								
7FF6D								
7FF6D								
7FF6D		OK	Cancel	Search	Help			
TEECD Line 1 of	1							
7FF6D6A47664		align 8	,	DATA ARELL	300_111000010	0001110010		

Jumping to String



Looking Upwards



Jumping to String

	*		•
📕 🗹 🖼		🛄 🖆 🖼	
00007FF6D681C9CA mov	rcx, r13 ; Memory	00007FF6D681C948 mov	rcx, r13 ; Memory
00007FF6D681C9CD call	j_free	00007FF6D681C94B call	j_free
00007FF6D681C9D2 mov	<pre>rcx, [rsp+11380h+File] ; File</pre>	00007FF6D681C950 mov	<pre>rcx, [rsp+11380h+File] ; File</pre>
00007FF6D681C9D7 call	fclose	00007FF6D681C955 call	fclose
00007FF6D681C9DC lea	<pre>rdx, aIncorrectAnswe ; "Incorrect answers."</pre>	00007FF6D681C95A lea	<pre>rdx, aProblem3Readin ; "Problem #3 reading LockBox file: "</pre>
00007FF6D681C9E3 lea	rcx, [rsp+11380h+var_11338]	00007FF6D681C961 lea	rcx, [rsp+11380h+var_11338]
00007FF6D681C9E8 call	sub_7FF6D681A7D0	00007FF6D681C966 call	sub_7FF6D681A7D0
00007FF6D681C9ED xor	r8d, r8d	00007FF6D681C96B mov	rdx, [rsp+11380h+Filename]
00007FF6D681C9F0 xor	edx, edx	00007FF6D681C970 lea	rcx, [rsp+11380h+var_11338]
00007FF6D681C9F2 mov	rcx, [rsp+11380h+var_11330]	00007FF6D681C975 call	sub_7FF6D6819B90
00007FF6D681C9F7 call	sub_7FF6D683C5C8	00007FF6D681C97A xor	r8d, r8d
00007FF6D681C9FC jmp	loc_7FF6D681D181	00007FF6D681C97D xor	edx, edx
		00007FF6D681C97F mov	rcx, [rsp+11380h+var_11330]
		00007FF6D681C984 call	sub_7FF6D683C5C8
		00007FF6D681C989 jmp	loc_7FF6D681D181

Looking Upwards



Setting Up Breakpoints

🚺 🚄 🔛					
00007FF6D	681CC63				
00007FF6D	681CC63	loc 7FF	6D681CC63:		
00007FF6D	681CC63	mov	[rsp+1138	0h+var 11348],	1
00007FF6D	681CC6B	mov	[rsp+1138	80h+nShowCmd],	40000000h
00007FF6D	681CC73	mov	[rsp+1138	80h+lpDirectory], r13
00007FF6D	681CC78	mov	r9d, 100h	ı	
00007FF6D	681CC7E	lea	r8, [rbp+	-11280h+var 130	1
00007FF6D	681CC85	mov	edx, r12d	-	.
00007FF6D	681CC88	mov	rcx, rbx		
00007FF6D	681CC8B	call	sub_7FF6D	068183A0	
00007FF6D	681CC90	xor	esi, esi		
00007FF6D	681CC92	mov	ecx, esi		
00007FF6D	681CC94	mov	eax, esi		
			- 👌 🐨		
	🗾 🚄 🖟	=			
	00007FF	-6D681CC	96		
	00007FF	-6D681CC	96 loc 7FF	6D681CC96:	
	00007FF	-6D681CC	96 cmp	[rax+rbx], si	1
	00007FF	-6D681CC	9A inz	loc 7FF6D681D	ØD3
			-	-	

N	۰	00007FF605C7CC57	48:8D15 0AA92200 lea	rdx,qword ptr ds:[7FF605EA7568] 00007FF	60
50	•	00007FF605C7CC5E	E9 AA000000 jmp	timelock.7FF605C7CD0D	
*0	L>•	00007FF605C7CC63	C74424 38 01000000 mov	dword ptr ss:[rsp+38],1	
	•	00007FF605C7CC6B	C74424 28 00000040 mov	dword ptr ss: rsp+28,4000000	
	•	00007FF605C7CC73	4C:896C24 20 mov	qword ptr ss:[rsp+20],r13	
	•	00007FF605C7CC78	41:B9 00010000 mov	r9d,100	
	•	00007FF605C7CC7E	4C:8D85 50110100 lea	r8,qword ptr ss:[rbp+11150]	
	•	00007FF605C7CC85	41:8BD4 mov	edx,r12d	
	•	00007FF605C7CC88	48:8BCB mov	rcx,rbx	
	•	00007FF605C7CC8B	E8 10B7FFFF call	timelock.7FF605C783A0	
	•	00007FF605C7CC90	33F6 xor	esi,esi	
	•	00007FF605C7CC92	8BCE mov	ecx,esi	
	\rightarrow	00007FF605C7CC94	8BC6 mov	eax,esi	
	>•	00007FF605C7CC96	40:383418 cmp	byte ptr ds:[rax+rbx],sil	
	I	00007FF605C7CC9A	V 0F85 33040000 jne	timelock.7FF605C7D0D3	
		0000755605676640	FFC1 inc	0.5%	

Decryption Function Found

💭 Dump 1 🛛 💭 Dump 2				🛄 Dump 3				🚛 Dump 4				🚛 Dump 5			💮 Watch 1				[x=] [ocals.	0	St
Address		He	K .															ASC	II			
000001C12E0	4DE80	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	«««	«««««	****	**	
000001C12E0	4DE90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
000001C12E0	4DEA0	EE	FE	EE	FE	EE	FE	EE	FE	B6	80	F4	3D	07	09	04	ЗA	îþî	þîþîþ	¶.Ô=.		
000001C12E0	4DEB0	A8	7A	04	Β4	06	53	5A	A6	59	E9	88	1C	FF	71	61	7D	z.	.SZ	Yéÿ	qa}	
000001C12E0	4DEC0	81	07	AD	A5	9A	05	A8	B7	4E	3D	1F	8F	71	C8	1F	A7		¥''	N=q	È.§	
000001C12E0	4DED0	59	09	12	F4	41	EF	63	51	DD	D5	8F	A3	9D	43	18	BA	Y	ÔAïcQ	ÝÕ.£.	c.°	
000001C12E0	4DEE0	30	83	96	94	CE	FB	18	BF	16	84	ЗF	19	7D	FD	43	D4	0	.Îû.¿	?.}	ýCÔ	
000001C12E0	4DEF0	7D	96	04	5 F	99	30	43	0C	1A	ED	52	59	4E	B7	86	5 B	}	OC.	.iRYN	• • E	
000001C12E0	4DF00	82	62	6E	24	87	F6	E4	5 B	68	01	CC	DB	BA	A1	0E	F8	.bn	\$.öä[h.ÌÙ∘	i.Ø	
000001C12E0	4DF10	98	1A	F3	7C	7A	C9	1F	46	A0	A3	5C	38	2D	6B	55	DF	ó	zÉ.F	£\8-	kUß	
000001C12E0	4DF20	6F	3F	74	5C	C1	CF	11	78	6E	DE	84	8A	06	44	ЗA	75	o?t	\Aï.x	nÞ	D:u	
00000101250	4DE20	DE	02	2.4	70	P.4	EQ	25	20	07	E.4	64	04	70	PC	24	20	h* ·	111/2	Td v	144.0	

Address	He	ĸ															ASCII	
000001C12E04DE80	AB	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~																
000001C12E04DE90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12E04DEA0	EE	FE	EE	FE	EE	FE	EE	FE	B6	80	F4	ЗD	07	09	04	ЗA	îþîþîþîþ¶.ô=:	
000001C12E04DEB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12E04DEC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12E04DED0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12E04DEE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12E04DEF0	73	65	63	72	65	74	32	2E	74	78	74	00	41	41	41	41	secret2.txt.AAAA	
000001C12E04DF00	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА	
000001C12E04DF10	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА	
000001C12E04DF20	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА	
0000010125040520	41	41	41	41	41	41	41	41	41	41	41	41	41	00	04	41	<u> </u>	

Validation Loop Immediately Below



Breakthrough Found

0 0 0	00007FF605C7CB5C 00007FF605C7CB63 00007FF605C7CB63	C685 90030000 00 48:8805 56302800 48:0305 57302800	mov byte ptr ss:[rbp+390],0 mov rax,qword ptr ds:[7FF605EFFBC0] add rax,qword ptr ds:[7FF605EFFBC8]	2
→ •	00007FF605C7CB71 00007FF605C7CB78	48:2B85 10110100 33D2	<pre>sub rax,qword ptr ss:[rbp+11110] xor edx,edx</pre>	

0x5C4E2C15 looks familiar

Converting to decimal: 1548626965

This is a Unix timestamp! 28/01/19 11:09:25

RAX	000000005C4E2C15
RBX	0000000000000008
RCX	000001C12A410000
RDX	000001C12A410000
RBP	00000072D26ED820
RSP	00000072D26ED720
RSI	0000000000000008
RDI	000001C12E159540

Modifying Timestamp

		^	Hide I	FPU	
0	ck on this	compute	RAX RBX RCX	0000000 0000000 000001C	05C4E2C15 000000008 12A410000
	Edit			2	× 410000
			15		6ED 820
	Expression:	000000	0005C6FA	624	000008
	Bytes:	24A66F	5C00000	0000	1000001
					FA5 401
	Signed:	155082	20900		FFFFFF
					6ED 620
	Unsigned:	155082	20900		1000001
					000001
	ASCII:	\a	\$		15 95 30
					C7CB71
		OK		Cancel	00000021

RAX	000000005C6FA624
RBX	0000000000000008
RCX	000001C12A410000
RDX	000001C12A410000
RBP	00000072D26ED820
RSP	00000072D26ED720
RSI	0000000000000008
RDI	000001C12E159540

-	0000111003010031	1010010 0/01012100	Treation of a per april recovery pee	0000711
	00007FF605C7CC5E	E9 AA000000	jmp timelock.7FF605C7CD0D	
→•	00007FF605C7CC63	C74424 38 01000000	mov dword ptr ss:[rsp+38],1	
	00007FF605C7CC6B	C74424 28 00000040	mov dword ptr ss:[rsp+28],4000000	
	00007FF605C7CC73	4C:896C24 20	mov qword ptr ss:[rsp+20],r13	
	00007FF605C7CC78	41:B9 00010000	mov r9d,100	
	00007FF605C7CC7E	4C:8D85 50110100	lea r8,qword ptr ss:[rbp+11150]	
	00007FF605C7CC85	41:8BD4	mov edx,r12d	
	00007FF605C7CC88	48:8BCB	mov rcx,rbx	
	00007FF605C7CC8B	E8 10B7FFFF	call timelock.7FF605C783A0	
	00007FF605C7CC90	33F6	xor esi,esi	
•	00007FF605C7CC92	VSBCE	mov ecx,esi	
•	00007FF605C7CC94	8BC 6	mov eax,esi	
>0	00007FF605C7CC96	40:383418	cmp byte ptr ds:[rax+rbx].sil	

Stepping Over Decryption

Dump 1 💭 Dump 2				🛄 Dump 3				🛄 Dump 4				🚛 Dump 5			🧶 Watch 1				[x=] Locals	4	Struct
Address		He	ĸ															ASC	II		
000001C12F3	9D6B0	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	«««	~~~~~~~	««««	
000001C12F3	9D6C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
000001C12F3	9D 6D 0	00	00	00	00	00	00	00	00	8C	80	F4	07	1A	09	10	35		ô.	5	
000001C12F3	9D6E0	AF	62	57	A5	BD	C 0	1A	F5	E3	ED	7F	AF	DC	F4	EF	6D	=bW	¥%A.õãí.⊤	ÜÔïm	
000001C12F3	9D6F0	57	18	3B	5C	86	AC	C6	F5	34	BB	F2	52	63	Ε4	AA	36	W.;	∖.¬ÆÕ4»ÒR	cä¤6	
000001C12F3	9D700	50	04	B7	44	B7	ЗC	EB	8D	E7	32	09	58	61	2A	65	73	P. •	D•<ë.c2.X	a*es	
000001C12F3	9D710	05	48	C7	C1	AF	66	8F	CC	8A	FB	F2	4F	07	CF	8B	45	. HÇ	A⁻f.Ì.ûòO	.Ï.E	
000001C12F3	9D720	EB	9D	5A	76	2E	00	27	4E	23	7C	43	74	89	9E	71	FO	ë.z	v'N# Ct	qð	
000001C12F3	9D730	5 B	ЗA	E1	44	69	AB	50	2D	91	31	31	22	BD	00	4A	63	[:á	Di«P11"	%.JC	
000001C12F3	9D740	2D	5 B	62	D7	87	F7	D8	EA	27	79	C6	A1	71	5A	66	98	-[b	x.÷Øê'yÆj	gZf.	
000001C12F3	9D750	40	DF	47	OB	9D	8A	A4	26	23	E2	6C	C0	EA	64	8F	30	@ßG	¤&#â1À</td><td>êd.0</td><td></td></tr><tr><td>00000101252</td><td>90760</td><td>70</td><td>7.4</td><td>20</td><td>EE</td><td>C 2</td><td>92</td><td></td><td>94</td><td>95</td><td>Δ.4</td><td>62</td><td>14</td><td>95</td><td>92</td><td>14</td><td>E.4</td><td>170</td><td>їÅ Ц йс</td><td>ä</td><td></td></tr></tbody></table>		

Command

									•									
Address	He	x															ASCII	
000001C12F39D6B0	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	*****							
000001C12F39D6C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12F39D6D0	00	00	00	00	00	00	00	00	8C	80	F4	07	1A	09	10	35	ô5	
000001C12F39D6E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12F39D6F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12F39D700	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12F39D710	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C12F39D720	4C	6F	63	6B	42	6F	78	2E	43	68	61	6C	6C	65	6E	67	LockBox.Challeng	
000001C12F39D730	65	2E	32	2E	70	72	69	76	61	74	65	5 F	6B	65	79	2E	e.2.private_key.	
000001C12F39D740	74	78	74	00	43	6F	6E	67	72	61	74	75	61	74	69	6F	txt.Congratuatio	
000001C12F39D750	6E	73	21	20	59	6F	75	20	68	61	76	65	20	73	75	63	ns! You have suc	
0000010125290760	62	GE	72	72	GG	75	GC.	GC.	79	20	62	CE.	GD	70	GC.	CE.	cessfully comple	

Looks Promising...

(pprogram)	
Browse For Folder	×
Select folder where LockBox.Challenge.2.private_key.t will be created.	xt
6 > Sun > Application Data	^
Cookies	
Pesktop Ps_Transcripts TimeLock 2	
> Documents + Downloads	
> 🔆 Favorites	<u> </u>
Folder: TimeLock_2	
Make New Folder OK Cance	



Loot #2

20	Graph 📝 Log 📋 Notes 🔍 Breakpoints 🛲 Memory Map
	LockBox.Challenge.2.private_key.txt - Notepad
	File Edit Format View Help
	Congratuations! You have successfully completed TimeLock Challenge #2.
	Please contact me via: https://www.algomachines.com/contact
	I will pay you an additional 0.02 BTC for a detailed report describing how you cracked TimeLock V1.2.
	Public BTC address for the reward: 3NuEijXKmnRUeri9DfvDZ2f5RDkHLUBgNS
	Private BTC address for the reward: KyYvEbvjFFGyHGQcRHYNvASQAMmNMtgcqHsgmoLTW62iY4rimcUV

Lessons Learned:

Vulnerability:

- Secret was found and replaced, with no additional validation. How to fix:
- Secrets should be hashed, so they are difficult / impossible to locate.
- Keys should not be generated locally, but instead supplied by a trusted third party.

Challenge #3

Posted by u/cryptocomicon 9 days ago

TimeLock your digital assets

Over the years I've seen many people wondering how they can transfer ownership of their digital assets in the future. They don't want to give a loved one a copy of their wallet seed, but they do want to make sure that no matter what, those assets are made available at a date in the future.

Designing an un-hackable TimeLock is challenging. This is my third version and the third challenge, with a 0.02 BTC reward.

Please give it a try.

More information at algomachines.com

Link to the challenge: challenge

Here's a link to the Creator screen for this lock box: <u>Creator</u>. This shows you the available time period for the lock box. I'm also giving you the password and the answer to the one question... much more information than you would have if you stumbled upon this file and wanted to crack it.

Plan of Attack

- Launch a "Sybil" Attack
 - Introduce malicious nodes as the network.
 - Behave exactly like legitimate nodes.
 - Have time set to the future.
 - Disable internet access and force local nodes.

TimeLock Uses DNS Seed Nodes



- seed.bitcoin.spia.be
- bitseed.xf2.org
- dnsseed.bitcoin.dashjr.org
- dnsseed.bluematt.org
- missionctrl.info

```
✓ Domain Name System (response)
     Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
     Ouestions: 1
     Answer RRs: 21
     Authority RRs: 0
     Additional RRs: 0
  Y Oueries
     > dnsseed.bluematt.me: type A, class IN
  Answers
     > dnsseed.bluematt.me: type A, class IN, addr 142.93.167.187
     > dnsseed.bluematt.me: type A, class IN, addr 70.120.24.242
     > dnsseed.bluematt.me: type A, class IN, addr 144.76.99.209
     > dnsseed.bluematt.me: type A, class IN, addr 24.101.67.50
     > dnsseed.bluematt.me: type A, class IN, addr 95.161.12.45
     > dnsseed.bluematt.me: type A, class IN, addr 188.193.164.196
     > dnsseed.bluematt.me: type A, class IN, addr 169.229.198.105
     > dnsseed.bluematt.me: type A, class IN, addr 91.121.97.23
     > dnsseed.bluematt.me: type A, class IN, addr 95.216.111.121
     > dnsseed.bluematt.me: type A, class IN, addr 111.90.159.213
     > dnsseed.bluematt.me: type A, class IN, addr 45.20.67.1
     > dnsseed.bluematt.me: type A, class IN, addr 86.15.59.249
     > dnsseed.bluematt.me: type A, class IN, addr 45.120.52.199
     > dnsseed.bluematt.me: type A, class IN, addr 37.59.63.56
     > dnsseed.bluematt.me: type A, class IN, addr 24.210.98.8
     > dnsseed.bluematt.me: type A, class IN, addr 129.122.222.134
     > dnsseed.bluematt.me: type A, class IN, addr 98.228.169.22
     > dnsseed.bluematt.me: type A, class IN, addr 144.76.78.214
     > dnsseed.bluematt.me: type A, class IN, addr 95.84.156.162
     > dnsseed.bluematt.me: type A, class IN, addr 71.13.92.62
```
Rolling Our Own DNS

basedns.py - C:/Users/Analysis/Desktop/basedns.py (3.7.2) - [] ;	×	🕞 *Python 3.7.2 Shell* -	_		\times
File Edit Format Run Options Window Help			File Edit Shell Debug Options Window Help			
<pre>#!/usr/bin/env python3</pre>		^	Python 3.7.2 (tags/v3.7.2:9a3ffc0492, Dec 23 2018, 23:09:28) [MSC v.]	1916 (54 bit	, ^
# (c) 2014 Patryk Hes			(AMD64)] on win32			
import socketserver			Type "help", "copyright", "credits" or "license()" for more informati	ion.		
import sys			>>>			
import random			======================================			
			U[36mStarted DNS server.U[39m			
DNS_HEADER_LENGTH = 12			0(31m1.0.0.127.1n-addr.arpa0(39m			
The lubra of the some DNS database with IPS connected to regexs			U[32mhello.ss.internal0[39m			
IP = (127.0.0.1)			0[31mmerro.ss.internal0[39m			
class DNSHandler (socketserver BasePerusetHandler) .			0[32mwpad.internal0[39m			
def handle(self):			0[32mwpad.internal0[39m			
<pre>socket = self.request[1]</pre>			0[32mwpad.internal0[39m			
<pre>data = self.request[0].strip()</pre>			0[32mwpad.internal0[39m			
			<pre>[32mwpad.internal0[39m</pre>			
<pre># If request doesn't even contain full header, don't respond.</pre>			Fail			
<pre>if len(data) < DNS_HEADER_LENGTH:</pre>			>>>			
return			======================================			
			U[36mStarted DNS server.U[39m			
# Try to read questions - if they're invalid, don't respond.			U[32mwpad.internal0[39m			
try:			U[31m1.0.0.127.1n-addr.arpau[39m			
all_questions = sell.dns_extract_questions(data)			0[31mballo eg internal0[39m			
return			[[3]m].0.0.127.in=addr.arna[[39m]			
			0[32mhello.com.internal0[39m			
<pre># Filter only those guestions, which have QTYPE=A and QCLASS=IN</pre>			0[31mhello.com.internal0[39m			
# TODO this is very limiting, remove QTYPE filter in future, handl	e diff	£	<pre>[32mwpad.internal0[39m</pre>			
accepted questions = []			<pre>[32mwpad.internal0[39m</pre>			
for question in all_questions:						
<pre>name = str(b'.'.join(question['name']), encoding='UTF-8')</pre>						
if question['qtype'] == b'\x00\x01' and question['qclass'] ==	b'\x00	0				
accepted_questions.append(question)						
print('\033[32m{}\033[39m'.format(name))						
cise. nrint(!\033[3]m(}\033[39m! format(name))						
prine((000[01m()(000[05m ·I01mdo(ndme))						
response = (
<pre>self.dns_response_header(data) +</pre>						
<pre>self.dns_response_questions(accepted_questions) +</pre>						
<pre>self.dns_response_answers(accepted_questions)</pre>		\sim				\sim
L	.n: 10 C	ol: 0		1	Ln: 28 (Col: 0

Adding Randomised DNS Entries to Lookup

records = b^{11} for question in questions: for i in range(1, 21): record = b''for label in question['name']: # Length octet record += bvtes([len(label)]) record += label # Zero length octet record $+= b' \times 00'$ # TYPE - just copy OTYPE # TODO QTYPE values set is superset of TYPE values set, handle record += question['gtype'] # CLASS - just copy QCLASS # TODO QCLASS values set is superset of CLASS values set, handl record += question['gclass'] # TTL - 32 bit unsigned integer. Set to 0 to inform, that respo # should not be cached. record += b'\x00\x00\x00\x00' # RDLENGTH - 16 bit unsigned integer, length of RDATA field. # In case of OTYPE=A and OCLASS=IN, RDLENGTH=4. record $+= b' \times 00 \times 04'$ # RDATA - in case of QTYPE=A and QCLASS=IN, it's IPv4 address. temp IP = IP + '.' + str(random.randint(1, 200))temp IP = temp IP + '.' + str(random.randint(1, 200)) temp_IP = temp_IP + '.' + str(random.randint(1, 200)) record += b''.join(map(lambda x: bytes([int(x)]), temp IP.split('.'))) records += record return records

C:\Users\Analysis>nslookup hello.com Server: UnKnown Address: 127.0.0.1 Non-authoritative answer: hello.com.internal Name: Addresses: 127.61.198.11 127.110.170.2 127.95.65.29 127.195.84.141 127.22.66.121 127.153.66.63 127.92.26.30 127.89.164.167 127.118.186.71 127.56.36.25 127.90.114.142 127.49.92.175 127.122.12.13 127.120.48.18 127.20.28.117 127.50.2.168 127.109.138.131 127.7.57.131 127.65.134.11 127.78.64.2

Starting Our Bitcoin Node

Date & time

Date and time

7:26 PM, Saturday, 9 March 2019

Set time automatically



Set time zone automatically



Change date and time

Change

Command Prompt - "C:\Program Files\Bitcoin\daemon\bitcoind.exe"	– 🗆 ×
2019-03-09T06:31:11Z init message: Verifying blocks	
2019-03-09T06:31:11Z block index 262ms	
2019-03-09T06:31:11Z init message: Loading wallet	
2019-03-09T06:31:11Z [default wallet] nFileVersion = 170100	
2019-03-09T06:31:11Z [default wallet] Keys: 2001 plaintext, 0 encrypted, 2001 w/ metadata, 2	001 total. Unknown wallet re
cords: 1	
2019-03-09T06:31:11Z [default wallet] Wallet completed loading in 168ms	
2019-03-09T06:31:11Z [default wallet] setKeyPool.size() = 2000	
2019-03-09T06:31:11Z [default wallet] mapWallet.size() = 0	
2019-03-09T06:31:11Z [default wallet] mapAddressBook.size() = 0	
2019-03-09T06:31:11Z mapBlockIndex.size() = 4001	
2019-03-09T06:31:11Z Imported mempool transactions from disk: 0 succeeded, 0 failed, 0 expir	ed, 0 already there
2019-03-09T06:31:11Z nBestHeight = 0	
2019-03-09106:31:112 torcontrol thread start	
2019-03-09106:31:112 Bound to [::]:8333	
2019-03-09106:31:112 Bound to 0.0.0.0:8333	
2019-03-09100:31:112 Init message: Loading P2P addresses	
2019-03-09100:31:112 Loaded 1033 addresses from peers.dat 0ms	
2019-03-09100:31:112 Init message: Loding Danist	
2019-05-09100.51.112 Init message. Starting network threads	
2019-03-00106:31:117 init message. Done loading	
2019-03-09T06:31:117 add on thread start	
2019-03-09T06:31:117 opencon thread start	
2019-03-09T06:31:117 msghand thread start	
2019-03-09T06:31:22Z Loading addresses from DNS seeds (could take a while)	
2019-03-09T06:31:22Z 140 addresses found from DNS seeds	
2019-03-09T06:31:22Z dnsseed thread exit	

Did We Hack The Thing Yet?



When Stuck – Search Strings

Address	Length
's' .rdata:0000	00000036
's' .rdata:0000	000003B
's' .rdata:0000	000000A1
's' .rdata:0000	00000045

_		- Charles	
IV	ne	Stu	nna
• *			mg
-			

C

С

C C

- AddSeedNode() : already has seed node matching url :
- AddSeedNode() : no more than 32 seed nodes may be added.
- Connect() : number of seed nodes is zero and the size of peer_info is less than 50, must h...
- Connect() : number of seed ports is not equal to number of seed urls



Determining How Seed Nodes are Added



Open Debugger; Set Breakpoint

🔆 TimeLock.exe - PID: 3A8 - Module: timelock.exe - Thread: Main Thread 15B4 - x64dbg — 🗆 X										
File View Debug Trace Plugins Favourites Options Help Jan 20 2019										
🚔 🧐 🔳 💠 🔢 🍷 🐟 🕎 🎍 🛊 📲 🥜 🚝 🛷 🥒 fx # Az 🏨 🗐 👮										
🖾 CPU 🧟 Graph 📝 Log 🖄 Notes 🔹 Breakpoints 📟	Memory Map 📋 Call Stack 🗠 SEH 🔟 Script	🐏 Symbols 🛛 😒 Sor	ource 🖉 References	😒 Threads 🛛 🗐 Snowman	Handles 👔 Trace					
 00007FF6134778AD 4C:8D85 A0000000 00007FF6134778B4 48:8B15 C5452800 	lea r8, qword ptr ss: [rbp+A0] mov rdx, gword ptr ds: [7FF6136FBE80] 00(07FF6136FBE A H	lide FPU							
OO007FF613477868 E8 E0EsFEFF 00007FF6134778C0 48:8805 39432800 00007FF6134778C0 8378 50 32 00007FF6134778C6 8378 50 32 00007FF6134778C6 8378 50 32 00007FF6134778C6 8378 50 32 00007FF6134778C6 85583FFFF 00007FF6134778D6 48:88D0 00007FF6134778C6 48:88D0 00007FF6134778C6 48:88D0 00007FF6134778C6 48:88D0 00007FF6134778C6 48:88D0 00007FF6134778C7 75 60 00007FF6134778C7 48:88D8 00007FF6134778C7 48:88D8 00007FF6134778C7 74 10 00007FF6134778C7 48:88C8 00007FF6134778C7 48:88C8 00007FF61347790 48:88C8 00007FF61347791 48:88D0 00007FF61347791 48:88D0 00007FF61347791 48:88D0 00007FF61347791 48:83D8 08000000 10 00007FF61347792 48:83D8 08000000 10 00007FF61347791 48:83D8 080000000 10 000007FF61347792 <td><pre>call timelock.7FF613465EA0 mov rax,qword ptr ds:[7FF6136FBC00] cmp dword ptr ds:[rax+s0],32 ge timelock.7FF613477A06 mov ecx,5D call timelock.7FF6134776C30 mov rdx,rax lea r9,qword ptr ss:[rbp+A0] call timelock.7FF613467C9 test al,al jne timelock.7FF61347794E mov rbx,qword ptr ds:[7FF6136FBC00] test rbx,rbx call timelock.7FF61347790A mov rcx,rbx call timelock.7FF61347790A mov rcx,rbx call timelock.7FF613467E0 mov rdx,rbx call timelock.7FF613467E0 mov rdx,rbx call timelock.7FF61346720 mov rcx,rbx call timelock.7FF61346720 mov rdx,rbx call timelock.7FF61347792E mov rdx,qword ptr ss:[rbp+A0] test rdx,rdx test rdx,rdx test rdx,rdx</pre></td> <td>'2' '2' ']' RD RD RD RD RD RD RD RD RD RD RD RD RD</td> <td>AX 000002AAA1530630 BX 000002AAA1613560 CX 000002AA9C840000 CX 000002AA9C840000 BP 0000002AA9C840000 BP 000000C53F5AD180 SI 000000C53F5AD180 SI 0000000000000000 BP 00000000000000000 B 000000000000000000000000000000000000</td> <td>L"C:\\Windows\\syst timelock.00007FF613</td> <td>em32\\mswsock.dll" 4778D1</td>	<pre>call timelock.7FF613465EA0 mov rax,qword ptr ds:[7FF6136FBC00] cmp dword ptr ds:[rax+s0],32 ge timelock.7FF613477A06 mov ecx,5D call timelock.7FF6134776C30 mov rdx,rax lea r9,qword ptr ss:[rbp+A0] call timelock.7FF613467C9 test al,al jne timelock.7FF61347794E mov rbx,qword ptr ds:[7FF6136FBC00] test rbx,rbx call timelock.7FF61347790A mov rcx,rbx call timelock.7FF61347790A mov rcx,rbx call timelock.7FF613467E0 mov rdx,rbx call timelock.7FF613467E0 mov rdx,rbx call timelock.7FF61346720 mov rcx,rbx call timelock.7FF61346720 mov rdx,rbx call timelock.7FF61347792E mov rdx,qword ptr ss:[rbp+A0] test rdx,rdx test rdx,rdx test rdx,rdx</pre>	'2' '2' ']' RD RD RD RD RD RD RD RD RD RD RD RD RD	AX 000002AAA1530630 BX 000002AAA1613560 CX 000002AA9C840000 CX 000002AA9C840000 BP 0000002AA9C840000 BP 000000C53F5AD180 SI 000000C53F5AD180 SI 0000000000000000 BP 00000000000000000 B 000000000000000000000000000000000000	L"C:\\Windows\\syst timelock.00007FF613	em32\\mswsock.dll" 4778D1					
	Imov esv edi	> 1:	rcx 000002AA9C84000	0						
eax=1CC L'm' ed1=10 .text:00007FF613477927 timelock.exe:\$17927 #16D27		2: 3: 4: 5:	rdx 000002AA9C84000 r8 000000000000001 r9 00002AAA15F6A01 [rsp+28] 000002AAA1	0 613560 "C:\\Users\\Analy:	sis\\AppData\\Roaming\\A					
💭 Dump 1 💭 Dump 2 💭 Dump 3 💭 Dump 4 💭 Dump 5	👹 Watch 1 🛛 🕼 🖉 Struct	0000	0000053F5AD0B0 000002A	A9C8D22E0	^					
ddress Hex ASCII 000000000000000000000000000000000000										
Command:					Default 🔻					
Running Thread 1740 created, Entry: ntdll.00007FF802FEB880				Т	ime Wasted Debugging: 0:03:13:47					

Breakpoint Hits, Familiar DNS Entry

00007FF61347	778AD 4C:8D85 A0000000	lea r8,qword ptr ss:[rbp+A0]
00007FF61347	7884 48:8815 C5452800	mov rdx, gword ptr ds: [7FF6136FBE80]
00007FF61347	78BB E8 E0E5FEFF	call timelock.7FF613465EA0
00007FF61347	78C0 48:8805 39432800	mov rax, qword ptr ds: [7FF6136FBC00]
00007FF61347	78C7 8378 50 32	cmp dword ptr ds:[rax+50],32
00007FF61347	78CB V 0F8D 35010000	jge timelock.7FF613477A06
RIP 00007FF6134	78D1 B9 5D000000	mov ecx,5D
00007FF61347	78D6 E8 55F3FFFF	call timelock.7FF613476C30
00007FF61347	78DB 48:8BD0	mov rdx,rax
00007FF61347	78DE 4C:8D8D A0000000	lea r9,qword ptr ss:[rbp+A0]
00007FF61347	78E5 E8 06D4FEFF	call timelock.7FF613464CF0
00007FF61347	78EA 84C0	test al,al
00007FF61347	78EC V 75 60	jne timelock.7FF61347794E
00007FF61347	78EE 48:8B1D 0B432800	mov rbx,qword ptr ds:[7FF6136FBC00]
00007FF61347	78F5 48:85DB	test rbx,rbx
r@ 00007FF61347	78F8 × 74 10	je timelock.7FF61347790A
00007FF61347	78FA 48:8BCB	mov rcx,rbx

RAX	000001FB750E7D90
RBX	000001FB751855A0
RCX	00000000FFFFFFF
RDX	00000000000000000
RBP	0000001352BAD260
RSP	0000001352BAD160
RSI	0000001352BAD480
RDI	000000000000000000000000000000000000000

"missionctrl.info" "C:\\Users\\Analysi

What Happens If We Do It Again?



Modify DNS Entry, Avoid Conflicts

RAX	000001FB794DDD00
RBX	000001FB751855A0
RCX	00000000FFFFFFFF
RDX	00000000000000000
RBP	0000001352BAD260
RSP	0000001352BAD160
RSI	0000001352BAD480
RDI	000000000000000000000000000000000000000

	• 0	000	7FF	613,	477	984	_	- 8	34C.0						t	est	a1	,al					
	0	000	7FF	613	🕮 Medificualue					~					me	loci	C.7F	F61	.347	79C	2		
	• 0	000	7FF	613	-						~						CX	,60					
	• 0	000	7FF	613													ti	melo	ock.	.7FF	613	476	23
	• 0	000	7FF	613	Ev	nroc	noion			69							dx	(,ra)	C			_	
	• 0	000	7FF	613		pres	SIUH	•	L	0.01							9,	qwor	d p	otr	SS:	[rb	p-
	• 0	000	7FF	613													ti	melo	ock.	.7FF	613	464(C F
	• 0	000	7FF	613	By	tes:				69							al	,al					
	•	000	700	612													me	loci	75	CC 61	247	700	•
	<pre></pre>				_				Г							_							
rdx=0					Sig	gned	:			105													_
ax=000001F	B794DD	DOO) "s	sss					_														
					Lle	eian	od.			105													
text:00007	FF6134	1779	958	tin	Ur	isign	eu:		Ľ	105													
				-																			_
Dump 1	Di Di	imo '	2	1	AS	SCII:						.i					tel	h 1	La:	=110	cale		Э
e-e bamp 1	9-0-01	amp .	2	0-0					L									11	1.0	100	COID	4	r.,
Address		Hex	C															ASC:	II				1
000001FB794	DDCD0	AB	AB	AB							OK			Ca	ncel		E	«««	« « « «	«««	«««î	þîþ	Т
000001FB794	DDCE0	00	00	00							OIL				in reer		0					2.2	
000001FB794	DDCF0	EE	FE	EE	TE	EE	TE	CC	TE	00	22	- 21	37	UI	05	04	-12	îþî	þîþ	îþ.'	".WÑ	2	
000001FB794	DDD00	73	73	73	73	2E	62	69	74	63	6F	69	6E	2E	73	69	70	SSS	s.b	itc	oin.	sip	
000001FB794	DDD10	61	2E	65	65	00	FO	AD	BA	OD	FO	AD	BA	EE	FE	AB	AB	a.e	e.ð	. °. č	ð.°î	þ««	
000001FB794	DDD20	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	EE	FE	«««	«««	«««		«îþ	
000001FB794	DDD 30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
		_											-		-		-	0, 0,	- A.	<u>, , , , , , , , , , , , , , , , , , , </u>	S		_

"seed.bitcoin.sipa.be"

"C:\\Users\\Analysis\\AppData\\Roaming\\Alc

Address	Hep	<															ASCII
000001FB794DDCD0	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	EE	FE	EE	FE	«««««««««««îþîþ
000001FB794DDCE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001FB794DDCF0	EE	FE	EE	FE	EE	FE	EE	FE	0C	22	9F	57	D1	05	04	32	îþîþîþîþ.".WÑ2
000001FB794DDD00	73	65	65	64	2E	62	69	74	63	6F	69	6E	2E	73	69	70	seed.bitcoin.sip
000001FB794DDD10	61	2E	62	65	00	F0	AD	BA	OD	FO	AD	BA	EE	FE	AB	AB	a.be.ð.º.ð.ºîþ««
000001FB794DDD20	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	EE	FE	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
000001FB794DDD30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	_																

Looks Promising...

ory map		<u> </u>	Doubt	
Browse	For Folder			Х
Select f TimeLoc created	older where k.VChallenge.V1.3. l.	PrivateKeyRe	eward.txt will be	1
> 🧉	OneDrive			^
~ 2	Analysis			
	.idlerc			
	🗊 3D Objects			
×	AppData			
	> Local			
	> 🔤 LocalLow			
	🗸 📙 Roaming			
	> 🔤 Adob	e		
	🗸 🔤 AlgoN	Aachines		~
Folder:	LockBoxes			
Make	New Folder	OK	Cancel	
Watch 1	x=11 ocals	# Struct		

	cimeroektriti ozororer o	
TimeLoc	¢	×
?	Reveal file TimeLock.VChallenge.V1.3.Private Windows Explorer?	eKeyReward.txt in
	Yes	No

Loot #3

TimeLock.VChallenge.V1.3.PrivateKeyReward - Notepad

File Edit Format View Help

Well done!

You have successfully completed the TimeLock V1.3 challenge.

I am impressed!

Please contact me via: https://www.algomachines.com/contact

I will happily send you at least 0.02 BTC for a detailed report describing how you cracked TimeLock V1.3.

TimeLock 1.3 challenge reward public address: 34r4PbKUM2odwf1EV2Jnxx9d3k1rWKgAzD TimeLock 1.3 challenge reward private address: Kx4TLBeaMLG19wkeocVX6YG63BTWErKvnTvnPfVgvXf5tD1U1Mij

Lessons Learned:

Vulnerability:

- DNS cannot be trusted, can be easily manipulated.
- Executables cannot be trusted as attackers can easily redirect execution flow.
- No attestation performed on connected nodes.

How to fix:

- Tunnel DNS via own dnssec validating resolver.
- Validate nodes, in this case, verify blockchain?
- No internet access should raise alarm bells.
- Do not peer with localhost.

Challenge #4

Posted by u/cryptocomicon 23 days ago

Quest for the unhackable TimeLock

Do you want to hand off your digital assets to your loved ones in the future without handing them off to a third party today?

I've created a software product to do that, using the decentralized Bitcoin network, and I'm perfecting it with challenges and rewards.

TimeLock 1.5 is free software. You can read about it here: https://www.algomachines.com/

The challenge history and latest installer / challenge is here: https://www.algomachines.com/people

Plan of Attack

- Find encryption / decryption functions
- Review encryption:
 - Look for improper use of modes.
 - Look for weak algorithms.

Anti Debugging Measures?

Thread SCC exit

Thread 620 exit Process stopped with exit code 0xFFFFFFF9

Saving database to C:\Users\Analysis\Downloads Debugging stopped!

Command:

Terminated Debugging stopped!

			· · · · · · · · · · · · · · · · · · ·	
🗾 🚄 🖼		🗾 🚄 🖼		
00007FF7673F99FD		00007FF7673F998E_sub	ebx, esi	
00007FF7673F99FD loc 7F	F7673F99FD: : uExitCode	00007FF7673F9990 sub	ebx, edi	
00007FF7673F99FD mov	ecx. ØFFFFFFBh	00007FF7673F9992 mov	eax, ebx	
00007FF7673F9A02 call	cs:ExitProcess	00007FF7673F9994 cda		
		00007FF7673F9995 xor	eax, edx	
		00007FF7673F9997 sub	eax, edx	
		00007FF7673F9999 cmp	eax, 0Fh	
		00007FF7673F999C jg	short loc 7FF7673F99F1	
	-		· · · · · · · · · · · · · · · · · · ·	
1 🖌 🖾			🖬 🎿 🖼	
20007FE7673E999E mov	ecx. 3E8h : dwMillisec/	onds	00007EE7673E99E1	
0007FE7673E9943 call	cs: imn Sleen	onus	00007FE7673E99E1 loc 7EE7673E9	PE1:ExitCode
20007FF7673E9949 lea	pcx_stpu_ZEEZ6Z693BE0 : lpCr	riticalSection	00007FE7673E99E1 mov ecx	AFFFFFFFAh
0007FE7673E99B0 call	cs:EnterCriticalSection	reconsection	00007EE7673E99E6 call cs:Ex	itProcess
00007FF7673F99B6 lea	rcx. [rsp+38h+arg 8] : lpPerf	formanceCount		
00007FF7673F99BB call	cs:OuervPerformanceCounter			
00007FF7673F99C1 xor	ecx. ecx : Time			
00007FF7673F99C3 call	time64			
00007FF7673F99C8 mov	rbx, rax			
00007FF7673F99CB mov	rax, gword ptr [rsp+38h+arg {	81		
00007FF7673F99D0 sub	rax, gword ptr [rsp+38h+Perfo	ormanceCount]		
00007FF7673F99D5 cqo		-		
00007FF7673F99D7 idiv	qword ptr [rsp+38h+Frequency]	1		
00007FF7673F99DC mov	edi, eax			
00007FF7673F99DE lea	eax, [rbp+3]			
00007FF7673F99E1 cmp	edi, eax			
00007FF7673F99E3 jle	short loc_7FF7673F9970			
	* *			
🗾 🚄 🖼				
00007FE7673E99E5				
	1 755767350055	tCode		
00007FF7673F99E5	TOC /FF/0/2F99E2: ; UEXI			
00007FF7673F99E5 00007FF7673F99E5	nov ecx, 0FFFFFF9h			

Patch Out CreateThread To Defeat Anti Debugging

			•	
	🗾 🚄 🛤	.		
	00007FF	7673F9A86		
	00007FF	7673F9A86 loc 7FF	7673F9A86:	
atal Error"	00007FF	7673F9A86 xor	eax, eax	
ype	00007FF	7673F9A88 lea	r8, sub_7FF767	3F98D0 ; lpStartAddress
Text	00007FF	7673F9A8F xor	r9d, r9d	; lpParameter
nd	00007FF	7673F9A92 mov	[rsp+38h+lpThre	eadId], rax ; lpThreadId
	00007FF	7673F9A97 xor	edx, edx	; dwStackSize
xitCode	00007FF	7673F9A99 <mark>xor</mark>	ecx, ecx	; lpThreadAttributes
	00007FF	7673F9A9B mov	[rsp+38h+dwCrea	ationFlags], eax ; dwCreationFlags
	00007FF	7673F9A9F call	cs:CreateThrea	d
	00007FF	7673F9AA5 test	rax, rax	
	00007FF	7673F9AA8 jnz	short loc_7FF7	673F9AD8
		•		· · · · · · · · · · · · · · · · · · ·
🚺 🚄 🔛				
00007FF7673F9	9AAA mov	ecx, 1A2h		00007FF7673F9AD8
00007FF7673F9	9AAF call	sub 7FF76740E10	0	00007FF7673F9AD8 loc 7FF7673F9AD8:
00007FF7673F9	9AB4 lea	r8, Caption	; "Fatal Error'	00007FF7673F9AD8 add rsp, 38h
00007FF7673F9	9ABB mov	r9d, 10h	; uType	00007FF7673F9ADC retn
00007FF7673F9	9AC1 mov	rdx, rax	; lpText	00007FF7673F9ADC sub_7FF7673F9A40 end
00007FF7673F9	9AC4 xor	ecx, ecx	; hWnd	00007FF7673F9ADC
00007FF7673F9	9AC6 call	cs:MessageBoxA		
			- 1	
00007FF7673F9	9ACC mov	ecx, 0FFFFFFFEh	i ; uExitCode	

inco.			
E Assemble at 00007FF7673F9A9F			×
mov eax, 0x1			
☐ Keep Size	l asmjit	OK Ca	ncel
	Instruction	on encoded succe	essfully!

Search for fread, fwrite and Encryption

🗹 🖼					
007FF7674180DB					
007FF7674180DB loc_7F	F7674180DB:				
007FF7674180DB movsxd	l rax, ecx				
007FF7674180DE lea	rcx, [rbx+41h]]			
007FF7674180E2 add	rcx, rax	; DstBuf			
007FF7674180E5 mov	r9, [rsp+530h-	+var_4D8] ; F	File		
007FF7674180EA mov	r8, rdi	; Count			
007FF7674180ED mov	edx, 1	; ElementS	Size		
007FF7674180F2 call	fread				
007FF7674180F7 cmp	rax, rdi				
007FF7674180FA jz	short loc_7FF	76741813E			
		_	•		
	🗾 🗹 🧕	2			
	00007FF	76741813E			
	00007FF	76741813E lo	c_7FF7674	1813E:	; File
	00007FF	76741813E mo	ov rex	, [rsp+530h+	var_4D8]
	00007FF	767418143 ca	all fcl	ose	
	00007FF	767418148 mo	ov [rs	p+530h+var_4	F8], 1
	00007FF	767418150 mo	ov [rs	p+530h+var_5	08], 40000000h
	00007FF	767418158 mo	ov [rs	p+530h+var_5	10], r15
	00007FF	76741815D mo	ov r9d	, 100h	
	00007FF	767418163 le	ea n8,	[rbp+430h+v	ar_260]
	00007FF	76741816A mo	ov edx	, esi	
	00007FF	76741816C mo	ov rex	, rbx	
	00007FF	76741816F ca	all <mark>sub</mark>	_7FF7673F924	<mark>0</mark>
	00007FF	767418174 ad	id [r1	3+0], esi	
	00007FF	767418178 mo	ov rex	, [rsp+530h+	File] ; File
	00007FF	76741817D ca	all _ft	elli64	
	00007FF	767418182 mo	ov r9,	[rsp+530h+F	ile] ; File
	00007FF	767418187 mo	ov r8,	r12	; Count
	00007FF	76741818A mo	ov edx	, 1	; Size
	00007FF	76741818F mo	ov rex	, rbx	; Str
	00007FF	767418192 ca	all fwr	ite	
	00007FF	767418197 mo	ov rex	, r15	; Memory
	00007FF	76741819A cm	np rax	, r12	
	00007FF	76741819D jz	z sho	rt loc_7FF76	74181DF

Stepping Over Function Call

	Address	He	<															ASCII
	0000020B685018E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	0000020B685018F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	0000020B68501900	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	0000020B68501910	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	0000020B68501920	73	65	63	72	65	74	2E	74	78	74	00	41	41	41	41	41	secret.txt.AAAAA
	0000020B68501930	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
	0000020B68501940	41	41	41	41	41	41	41	OD	0A	41	41	41	41	41	41	41	АААААААААААААА
	0000020B68501950	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
	0000020B68501960	41	41	41	41	41	OD	0A	41	41	41	41	41	41	41	41	41	АААААААААААААА
	0000020B68501970	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
	0000020B68501980	41	41	41	OD	0A	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAA
	0000020B68501990	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA
	0000020B685019A0	41	OD	0A	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAA
	0000020868501980	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	OD	АААААААААААААААА
h	Address	He)	<u>(</u>	_	_			_	_				_			_	_	ASCTT
þ	Address	He)	(E6	AP	67	D1	17	05	65	20	84	5.9	00		2.4	56	69	ASCII
	Address 0000020B685018E0 0000020B685018E0	He)	E6	AB	C7	D1	17	0F	65	38	8A	59	00	12	34	F6	C9	ASCII
	Address 00000208685018E0 00000208685018F0 0000020868501900	He) 3F 85 FF	E6 2D 5D	AB 05	C7 F0	D1 A2 37	17 18 FF	0F 5D 63	65 E6	3B B3 D4	8A 6D	59 37 4F	00 99 38	12 F4	34 51 54	F6 68	C9 47 89	ASCII ?æ«ÇŇe;.Y4öÉ ô¢.]æ*m7.ôQhG blót7îc.Ô\oTa
	Address 00000208685018E0 00000208685018F0 0000020868501900 0000020868501910	He) 3F 85 FE 85	E 6 2D 5D 05	AB 05 F3	C7 F0 54	D1 A2 37 92	17 18 EE 25	0F 5D 63	65 E6 86	3B B3 D4 32	8A 6D 5C 21	59 37 AF FB	00 99 38 85	12 F4 6F	34 51 54	F6 68 61 73	C9 47 B9	ASCII @æ«ÇÑe;.Y4öĔ ô¢.]æ*m7.ôQhG þ]óT7îc.ô\;;oTa'
	Address 0000020B685018E0 0000020B685018F0 0000020B68501900 0000020B68501910 0000020B68501920	He) 3F 85 FE 85 26	E6 2D 5D 05 A3	AB 05 F3 C5 F9	C7 F0 54 E9 25	D1 A2 37 92 00	17 18 EE 25 AF	0F 5D 63 C1 04	65 E6 86 9D	3B B3 D4 32 D0	8A 6D 5C 21 E2	59 37 AF EB 08	00 99 38 BF A5	12 F4 6F 60 23	34 51 54 A1 9F	F6 68 61 73 40	C9 47 89 39	ASCII ?æ«ÇÑe;.Y4öé ô¢.]æ*m7.ôQhG þ]óT7îc.ô\ ;oTa' Áé.%Á.2!ë¿`is9 &fé%_epå.¥#.@¥
	Address 0000020B685018E0 0000020B685018F0 0000020B68501900 0000020B68501920 0000020B68501920	He) 3F 85 FE 85 26 CC	E6 2D 5D 05 A3 C7	AB 05 F3 C5 E9 FC	C7 F0 54 E9 25 AF	D1 A2 37 92 00 3F	17 18 25 AE FA	0F 5D 63 C1 04 6D	65 E6 86 9D 11 0D	3B B3 D4 32 D0 4F	8A 6D 5C 21 E2 E6	59 37 AF EB 08 BC	00 99 38 BF A5 30	12 F4 6F 60 23 31	34 51 54 A1 9F 92	F6 68 61 73 40 76	C9 47 B9 39 A5 07	ASCII ?æ«ÇÑe;.Y4öÉ 0¢.]æ*m7.ôQhG þ]óT7îc.0_;oTa' Aé.%Á.2!ë¿`is9 &fé%.®Dâ.¥#.@¥ Tcì~?úm.Næ%<1.V.
	Address 00000208685018E0 00000208685018F0 0000020868501900 0000020868501920 0000020868501920 0000020868501930	He) 3F 85 FE 85 26 CC 4B	E6 2D 5D 05 A3 C7 64	AB 05 F3 C5 E9 EC A1	C7 F0 54 E9 25 AF 8C	D1 A2 37 92 00 3F 3F	17 18 25 AE FA 97	0F 5D 63 C1 04 6D 9F	65 E6 86 9D 11 0D AA	3B B3 D4 32 D0 4E 36	8A 6D 5C 21 E2 E6 6B	59 37 AF EB 08 BC AB	00 99 3B BF A5 3C 61	12 F4 6F 60 23 31 BF	34 51 54 A1 9F 92 CC	F6 68 61 73 40 76 88	C9 47 B9 39 A5 07 0A	ASCII @æ«ÇŇe;.Y4öÉ ô¢.]æ*m7.ôQhG þ]óT7îc.ô\~;oTa' Áé.%Á.2!ë¿`is9 &fé%.®Dâ.¥#.@¥ İÇì ?úm.Næ%<1.v. Kdi.?6k«a;I.v.
	Address 00000208685018E0 00000208685018F0 0000020868501900 0000020868501920 0000020868501930 0000020868501940 0000020868501940	He) 3F 85 FE 85 26 CC 4B 24	E6 2D 5D 05 A3 C7 64 68	AB 05 F3 C5 E9 EC A1 9C	C7 F0 54 E9 25 AF 8C F6	D1 A2 37 92 00 3F 3F C2	17 18 25 AE FA 97 8F	0F 5D 63 C1 04 6D 9F CD	65 E6 9D 11 0D AA 46	3B B3 D4 32 D0 4E 36 98	8A 6D 5C 21 E2 E6 6B 88	59 37 AF EB 08 BC AB F5	00 99 3B BF A5 3C 61 DA	12 F4 6F 60 23 31 BF 16	34 51 54 A1 9F 92 CC E0	F6 68 61 73 40 76 88 F4	C9 47 B9 39 A5 07 0A F0	ASCII @æ«ÇŇe;.Y4öÉ ò¢.]æ*m7.ôQhG þ]óT7îc.ô\;oTa' Áé.%Á.2!ë¿`;s9 &fé%.®Dâ.¥#.@¥ ÌÇì?úm.Næ¼<1.v. Kdį.?ª6k«a¿l \$h.öÅ.IFöÚ.àòã
	Address 00000208685018E0 00000208685018F0 0000020868501900 0000020868501910 0000020868501920 0000020868501930 0000020868501940 0000020868501950	He) 3F 85 FE 85 26 CC 4B 24 59	E6 2D 5D 05 A3 C7 64 68 7E	AB 05 F3 C5 E9 EC A1 9C 6B	C7 F0 54 E9 25 AF 8C F6 9A	D1 A2 37 92 00 3F 3F C2 0D	17 18 25 AE 54 97 8F 47	0F 5D 63 C1 04 6D 9F CD 19	65 E6 9D 11 0D AA 46 74	3B B3 D4 32 D0 4E 36 98 E2	8A 6D 5C 21 E2 E6 6B 88 6B	59 37 AF EB 08 BC AB F5 47	00 99 3B BF A5 3C 61 DA D5	12 F4 6F 23 31 BF 16 91	34 51 54 9F 92 CC E0 C0	F6 68 61 73 40 76 88 F4 CA	C9 47 B9 39 A5 07 0A F0 97	ASCII @æ«ÇÑe;.Y4öĔ ô¢.]æ*m7.ôQhG þ]óT7îc.ô\;oTa' .Aé.%A.2!ē¿`is9 &fé%.®Dâ.¥#.@¥ İÇì?ûm.Næ%<1.v. Kdi.?a6k«a¿I \$h.öÅ.İFõÙ.àôđ Y~ks.tākgŎ.AĚ.
	Address 00000208685018E0 00000208685018F0 0000020868501900 0000020868501920 0000020868501920 0000020868501930 0000020868501940 0000020868501950 0000020868501960	He) 3F 85 FE 85 26 CC 4B 24 59 02	E6 2D 5D 05 A3 C7 64 68 7E 70	AB 05 F3 C5 E9 EC A1 9C 6B A0	C7 F0 54 E9 25 AF 8C F6 9A CC	D1 A2 37 92 00 3F 3F C2 0D 51	17 18 25 AE FA 97 8F A7 FC	0F 5D 63 C1 04 6D 9F CD 19 85	65 E6 9D 11 0D AA 46 74 75	3B B3 D4 32 D0 4E 36 98 E2 DD	8A 6D 5C 21 E2 E6 6B 88 6B 6B	59 37 AF EB 08 BC AB F5 47 FB	00 99 38 BF 30 61 DA D5 02	12 F4 6F 60 23 31 BF 16 91 81	34 51 54 A1 9F 92 CC E0 C0 86	F6 68 61 73 40 76 88 F4 CA 41	C9 47 B9 39 A5 07 0A F0 97 3C	ASCII @æ«ÇÑe;.Y4öĔ ô¢.]æ*m7.ôQhG þ]óT7îc.ô\~;oTa' .Aé.%A.2!ë¿`;s9 &fé%.@Dâ.¥#.@¥ İÇì~?úm.Næ%<1.v. Kd;.?ª6k«a;l \$h.öA.1Fôú.àôđ Y~k§.tàkgð.AÊ. .p IQūµuÝkûAč
	Address 00000208685018E0 0000020868501900 0000020868501900 0000020868501920 0000020868501930 0000020868501930 0000020868501940 0000020868501950 0000020868501970	He) 3F 85 FE 85 26 CC 4B 24 59 02 23	E6 2D 5D 05 A3 C7 64 68 7E 70 37	AB 05 F3 C5 E9 EC A1 9C 6B A0 C3	C7 F0 54 E9 25 AF 8C F6 9A CC 7D	D1 A2 37 92 00 3F 3F C2 0D 51 4E	17 18 25 AE FA 97 8F A7 FC 9A	0F 5D 63 C1 04 6D 9F CD 19 85 98	65 E6 9D 11 0D AA 46 74 75 48	3B B3 D4 32 D0 4E 36 98 E2 DD BC	8A 6D 5C 21 E2 E6 6B 88 6B 6B DB	59 37 AF EB 08 BC AB F5 47 FB 14	00 99 3B BF A5 3C 61 DA D5 02 86	12 F4 6F 60 23 31 BF 16 91 81 3A	34 51 54 41 9F 92 CC E0 C0 86 81	F6 68 61 73 40 76 88 F4 CA 41 7D	C9 47 B9 39 A5 07 0A F0 97 3C 80	ASCII 2æ«ÇÑe;.Y4öÉ ô¢.]æ°m7.ôQhG þ]óT7îc.ô\`;oTa' .Áé.%Á.2!ë¿`;s9 &fé%.@.Dâ.¥#.@¥ İÇì?úm.Næ4<1.v. Kd;.?.°6k«a;İ \$h.öÅ.IFöÚ.àôđ Y~k§.tâkGÔ.ÀÊ. .p IQܵµÝkûA
	Address 00000208685018E0 0000020868501900 0000020868501910 0000020868501920 0000020868501930 0000020868501940 0000020868501950 0000020868501950 0000020868501970 0000020868501990	He) 3F 85 FE 85 26 CC 4B 24 59 02 23 5B	E6 2D 5D 05 A3 C7 64 68 7E 70 37 00	AB 05 F3 C5 E9 EC A1 9C 6B A0 C3 BC	C7 F0 54 E9 25 AF 8C F6 9A CC 7D 33	D1 A2 37 92 00 3F 3F C2 0D 51 4E 95	17 18 25 AE FA 97 8F A7 FC 9A 35	0F 5D 63 C1 04 6D 9F CD 19 B5 98 61	65 E6 9D 11 0D AA 46 74 75 48 B5	3B B3 D4 32 D0 4E 36 98 E2 DD BC C9	8A 6D 5C 21 E2 6B 88 6B 6B 6B 5B FB	59 37 AF EB 08 BC AB F5 47 FB 14 64	00 99 3B 8F 45 3C 61 DA D5 02 86 45	12 F4 6F 60 23 31 BF 16 91 81 3A DF	34 51 54 A1 9F 92 CC E0 C0 86 81 A5	F6 68 61 73 40 76 88 F4 CA 41 7D AD	C9 47 B9 39 A5 07 0A F0 97 3C 80 07	ASCII ?æ«ÇÑe;.Y4öé ô¢.]æ*m7.ôQhG þ]óT7îc.ô\`;oTa' Aé.%Á.2!ë¿`;s9 &fé%.@Dà.¥#.@¥ Içì~?úm.Næ4<1.v. Kd;.?ª6k«a;1 \$h.öA.1FôÚ.àôô Y~k§.tâkGÕ.AÊ. .p IQܵuÝkûA< #7Å}NH%D.:.}.
	Addr ess 00000208685018E0 0000020868501900 0000020868501900 0000020868501920 0000020868501930 0000020868501940 0000020868501950 0000020868501960 0000020868501980 0000020868501980	He) 3F 85 FE 85 26 CC 4B 24 59 02 23 58 E9	E6 2D 5D 05 A3 C7 64 68 7E 70 37 00 D0	AB 05 F3 C5 E9 EC A1 9C 6B A0 C3 BC 98	C7 F0 54 E9 25 AF 8C F6 9A CC 7D 33 F8	D1 A2 37 92 00 3F 3F C2 0D 51 4E 95 24	17 18 25 AE FA 97 8F A7 FC 35 80	0F 5D 63 C1 04 6D 9F CD 19 85 98 61 29	65 E6 9D 11 0D AA 46 74 75 48 B5 B5	3B B3 D4 32 D0 4E 36 98 E2 DD BC C9 DE	8A 6D 5C 21 E2 6B 88 6B 5B FB 41	59 37 AF EB 08 BC AB F5 47 FB 14 64 3C	00 99 3B A5 3C 61 DA D5 02 86 45 75	12 F4 6F 60 23 31 BF 16 91 3A DF 7B	34 51 54 9F 92 CC E0 C0 86 81 A5 17	F6 68 61 73 40 76 88 F4 CA 41 7D AD 32	C9 47 B9 39 A5 07 0A F0 97 3C 80 07 B1	ASCII [æ«ÇÑe;.Y4öέ ô¢.]æ*m7.ôQhG þ]óT7îc.ô\`;oTa' Âé.%Å.2!ë¿`;s9 &£é%.@Dâ.¥#.@¥ lçì~?úm.Næ%<1.v. Kd;.?*Gk.«a;l \$h.öÅ.İFõÙ.àôð Y~k§.tàkgÕ.ÅÊ. .p lQüµuÝkûA< #7Å}NH¾0.:.} [.¼3.5aµÉûdEߥ éĐ.@\$.)µÞA <u{.2}< td=""></u{.2}<>

Generates single byte keystream



XOR 1 byte plaintext with 1 byte keystream

Symmetric Encryption

- Ciphertext is deterministic:
 - Same inputs create same outputs.
- Encryption is performed by xor...
 - ... so we can "decrypt" by xoring again!
- We have symmetric encryption!

Extract Ciphertext, Create New LockBox

0000022001010100	1.10																www.www.ubububub
000001E3043494D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E3043494E0	EE	FE	EE	FE	EE	FE	EE	FE	EB	62	3F	F9	7D	4B	08	35	îþîþîþîþëb?ù}K.5
000001E3043494F0	3F	E6	AB	C7	D1	17	0F	65	3B	8A	59	00	12	34	F6	C9	?æ«ÇÑe;.Y4öÉ
000001E304349500	85	2D	05	FO	A2	18	5D	E6	B3	6D	37	99	F4	51	68	47	.–.ð¢.]æ⁼m <u>7</u> .ôQhG
000001E304349510	FE	5D	F3	54	37	EE	63	86	D4	5C	AF	3B	6F	54	61	B9	þ]óT7îc.Ô\¨;oTa'
000001E304349520	85	05	C5	E9	92	25	C1	9D	32	21	EB	BF	60	A1	73	39	Aé.%A.2!ë¿`is9
000001E304349530	01	AF	E7	32	29	B5	49	0E	86	C 0	4B	8C	03	B2	6D	81	. ç2)µIÀK≞m.
000001E304349540	E3	Ε1	C8	CO	28	8A	02	79	21	F7	8F	14	06	B2	43	23	ãáÈÀ(y!÷⁼C#
000001E304349550	41	40	99	9F	1B	A1	BF	D5	58	04	9E	58	8A	8D	93	24	A@;¿ÖXX\$
000001E304349560	10	09	B5	D6	F5	AB	AC	74	AC	AA	D7	FE	24	D2	D3	C4	µÖõ≪¬t¬ª×þ\$ÒÓÃ
000001E304349570	74	53	53	FB	2F	C5	7E	45	CF	4F	72	F1	B4	A1	FF	BE	tSSû/Â~EÏOrñ_iÿ%
000001E304349580	26	11	B5	E4	7D	D8	B8	5 B	FF	41	9A	15	F1	E9	35	5D	&.μä}Ø [ÿΑñé5]
000001E304349590	01	1E	E3	1C	28	BE	B7	6E	98	Β4	58	CD	76	CA	75	E6	ã.(≯ n. XÍvÊuæ
000001E3043495A0	77	61	99	OB	BD	1A	47	D4	FC	D5	05	6F	FO	8B	9B	66	wa%.GÔüÔ.oôf
000001E3043495B0	C0	B2	E5	99	1C	AE	1D	D4	FB	69	19	14	53	22	5D	FD	A⁼å⊜.Ôûis"]ý
000001E3043495C0	C0	61	C4	ED	1A	A5	C 0	23	E8	OD	ЗE	07	CF	16	37	E9	ÀaÄí.¥ <u>À</u> #è.>.Ï.7é
000001E3043495D0	13	86	5E	97	77	76	AF	60	CA	FF	44	A5	78	2E	BA	34	^.wv ÈÿD¥x.∘4
000001E3043495E0	DC	FB	60	F9	41	4C	AD	8D	34	F7	D4	36	70	79	14	CA	Üü`ùAL4÷Ô6py.Ē
000001E3043495F0	FF	9B	AC	B1	C3	DO	FO	ЗA	58	95	34	7B	EF	9B	28	CE	ÿ.¬±ÅÐð:X.4{ï.(Î
000001E304349600	92	AA	49	29	EO	AF	5 B	82	42	10	93	A5	2D	65	75	75	.•I)a [.B¥-euu
000001E304349610	C0	F6	73	2D	65	B1	1F	1D	6B	56	48	F1	ED	65	80	74	Aös-e±kVHñie.t
000001E304349620	ЗA	49	EF	A5	OC.	DE	C6	FD	C4	9B	F0	4B	2F	76	A7	F8	:Iï¥.ÞÆýÄ.ðK/v§ø
000001E304349630	75	B0	45	B3	31	03	CC	F9	11	F3	7C	58	31	78	41	CB	u°E*1.Ìù.ó X1XAÉ
000001E304349640	7A	4E	E9	27	2B	E8	30	29	70	OB	0E	4E	0A	64	FF	B8	zNé'+èO)pN.dÿ
000001E304349650	B6	A5	A1	02	4B	64	82	6A	F2	8A	27	FA	70	62	DC	D6	¶¥i Kd jò 'úpbÜÖ
000001E304349660	EO	70	81	B8	C7	49	26	4D	01	12	FF	5 F	FB	3D	10	B6	ap. CI&M. ÿ_û=.¶
000001E304349670	62	BD	60	83	GD	A7	31	D3	CO	Ε1	FB	74	05	DC	5 B	A1	b½`.m§1ÓAáût.Ü[;
000001E304349680	7B	C1	50	1E	9E	7A	D7	BD	F2	17	9C	08	48	22	29	67	{APzx%oH")g
000001E304349690	4A	EB	6E	4A	95	4B	AD	D0	F3	DB	1A	93	5A	F7	F6	16	JënJ.K.ĐóŲZ÷ö.
000001E3043496A0	6A	A2	56	54	5 B	7F	29	46	C1	C4	81	29	1F	7C	CA	A2	j¢VT[.)FAA.). Ē¢
000001E3043496B0	54	11	00	83	D9	25	29	CA	39	51	08	Ε4	A3	E6	6D	0C	TÙ%)Ê9Q.䣿m.
000001E3043496C0	7F	77	45	DO	BE	89	C9	2C	63	74	9D	79	67	63	2D	EE	.wED% É,ct.ygc-î
000001E3043496D0	0E	69	9A	4B	77	F1	OB	75	EE	87	79	2E	EO	57	9F	D9	.i.Kwñ.uî.y.àW.Ù
000001E3043496E0	7E	31	D8	66	32	58	ЗD	FF	3B	2C	14	9F	56	1B	83	24	~10f2X=ÿ;,V\$
000001E3043496F0	3E	F7	70	A9	57	60	33	A0	0E	45	CB	3F	84	96	2D	9B	>÷p@W`3_EË?
000001E304349700	26	44	0D	30	43	55	77	38	76	B9	FO	09	A7	ЗA	8C	D4	&D.OCUW8∨`∂.§:.Ô
000001E304349710	49	0A	A6	6A	9C	11	22	B2	74	C6	8A	FC	C8	9A	EE	85	I.¦j"≣tÆ.üÈ.î.
000001E304349720	7B	OD	64	BB	87	63	7E	07	25	03	DD	AB	AB	AB	AB	AB	{.d».c~.%.Y«««««
000001E304349730	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	FE	EE	FE	EE	FE	««««««««««»»»)
0000015204240740	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Address	He	x															ASCII
000001E3048732A0	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	00	00	00	00	00	00	«««««««««
000001E3048732B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E3048732C0	00	00	00	00	00	00	00	00	AO	62	3F	B2	72	4B	28	32	b?=rK(2
000001E3048732D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E3048732E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E3048732F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E304873300	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E304873310	73	65	63	72	65	74	32	2E	74	78	74	00	41	41	41	41	secret2.txt.AAAA
000001E304873320	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
000001E304873330	41	41	41	41	41	41	41	41	0D	0A	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E304873340	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E304873350	41	41	41	41	41	41	0D	0A	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E304873360	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E304873370	41	41	41	41	OD	0A	41	41	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E304873380	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
000001E304873390	41	41	0D	0A	41	41	41	41	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E3048733A0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E3048733B0	0D	0A	41	41	41	41	41	41	41	41	41	41	41	41	41	41	
000001E3048733C0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
000001E3048733D0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E3048733E0	41	41	41	41	41	41	41	41	41	41	0D	0A	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E3048733F0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
000001E304873400	41	41	41	41	41	41	41	41	0D	0A	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E304873410	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
000001E304873420	41	41	41	41	41	41	0D	0A	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E304873430	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E304873440	41	41	41	41	OD	0A	41	41	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E304873450	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E304873460	41	41	0D	0A	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAA
000001E304873470	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E304873480	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E304873490	41	41	41	41	41	41	41	41	41	41	41	41	OD	0A	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E3048734A0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E3048734B0	41	41	41	41	41	41	41	41	41	41	OD	0A	41	41	41	41	АААААААААААААА
000001E3048734C0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА
000001E3048734D0	41	41	41	41	41	41	41	41	OD	0A	41	41	41	41	41	41	AAAAAAAA AAAAAA
000001E3048734E0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА
000001E3048734F0	41	41	41	41	41	41	OD	0A	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
000001E304873500	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA
000001E304873510	41	41	41	41	OD	OA	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAA

Replace Dummy Data With Ciphertext

	ampe eessamps	and points .	
Address	Hex		Hex:
000001E3048732A0	AB AB AB AB AB AB	AB AB AB	92 AA 49 29 E0 AE 58 82 42 10 93 A5 20 65 75 75
000001E3048732B0	0 00 00 00 00 00 00	00 00 00	CO EG 73 2D G5 B1 1E 1D GB 56 48 E1 ED G5 80 74
000001E3048732C0	0 00 00 00 00 00 00	00 00 A0	34 49 FE AS OC DE C6 FD C4 98 FO 48 2E 76 A7 F8
000001E3048732D0	00 00 00 00 00 00 00	00 00 00	75 B0 45 B3 31 03 CC E9 11 E3 7C 58 31 78 41 CB
000001E3048732E0	00 00 00 00 00 00 00	00 00 00	74 46 59 27 28 58 20 29 70 08 06 46 04 64 56 88
000001E3048732F0	00 00 00 00 00 00 00	00 00 00	R6 45 41 02 48 64 82 64 F2 84 27 F4 70 62 DC D6
000001E304873300	00 00 00 00 00 00	00 00 00	E0 70 81 88 C7 49 26 4D 01 12 EE 55 ER 3D 10 86
000001E304873310	73 65 63 72 65 74	32 2E 74	
000001E304873320	41 41 41 41 41 41 41	41 41 41	
000001E304873330	41 41 41 41 41 41	41 41 OD	
000001E304873340	41 41 41 41 41 41	41 41 41	4A EB 6E 4A 55 4B AD DO F5 DB 1A 55 5A F7 F6 16
000001E304873350	41 41 41 41 41 41 41	OD 0A 41	54 11 00 82 D9 25 29 C4 29 51 08 54 42 56 60 0C
000001E304873360	41 41 41 41 41 41 41	41 41 41	75 77 45 D0 PE 29 C9 20 62 74 9D 79 67 63 20 55
000001E304873370	41 41 41 41 0D 0A	41 41 41	0E 69 94 49 77 E1 09 7E EE 97 79 2E E0 E7 9E D9
000001E304873380	41 41 41 41 41 41 41	41 41 41	7 51 D 6 6 33 E 6 7 E 5 D E 5 2 3 14 5 E 6 3 7 3 24
000001E304873390	41 41 0D 0A 41 41	41 41 41	7E 51 D0 00 52 50 5D FF 5B 2C 14 5F 50 1B 65 24
000001E3048733A0	41 41 41 41 41 41	41 41 41	36 44 0D 20 42 55 77 28 76 P9 50 09 47 24 80 D4
000001E3048733B0	OD 0A 41 41 41 41	41 41 41	40 00 AC CA OC 11 22 P2 74 CC PA EC CP 04 EE PE
000001E3048733C0	41 41 41 41 41 41	41 41 41	47 0A A0 6A 9C 11 22 62 /4 C0 6A FC C0 5A EE 65
000001E3048733D0	41 41 41 41 41 41	41 41 41	
000001E3048733E0	41 41 41 41 41 41	41 41 41	
000001E3048733F0	41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 41 41 41 41 41 41 41 4
000001E304873400	41 41 41 41 41 41	41 41 OD	
000001E304873410	41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 41 41 41 41 41 41 41 4
000001E304873420	41 41 41 41 41 41	OD 0A 41	41 41 41 41 41 41 41 41 41 41 41 41 41 4
000001E304873430	41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 41 41 41 41 41 41 40 00 0A 41 41
000001E304873440	41 41 41 41 0D 0A	41 41 41	
000001E304873450	41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 41 41 41 41 41 00 0A 41 41 41 41
000001E304873460	41 41 0D 0A 41 41	41 41 41	41 41 41 41 41 41 41 41 41 41 41 41 41 4
000001E304873470	41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 41 41 0D 0A 41 41 41 41 41 41
000001E304873480	41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 41 41 41 41 41 41 41 4
000001E304873490	41 41 41 41 41 41	41 41 41	
000001E3048734A0	41 41 41 41 41 41	41 41 41	
000001E3048734B0	41 41 41 41 41 41	41 41 41	Keep Size
000001E3048734C0	41 41 41 41 41 41	41 41 41	
000001E3048734D0	41 41 41 41 41 41	41 41 0D	UA 41 41 41 41 41 41 AAAAAAAAAAAAAA
000001E3048734E0	41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAA
000001E3048734F0	41 41 41 41 41 41	OD 0A 41 4	41 41 41 41 41 41 41 AAAAAAAAAAAAAA
000001E304873500	41 41 41 41 41 41 41	41 41 41	41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA
000001E304873510	41 41 41 41 0D 0A	41 41 41	41 41 41 41 41 41 41 AAAAAAAAAAAAAAA
0000015204872520	41 41 41 41 41 41 41	41 41 41	00000000000000000000000000000000000000

Address	He	¢.															ASCII
000001E3048732A0	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	00	00	00	00	00	00	«««««««««
000001E3048732B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E3048732C0	00	00	00	00	00	00	00	00	A0	62	ЗF	B2	72	4B	28	32	b?=rK(2
000001E3048732D0	3F	E6	AB	C7	D1	17	0F	65	3B	8A	59	00	12	34	F6	C9	?æ«ÇŇe;.Y4öÉ
000001E3048732E0	85	2D	05	F0	A2	18	5D	E6	В3	6D	37	99	F4	51	68	47	.–.ð¢.]æ⁼m7.ôQhG
000001E3048732F0	FE	5D	F3	54	37	EE	63	86	D4	5C	AF	3B	6F	54	61	В9	þ]óT7îc.Ô\ˈ;oTaː
000001E304873300	85	05	C5	E9	92	25	C1	9D	32	21	EB	BF	60	A1	73	39	Åé.%Å.2!ë¿`is9
000001E304873310	01	AF	E7	32	29	B5	49	0E	86	C 0	4B	8C	03	B2	6D	81	. c2)µIÀK≖m.
000001E304873320	E3	Ε1	C8	C 0	28	8A	02	79	21	F7	8F	14	06	B2	43	23	ãáÉÀ(y!÷⁼C#
000001E304873330	41	40	99	9F	1B	A1	BF	D5	58	04	9E	58	8A	8D	93	24	A@;¿ŎXX\$
000001E304873340	10	09	B5	D6	F5	AB	AC	74	AC	AA	D7	FE	24	D2	D3	C4	µÖõ«¬t¬ª×þ\$ÒÓÄ
000001E304873350	74	53	53	FB	2F	C5	7E	45	CF	4F	72	F1	B4	A1	FF	BE	tSSû/Â~EÏOrñ´;ÿ%
000001E304873360	26	11	B5	Ε4	7D	D8	88	5 B	FF	41	9A	15	F1	Ε9	35	5D	&.µä}Ø_[ÿAñé5]
000001E304873370	01	1E	E3	1C	28	BE	B7	6E	98	Β4	58	CD	76	CA	75	E6	ã.(¾∙n. XÍvÊuæ
000001E304873380	77	61	99	0B	BD	1A	47	D4	FC	D5	05	6F	F0	8B	9B	66	wa½.GÔüÔ.oðf
000001E304873390	C0	B2	E5	99	1C	AE	1D	D4	FB	69	19	14	53	22	5D	FD	A⁼å⊜.Ôûis"]ý
000001E3048733A0	C0	61	C4	ED	1A	A5	C 0	23	E8	0D	3E	07	CF	16	37	E9	AaÄí.¥A#è.>.Ï.7é
000001E3048733B0	13	86	5 E	97	77	76	AF	60	CA	FF	44	A5	78	2E	BA	34	^.wv [™] `ÊÿD¥x.º4
000001E3048733C0	DC	FB	60	F9	41	4C	AD	8D	34	F7	D4	36	70	79	14	CA	Üû`ùAL4÷Ô6py.Ê
000001E3048733D0	FF	9B	AC	B1	C3	DO	F0	ЗA	58	95	34	7B	EF	9B	28	CE	ÿ.¬±ÅÐð:X.4{ï.(Î
000001E3048733E0	92	AA	49	29	EO	AF	5 B	82	42	10	93	A5	2D	65	75	75	.ªI)a [.B¥-euu
000001E3048733F0	C0	F6	73	2D	65	Β1	1F	1D	6B	56	48	F1	ED	65	80	74	Aös-e±kVHñie.t
000001E304873400	3A	49	EF	A5	0C	DE	C6	FD	C4	9B	F0	4B	2F	76	A7	F8	:Iï¥.ÞÆýÄ.∂K/v§ø
000001E304873410	75	BO	45	В3	31	03	CC	F9	11	F3	7C	58	31	78	41	CB	u°E⁼1,Ìù.ó X1xAË
000001E304873420	7A	4E	Ε9	27	2B	E8	30	29	70	OB	0E	4E	0A	64	FF	B8	zNé'+èO)pN.dÿ
000001E304873430	B6	A5	A1	02	4B	64	82	6A	F2	8A	27	FA	70	62	DC	D6	¶¥i.Kd.jò.'úpbÜÖ
000001E304873440	EO	70	81	88	C7	49	26	4D	01	12	FF	5 F	FB	3D	10	B6	àp. ÇI&Mÿ_û=.¶
000001E304873450	62	BD	60	83	GD	A7	31	D3	C 0	Ε1	FB	74	05	DC	5 B	A1	b½`.m§1ÓÀáùt.Ü[i
000001E304873460	7B	C1	50	1E	9E	7A	D7	BD	F2	17	9C	08	48	22	29	67	{ÅPz׉òH")g
000001E304873470	4A	EB	6E	4A	95	4B	AD	D 0	F3	DB	1A	93	5A	F7	F6	16	JënJ.K.ĐóÛZ÷ö.
000001E304873480	6A	A2	56	54	5 B	7F	29	46	C1	C4	81	29	1F	7C	CA	A2	j¢VT[.)FÁÄ.). Ê¢
000001E304873490	54	11	00	83	D9	25	29	CA	39	51	08	Ε4	A3	E6	GD	0C	TÜ%)Ê9Q.䣿m.
000001E3048734A0	7F	77	45	D 0	BE	89	С9	2C	63	74	9D	79	67	63	2D	EE	.wED¾.Ė,ct.ygc-î
000001E3048734B0	0E	69	9A	4B	77	F1	OB	75	EE	87	79	2E	EO	57	9F	D9	.i.Kwñ.uî.y.àW.Ù
000001E3048734C0	7E	31	D8	66	32	58	3D	FF	3B	2C	14	9F	56	1B	83	24	~10f2X=ÿ;,V\$
000001E3048734D0	3E	F7	70	Α9	57	60	33	A0	0E	45	CB	3F	84	96	2D	9B	>÷p©W`3 .EË?,
000001E3048734E0	26	44	OD	30	43	55	77	38	76	89	FO	09	A7	3A	8C	D4	&D.OCUW8v'ð.§:.Ô
000001E3048734F0	49	0A	A6	6A	9C	11	22	B2	74	C6	8A	FC	C8	9A	EE	85	I.¦j"⁼tÆ,üÈ.î.
000001E304873500	7B	OD	64	BB	87	63	7E	07	25	03	DD	41	41	41	41	41	{.d».c~.%.ÝAAAAA
000001E304873510	41	41	41	41	0D	0A	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAA
0000015204872520	4.1	4.1	4.1	4.1	4.1	4.4	4.1	4.1	4.1	4.1	4.1	4.1	4.1	4.1	4.1	4.1	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Commande

Success! Symmetric Encryption Used!

		-	-						÷ .						· ·		
Address	He	C															ASCII
000001E3048732A0	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	00	00	00	00	00	00	««««««««««
000001E3048732B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E3048732C0	00	00	00	00	00	00	00	00	A0	62	ЗF	B2	72	4B	28	32	b?⁼rK(2
000001E3048732D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	· · · · · · · · · · · · · · · · · · ·
000001E3048732E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E3048732F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E304873300	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E304873310	54	69	6D	65	4C	6F	63	6B	2E	56	43	68	61	6C	6C	65	TimeLock.VChalle
000001E304873320	6E	67	65	2E	56	31	2E	35	2E	50	72	69	76	61	74	65	nge.V1.5.Private
000001E304873330	4B	65	79	52	65	77	61	72	64	2E	74	78	74	00	59	6F	KeyReward.txt.Yo
000001E304873340	75	20	68	61	76	65	20	73	75	63	63	65	73	73	66	75	u nave successtu
000001E304873350	6C	6C	79	20	63	6F	6D	70	6C	65	74	65	64	20	74	68	Thy completed th
000001E3048/3360	65	20	54	69	6D	65	4C	6F	63	68	20	56	31	2E	35	20	e IIMELOCK VI.5
000001E3048/33/0	63	68	61	6C	6C	65	6E	67	65	ZE	OD	OA	OD	0A	49	27	challenge
000001E304873380	60	20	64	79	59	6E	57	20	74	65	20	68	6E	51	25	20	how you did it
000001E304873390	68	61	<i></i>	20	79	65	75	20	64	69	64	20	69	74	ZE CA	00	now you all it
000001E3048733A0	UA ZA	20	CD	50	30	76	61	73	24	20	63	51	5E	74	51	24	t ma wias https:
000001E304873360	25	20	50	55	20	25	69	61	SA CZ	20	68	61	62	60	73	SA	//www.plcompchin
000001E3048733D0	65	22	25	62	65	CD CD	25	62	67	CE	74	61	62	74	00	OA	es com/contact
000001E3048733E0	00	04	40	20	77	60	60	60	20	60	61	70	70	60	ec.	70	T will happily
000001E3048733E0	20	72	65	65	GA	20	79	GE	75	20	61	74	20	60	GE	61	send you at lea
000001E304873400	73	74	20	30	25	30	32	20	42	54	43	20	66	6E	72	20	st 0.02 BTC for
000001E304873410	61	20	64	65	74	61	69	6C	65	64	20	72	65	70	6E	72	a detailed report
000001E304873420	74	20	64	65	73	63	72	69	62	69	6E	67	20	68	6E	77	t describing how
000001E304873430	20	79	6F	75	20	63	72	61	63	6B	65	64	20	54	69	6D	vou cracked Tim
000001E304873440	65	4C	6F	63	6B	20	56	31	2E	35	2E	OD	0A	OD	0A	OD	eLock V1.5
000001E304873450	0A	54	69	6D	65	4C	6F	63	6B	20	31	2E	35	20	63	68	.TimeLock 1.5 ch
000001E304873460	61	6C	6C	65	6E	67	65	20	72	65	77	61	72	64	20	70	allenge reward p
000001E304873470	75	62	6C	69	63	20	61	64	64	72	65	73	73	ЗA	20	20	ublic address:
000001E304873480	33	47	42	78	4E	51	74	39	54	63	43	4A	79	68	51	6B	3GBxNQt9TcCJyhQk
000001E304873490	7A	41	76	59	54	70	59	39	37	42	78	6A	33	39	4C	5A	zAvYTpY97Bxj39LZ
000001E3048734A0	58	4C	OD	0A	54	69	6D	65	4C	6F	63	6B	20	31	2E	35	XLTimeLock 1.5
000001E3048734B0	20	63	68	61	6C	6C	65	6E	67	65	20	72	65	77	61	72	challenge rewar
000001E3048734C0	64	20	70	72	69	76	61	74	65	20	61	64	64	72	65	73	d private addres
000001E3048734D0	73	ЗA	20	4B	79	62	32	66	65	77	71	6E	46	4D	53	33	s: Kyb2fewqnFMS3
000001E3048734E0	6D	46	44	35	43	64	42	65	61	34	48	47	66	64	56	57	mFD5CdBea4HGfdVW
000001E3048734F0	33	44	59	62	66	4B	6E	79	5A	69	32	59	70	46	69	35	3DYbfKnyZi2YpFi5
000001E304873500	72	53	56	32	42	79	44	OD	0A	OD	0A	F2	49	OB	9E	DD	rSV2ByDÒIÝ
000001E304873510	A2	89	2A	97	41	17	48	98	F1	95	C6	93	F2	9F	33	C9	¢.*.A.H.ñ.A.o.3É
0000015204072520	A D	01	22	E 4 .	0.0	0.0	E F	20	0.0	0.5	0.2	20	E 7	0.2	A F	25	· · · · · · · · · · · · · · · · · · ·

Looks Promising...

,	Browse For Folder	×
-1 -7	Select folder where TimeLock.VChallenge.V1.5.PrivateKeyReward.txt will be created.	
1X 75	Desktop ^ >	
-5	 >	
(+ 1X (+	LocalLow Roaming Adobe	
	Folder: LockBoxes Make New Folder OK Cancel	



Loot #4

TimeLock.VChallenge.V1.5.PrivateKeyReward - Notepad File Edit Format View Help You have successfully completed the TimeLock V1.5 challenge.

I'm dying to know how you did it.

Please contact me via: https://www.algomachines.com/contact

I will happily send you at least 0.02 BTC for a detailed report describing how you cracked TimeLock V1.5.

TimeLock 1.5 challenge reward public address: 3GBxNQt9TcCJyhQkzAvYTpY97Bxj39LZXL TimeLock 1.5 challenge reward private address: Kyb2fewqnFMS3mFD5CdBea4HGfdVW3DYbfKnyZi2YpFi5rSV2ByD

Lessons Learned:

Vulnerability:

- Symmetric encryption means we could bypass decryption step completely.
- Ability to create lockboxes means we can use known plaintext attacks to find vulnerabilities faster.

How to fix:

- Symmetric encryption does not provide any security if the secrets needed to make keys are available
- Public Private key based encryption schemes should be used instead.
- A trusted third party should be the only one with access to decryption keys.

Challenge #5

TimeLock your digital assets (V1.7 / Challenge #5)

RELEASE

Safely pass your digital assets on to your loved ones

- · Securely lock your data until a time you choose.
- Create LockBoxes up to 10KB.
- TimeLock synced to the Bitcoin Network, using immutable block header timestamp.
- Retain privacy. Your data stays on your computer and nowhere else.
- Distribute your time locked LockBox to whomever you wish.

https://www.algomachines.com/

This is the seventh major version of TimeLock, and the second version anchored to the immutable timestamp of the Bitcoin network.

TimeLock has been improved via a series of challenges. You can see the reports on these challenges here:

https://ruffell.nz/reverse-engineering/writeups/2019/01/18/timelock-analysis-and-vulnerability-writeup.html

https://ruffell.nz/reverse-engineering/writeups/2019/01/28/revisiting-timelock-1-2-vulnerability-writeup.html

https://ruffell.nz/reverse-engineering/writeups/2019/02/18/unleashing-a-sybil-attack-against-timelock-1-3vulnerability-writeup.html

https://ruffell.nz/reverse-engineering/writeups/2019/03/20/double-trouble-with-symmetric-encryption-in-timelock-1-5vulnerability-writeup.html

The program is easy to use, and the free version supports LockBoxes of up to 10 Kbytes.

Plan of Attack

- Review crypto again:
 - See if symmetric encryption is still used.
 - Look for weak algorithms.
 - Look for bad modes of encryption.

Locate Encryption Functions

				• • •	
	🚺 🚄 🔛				
	00007FF7E	FB8EADB			
	00007FF7E	FB8EADB	loc 7FF	7EFB8EADB:	
	00007FF7E	FB8EADB	movsxd	rcx, ecx	
	00007FF7E	FB8EADE	add	rcx, 41h	
	00007FF7E	FB8EAE2	add	rcx, r15	; DstBuf
	00007FF7E	FB8EAE5	mov	r9, [rsp+9C0	h+var_970] ; File
	00007FF7E	FB8EAEA	mov	r8, r14	; Count
	00007FF7E	FB8EAED	mov	edx, 1	; ElementSize
	00007FF7E	FB8EAF2	call	fread	
	00007FF7E	FB8EAF7	cmp	rax, r14	
	00007FF7E	FB8EAFA	jz	short loc_7F	F7EFB8EB40
🚺 🚄 🔛					
00007FF7EFB8EB4	10				
00007FF7EFB8EB4	40 loc_7FF	7EFB8EB4	40:	; File	
00007FF7EFB8EB4	10 mov	rcx, [r	rsp+9C0h	+var_970]	
00007FF7EFB8EB4	45 call	fclose			
00007FF7EFB8EB4	1A mov	ebx, eo	di		
00007FF7EFB8EB4	1C and	ebx, 3			
00007FF7EFB8EB4	4F jz	short]	loc_7FF7	EFB8EB86	

CPU	👰 Grapl	h		Log		ß	Not	es		Br	eak	point	s		Me	mor	y Maj	p		Call St	ack	~	SEH	0	Script	t (🖭 sy	mbols	<>> Sour
			• (0000)7FF	F7E	FB8	EAE	5		4C :	8B40	24	50				mov	r9,	qwore	d ptr	SS:	[rsp	+50					
			•	0000)7FF	E7E	FB8	EAE.	A		4D :	8BC	5	~~				mov	r8,	r14									
			•	0000)7FI	F7E	FB8	EAE	D		BA	010	000	00				mov	edx	,1									
			•	0000)7 F I	F7E	F B S	EAF	4		E8	612.	319	00	_	_	_	call	T1	mero	ск_ра	atche	ea./⊢	+/EF	DZOES	,8	Т	read	
IP		-	•	0000	07 FI	-7E	FB8	EAF	7		49:	3BC	5					cmp	rax	,r14									
	1		•	0000)/ FB	E/E	FB8	EAF	A	× .	<u>/4</u>	44	_					јет	1me	TOCK	_ρατο	ined.	7667	EFBS	EB40				
			-	0000	17 FB	E/E	FB8	EAF	2		48:	SBCI	-	~~				mov	rcx	, 151	- Le					20			
				0000	17	-4E	FB8	EAF	5		Eð	8C 41	-00	00				call	L.	mero	ск_ра	auche	:u./F	F/EF	89292	2 0			
				0000	7	- 4 E	F B B	EBU	-		491	BECI	-	00				mov	LCX	, 115	els as	a the color of							
				0000	7751	-/E	F B B	EBO	2		40.	8441	200	20				Call		mero	CK_pa	accrie	u.//	P/EP	89395	90			
			- L	,	17 10 1	EZ E	r no	P BU			401	00.40		- 10				muv	rt x	- tiwth		12.55	in the second						
		/		<u> </u>																									
r14=139 L'l	Č' 7FF7EFI	B8EA	F7	tim	elo	ock_	_pat	tche	ed.e	exe:	\$28	AF7	#2	DEF	-7									_					
🚚 Dump 1	🦲 D	ump 3	2	.	Du	mp 3	3	٩.,	Dun	np 4			Dum	p 5	1	🤴 V	Vatc	h 1	[x	=l Loca	ls	2 s	truct						
Address		Hex	c i															ASC	II										
0000022064	EA6116	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					•							
00000220648	EA6126	00	00	DD	DF	75	17	46	4D	03	31	00	00	00	00	00	00	Ý	ßu.R	FM.1.									
00000220648	EA6136	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00												
00000220648	EA6146	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00												
00000220648	EA6156	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00												
00000220648	EA6166	00	00	00	00	00	00	00	00	00	00	61	2E	74	78	74	00			a	i.txt								
00000220648	EA6176	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	مممم	AAAA	A							
0000022064	EA6186	41	41	41	41	41	41	41	41	41	41	41	41	0D	0A	41	41	ĀĀĀ	AAA	مممم	AA	A							
00000220648	EA6196	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	مممم	AAAA	A							
00000220648	EA61A6	41	41	41	41	41	41	41	41	41	41	0D	0A	41	41	41	41	AAA	AAA	аааа.	. AAA	A							
00000220648	EA61B6	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	مممم	AAAA	A							
00000220648	EA61C6	41	41	41	41	41	41	41	41	0D	0A	41	41	41	41	41	41	AAA	AAA	AAA	AAAA	A							
0000022064	EA61D6	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	مممم	AAAA	A							
00000220648	EAG1E6	41	41	41	41	41	41	0D	0A	41	41	41	41	41	41	41	41	AAA	AAA.		AAAA	A							
0000022064	EAG1F6	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	مممم	AAAA	A							
0000022064	EA6206	41	41	41	41	OD	0A	41	41	41	41	41	41	41	41	41	41	AAA	A/	مممم	AAAA	A							
0000022064	EA6216	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	مممم	AAAA	A							
00000220648	EA6226	41	41	0D	0A	41	41	41	41	41	41	41	41	41	41	41	41	AA.	. AA/	مممم	AAAA	A							
00000220648	EA6236	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	مممم	AAAA	A							
00000220648	EA6246	OD	0A	41	41	41	41	41	41	41	41	41	41	41	41	41	41	A	AAA	مممم	AAAA	A							
0000022064	EA6256	41	41	41	41	41	41	41	41	41	41	41	41	41	41	OD	0A	AAA	AAA	4444	AAA.								
0000022064	EA6266	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	AAAA	AAAA	A							
0000022064	EA6276	41	41	41	41	41	41	41	41	41	41	41	41	OD	0A	41	41	AAA	AAA	AAAAA	AA	A							
0000022064	EA6286	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAA	AAA	AAAA	AAAA	A							
0000022064	EA6296	41	41	41	41	41	41	41	41	41	41	OD	0A	41	41	41	41	AAA	AAA	AAAA.	. AAA	A							
0000022064	EA62A6	41	41	41	41	41	41	41	41	41	AB	AB	AB	AB	AB	AB	AB	AAA	AAA	AAA««		«							
0000022064	EA62B6	AB	AB	AB	AB	AB	AB	AB	AB	AB	FE	00	00	00	00	00	00	«««	««««	«««þ.									
00000220648	EA62C6	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00												
						_																							



Encryption Rounds One and Three

ADADZEEZEEBSEBCO
00007FF7EFB8EBC0 loc 7FF7EFB8EBC0:
00007FF7EFB8EBC0 imul eax, [rbp+rdx*4+8C0h+var 180], 0CC9E2D51
00007FF7EFB8EBCB rol eax, 0Fh
00007FF7EFB8EBCE imul ecx, eax, 18873593h
00007FF7EFB8EBD4 xor r8d, ecx
0000/FF/EFB8EBD/ rol r8d, 0Dh
00007FF7EFB8EBE2 lea r8d [r8±c8*4]
00007FF7EFB8EBE6 inc rdx
00007FF7EFB8EBE9 jnz short loc 7FF7EFB8EBC0
00007FF7EFB8EBEB btc r8d, 8
00007FF7EFB8EBF0 mov eax, r8d
00007FF7EFB8EBF3 shr eax, 10h
00007FF/EFB8EBF6 XOP eax, r8d
0000/FF/EFDSEDF9 IMUL ECX, EdX, OSEDCAODI
00007FF7EFB8EC01 shr eax, 0Dh
00007FF7EFB8EC04 xor eax, ecx
00007FF7EFB8EC06 imul ecx, eax, 0C2B2AE35h
00007FF7EFB8EC0C mov edx, ecx
00007FF7EFB8EC0E shr edx, 10h
00007FF7EFB8EC11 xor edx, ecx
00007FF7EFB8EC1A iz short loc 7EE7EE88EC23
doddyn yer baccik jz
· · · · · · · · · · · · · · · · · · ·
00007EE7EE88EC1C mov eax, ebx
00007FF7EFB8EC1E sub eax, r12d
00007FF7EFB8EC21 add edx, eax
00007FF7EFB8EC23
00007FF7EFB8EC23 loc_7FF7EFB8EC23:
00007FF7EFB8EC23 and edx, 3FFFFFFFh
10000/FF/EFB8EC2C inz short loc 7EE7EE88EC36
↓
00007FF7EFB8EC2E inc edx
00007FF7EFB8EC30 and edx, 3FFFFFFFh
¥ ¥
0000/FF/EF88EC36
00007171100LC00 IOC_/FF/EFDOCC00:
00007FF7EFB8EC39 movzx eax, byte ptr [rdx+rsi]
00007FF7EFB8EC3D xor [r9], al
00007FF7EFB8EC40 movzx ecx, r10b
00007FF7EFB8EC44 movzx eax, byte ptr [rdx+rsi]
00007FF7EFB8EC48 mov byte ptr [rbp+rcx+8C0h+var_280], al
0000/FF/EF88EL4F Inc F10
00007171100LC52 IIIC 19
00007FF7EFB8EC58 inz loc 7FF7EFB8EBB0

Rounds One and Three are Unchanged, Still Symmetric

Address		He	<															ASCII
0000022064F0	DEFEO	66	DA	E1	21	10 (CF /	AE	26	F0	F6	53	AA	0A	CF	B3	53	fúá!.ï®&ðöSª.ï*S
0000022064F0	DEFFO	36	7E	38	55	7B	9E 7	78	9E	BB	5C	5A	D5	4B	4F	DC	FO	6~8U{.x.»\Z0K0U0
0000022064F0	DF000	EF	B6	EF	EO	C2	E8 E	B9 (C3	25	88	FZ .	AE	13	74	97	87	1111AAe'A%.÷0.t.
0000022064F0	01010	21	93	26	15	08	EA :	52	54	87	CB	5E	DO	56	EA	50	CE	7.V-Eezi.EADVEPI
0000022064F0	E020	°é	27	A1	5	40	60 S		60	65	76	-+0	16	97	20	20	÷2	TA: Ma Uiv0 088
0000022064F0	DE040	33	30	30	3E	FD	83 (00	37	22	40	6E	oc l	17	37	63	22	3<=>17Å@07Å"
0000022064F0	0F050	63	AS	14	9D	AD	A2 4	4C	14	05	32	3E	88	ED	31	D1	45	C¥¢L2>.11ÑE
0000022064F0	0F060	36	72	44	72	53	A0 5	59	2F	11	1B	ED	E4	A2	08	FA	62	GrDrS Y/íä¢.úb
0000022064F0	0F070	C4	D1	EB	8F	10	62 9	94	9E	F6	18	7B	DO	A5	62	22	AЗ	ÄŇëbö.{Đ¥b"£
0000022064F0	0F080	A3	89	7B	0C	35	33 /	A8	05	EF	96	79	13	9F	6F	48	5A	£.{.53".".yoHZ
0000022064F0	0F090	0A	E8	EO	18	AD	28 E	D 3	F7	92	ED	C8	77	11	GD	FC	2F	.ea(O÷.iÈw.mü/
0000022064F0	DFOAO	C3	D2	C0	2C	75	EE E	EC I	D3	DC	6E	AD	ec	CF	64	39	D4	AOA, u110Un. 11d90
0000022064F0	DFOBO	18	DE	8D	F5	B3 (CD 1	15	E5	D5	2D	8C	38	B1	3C	B5	24	
0000022064F0		B/	32	90	80	PE I			ED	22	99	50	F2	31	FA	47	22	V: W U TTOP APER
0000022064F0		22	E4	86	46	14	40 . AE E	10		22	66	40	24	82	6C	55	25	:39' 0000fM = ùA
0000022064F0	FOFO	84	70	10	46	FR (09 3	30	53	AD	D7	A7	47	30	õč l	8F	DA	.]. FÛ. 05. x86=. Ú
0000022064F0	0F100	76	BA	7B	FD	13	7E 9	51	21	oc	1D	94	63	27	34	B1	5E	V°{Ý.~0!c'4±^
0000022064F0	0F110	D8	69	ЗA	63	CO I	F8 /	A5	FB	GD	18	5C	38	C3	3E	13	37	Øi:cAø¥ûm.\8Å>.7
0000022064F0	0F120	34	39	73	25	9C	E8 8	B5	56	39	F5	C6	8B	41	BF	44	CC	495%.èµV9õÆ.A¿DÌ
0000022064F0)F130	D1	BE	D3	96	CC	25 C	C1	FC	FE	12	B1	4F	4F	95	15	1A	Ñ%Ó.1%Äüþ.±00
0000022064F0	0F140	61	30	04	78	94 :	16 1	19	91	8F	EE	D9	03	32	FB	вв	Α4	a0.xî0.2ů»¤
0000022064F0	0F150	03	66	85	E1	EC I	EO S	52	1A	OD	FE	A1	3A	55	97	85	01	.f.a1aRp;:U
0000022064F0	0F160		89	AB	AB			AB .	AB	AB	AB	AB	AB	AB	AB	AB	AB	0'««««««««««««««««««««««
0000022064F0	JF170	AB	AD	EE	FE	EE			FEI	EE	FE	EE	FE	EE	FE	EE	FE	««ipipipipipipipip
	4		_	_	_		_	_	_		_	_	_		_	_	4	
ess	Hex																	ASCII
0220649A9010						00 (00 (00	
0220649A9020						00 (00 (00	
0220649A9030						00 (00 (0				00	
0220649A9040						00 (00 (0				00	
0220649A9050	61 2	2E 7	4 7		74 (41 4	41	41	41	41	. 41	. 4:	1 4	1 4	1 4	1	a.txt.AAAAAAAAAAA
0220649A9060	41 4	11 4	11 4	41	41 4	41 4	41 4	41	41	41	41	. 41	. 4:	1 4	1 4	1 4	11	АААААААААААААА
0220649A9070	41 4	11 0	DD (0A	41 4	41 4	41 4	41	41	41	41	. 41	. 4:	1 4	1 4	1 4	11	ААААААААААААА
0220649A9080	41 4	11 4	11 4	41	41 4	41 4	41 4	41	41	41	41	. 41	. 4:	14	1 4	1 4	11	ААААААААААААААА
0220649A9090	OD 0	DA 4	11 4	41	41 4	41 4	41 4	41	41	41	41	. 41	4:	1 4	1 4	1 4	11	AAAAAAAAAAAAAA
0220649A90A0	41 4	11 4	11 4	41	41 4	41 4	41 4	41	41	41	41	. 41	. 4:	1 4	1 0	DO	A	ААААААААААААА
0220649A90B0	41 4	11 4	11 4	41	41 4	41 4	41 4	41	41	41	41	. 41	. 4:	1 4	1 4	1 4	11	ААААААААААААААА
0220649A90C0	41 4	11 4	11 4	41	41 4	41 4	41 4	41	41	41	41	. 41		0 0	A 4	1 4	11	АААААААААААААА
0220649A90D0	41 4	11 4	11 4	41	41 4	41 4	41 4	41	41	41	41	. 41	. 4:	1 4	1 4	1 4	11	ААААААААААААААА
022064949050	41 4	11 /	11	4-1	11 /	41	41 1	11	11	41	00		111	1 1	1 1	1 1	1 1 1	ΑΛΛΛΛΛΛΛΛΛ ΛΛΛΛ

00000220649A91A0	AB	AB	EE	FE	EE	FE	EE	FE	EE	FE	EE	FE	EE	FE	EE	FE	««ïþïþïþîþîþîþî	
00000220649A9190	00	00	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	«««««««««««««««««	
00000220649A9180	OD	0A	41	41	41	41	41	41	41	41	41	41	41	41	41	00		
00000220649A9170	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA	
00000220649A9160	41	41	OD	0A	41	41	41	41	41	41	41	41	41	41	41	41	AA AAAAAAAAAAAA	
00000220649A9150	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAA	
00000220649A9140	41	41	41	41	OD	0A	41	41	41	41	41	41	41	41	41	41	AAAA AAAAAAAAAAA	
00000220649A9130	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА	
00000220649A9120	41	41	41	41	41	41	0D	0A	41	41	41	41	41	41	41	41	AAAAAA AAAAAAAA	
00000220649A9110	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА	
00000220649A9100	41	41	41	41	41	41	41	41	OD	0A	41	41	41	41	41	41	AAAAAAAA AAAAAA	
00000220649A90F0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	АААААААААААААА	
00000220649A90E0	41	41	41	41	41	41	41	41	41	41	OD	0A	41	41	41	41	AAAAAAAAA AAAA	
00000220649A90D0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ААААААААААААААА	
00000220649A90C0	41	41	41	41	41	41	41	41	41	41	41	41	OD	OA	41	41	AAAAAAAAAAAAAA	
00000220649A90B0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑ	
00000220649A90A0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	OD	0A	AAAAAAAAAAAAAA	
00000220649A9090	OD	0A	41	41	41	41	41	41	41	41	41	41	41	41	41	41		
00000220649A9080	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	ΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑ	
00000220649A9070	41	41	OD	0A	41	41	41	41	41	41	41	41	41	41	41	41	AA AAAAAAAAAAAAAA	
00000220649A9060	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAA	
00000220649A9050	61	2E	74	78	74		41	41	41	41	41	41	41	41	41	41	a.txt.AAAAAAAAAAA	
00000220649A9040																		
00000220649A9030																		
00000220649A9020																		

Encryption Round Two

		•		
🚺 🛃 🖾		-		
00007FF7EFB8ECAD	xor	r8d,	8	
00007FF7EFB8ECB1	mov	eax,	r8d	
00007FF7EFB8ECB4	shr	eax,	10h	
00007FF7EFB8ECB7	xor	eax,	r8d	
00007FF7EFB8ECBA	imul	ecx,	eax,	85EBCA6Bh
00007FF7EFB8ECC0	mov	eax,	ecx	
00007FF7EFB8ECC2	shr	eax,	ØDh	
00007FF7EFB8ECC5	xor	eax,	ecx	
00007FF7EFB8ECC7	imul	ecx,	eax,	0C2B2AE35h
00007FF7EFB8ECCD	mov	ebx,	ecx	
00007FF7EFB8ECCF	shr	ebx,	10h	
00007FF7EFB8ECD2	xor	ebx,	ecx	
00007FF7EFB8ECD4	mov	ecx,	edi	
00007FF7EFB8ECD6	shr	rcx,	1	
00007FF7EFB8ECD9	mov	eax,	4	
00007FF7EFB8ECDE	mul	rcx		
00007FF7EFB8ECE1	CMOVO	rax,	r13	
00007FF7EFB8ECE5	mov	rcx,	rax	
00007FF7EFB8ECE8	call	mallo	c_wr	apper
00007FF7EFB8ECED	mov	r13,	rax	
00007FF7EFB8ECF0	mov	[rbp+	8C0h	+var 908], rax
00007FF7EFB8ECF4	mov	r14,	rax	
00007FF7EFB8ECF7	mov	r8d,	ebx	
00007FF7EFB8ECFA	mov	rax,	5010	7E74251C8553h
00007FF7EFB8ED04	imul	r8		
00007FF7EFB8ED07	sub	rdx,	r8	
00007FF7EFB8ED0A	sar	rdx,	9	
00007FF7EFB8ED0E	mov	rcx,	rdx	
00007FF7EFB8ED11	shr	rcx,	3Fh	
00007FF7EFB8ED15	add	rdx,	rcx	
00007FF7EFB8ED18	imul	rax,	rdx,	2E9h
00007FF7EFB8ED1F	add	r8, r	ax	
00007FF7EFB8ED22	mov	eax,	1	
00007FF7EFB8ED27	CMOVZ	r8, r	ax	
00007FF7EFB8ED2B	xorps	xmm8,	xmm	8
00007FF7EFB8ED2F	cvtsi2ss	s xmm8	, r8	
00007FF7EFB8ED34	divss	xmm8,	CS:	dword_7FF7EFDB4D7
00007FF7EFB8ED3D	shr	edi,	2	
00007FF7EFB8ED40	test	edi,	edi	
00007FF7EFB8ED42	jle	short	loc	7FF7EFB8EDC1
		1		
I I				
0007FF7EFB8ED44	nov e	ebx, e	di	
0007FF7EFB8ED46	db (56h, 6	6h	
			-	and the second second second second second second second second second second second second second second second

🔲 💰 🖼		1
	mau	abu adi
00007FF7EFD0ED44	db	cch cch
00007FF7EFD0ED40	ab	bon, con
0000/FF/EFB8ED46	nop	word ptr [rax+rax+00000000n]
		•••
📕 🛋 🖾		• •
00007FF7EFB8ED50		
00007FF7EFB8ED50	loc 7FF	7EFB8ED50:
00007FF7EFB8ED50	mov	eax, [r15]
00007FF7EFB8ED53	mov	[rbp+8C0h+var_918], eax
00007FF7EFB8ED56	mov	r8d, 4 ; Size
00007FF7EFB8ED5C	lea	rdx, [rbp+8C0h+var 918] ; Sr
00007FF7EFB8ED60	lea	rcx, [rsp+9C0h+var 960] ; Ds
00007FF7EFB8ED65	call	memmove
00007FF7EFB8ED6A	movzx	eax, [rsp+9C0h+var 960]
00007FF7EFB8ED6F	movd	xmm7, eax
00007FF7EFB8ED73	cvtdq2p	s xmm7, xmm7
00007FF7EFB8ED76	movzx	eax, [rsp+9C0h+var 95E]
00007FF7EFB8ED7B	movd	xmm6, eax
00007FF7EFB8ED7F	cvtda2p	s xmm6, xmm6
00007FF7EFB8ED82	movaps	xmm0, xmm6
00007FF7EFB8ED85	mulss	xmm0, xmm6
00007FF7EFB8ED89	movaps	xmm2, xmm7
00007FF7EFB8ED8C	mulss	xmm2, xmm7
00007FF7EFB8ED90	addss	xmm0, xmm2 : X
00007FF7EFB8ED94	call	sartf
00007FF7EFB8ED99	movss	dword ptr [r14], xmm0
00007FF7EFB8ED9E	movaps	xmm1, xmm7 ; X
00007FF7EFB8EDA1	movaps	xmm0, xmm6 ; Y
00007FF7EFB8EDA4	call	atan2f
00007FF7EFB8EDA9	addss	xmm0, xmm8
00007FF7EFB8EDAE	movss	dword ptr [r14+4], xmm0
00007FF7EFB8EDB4	add	r14, 8
00007FF7EFB8EDB8	add	r15, 4
00007FF7EFB8EDBC	dec	rbx
00007FF7EFB8EDBF	inz	short loc 7EE7EE88ED50

00007FF7EFB8EDC	1	
00007FF7EFB8EDC	l loc_7FF	7EFB8EDC1:
00007FF7EFB8EDC	1 mov	<pre>rax, [rsp+9C0h+var_958]</pre>
00007FF7EFB8EDC	5 add	[rax], r12d
00007FF7EFB8EDC	9 mov	rcx, cs:qword_7FF7EFDB2D78
00007FF7EFB8EDD	o mov	r9, 87C37B91114253D5h
00007FF7EFB8EDD	A imul	rcx, r9
00007FF7EFB8EDD	E rol	rcx, 1Fh
00007FF7EFB8EDE	2 mov	rdx, 4CF5AD432745937Fh
00007FF7EFB8EDE	c imul	rcx, rdx
00007FF7EFB8EDF	a xor	rcx, 48F73C39h
00007FF7EFB8EDF	7 rol	rcx, 1Bh
00007FF7EFB8EDF	B mov	rax, 18FB11446h
00007FF7EFB8EE0	5 add	rax, rcx
00007FF7EFB8EE0	B lea	r8, [rax+rcx*4]
00007FF7EFB8EE0	c mov	rax, cs:gword 7FF7EFDB2D80
00007FF7EFB8EE1	3 imul	rax, rdx
00007FF7EFB8EE1	7 rol	rax, 21h
00007FF7EFB8EE1	3 imul	rax, r9
00007FF7EFB8EE1	Fxor	rax, 48F73C39h
00007FF7EFB8EE2	5 rol	rax, 1Fh
00007FF7EFB8EE2	add	rax, 0B41DEF1h
00007FF7EFB8EE2	F add	rax, r8
00007FF7EFB8EE3	2 lea	rcx, [rax+rax*4]
00007FF7EFB8EE3	5 xor	rcx, 10h
00007FF7EFB8EE3	A xor	r8, 10h
00007FF7EFB8EE3	E add	r8. rcx
00007FF7EFB8EE4	1 mov	rax, r8
00007FF7EFB8EE4	\$ shr	rax, 21h
00007FF7EFB8EE4	s xor	rax, r8
00007FF7EFB8EE4	mov	r9. 0FF51AFD7ED558CCDh
00007FF7EFB8EE5	5 imul	rax, r9
00007FF7EFB8EE5	mov	rdx, rax
00007FF7EFB8EE5	shr	rdx, 21h
00007FF7EFB8EE6	xor	rdx, rax
00007FF7EFB8EE6	3 mov	r10, 0C4CEB9FE1A85EC53h
00007FF7EFB8EE6	imul	rdx, r10
00007FF7EFB8EE7	l lea	rax, [rcx+r8]
00007FF7FFB8FF7	mov	rcx. rax
00007FF7EFB8EE7	B shr	rcx, 21h
00007FF7EFB8EE7	xor	rcx, rax
00007FF7EFB8EE7	F imul	rcx, r9
00007FF7EFB8EE8	mov	rax. rcx
00007FF7EFB8EE8	5 shr	rax, 21h
00007FF7EFB8FE8	xor	CAX. CCX
00007FF7EFB8EE8	imul	rax, r10
00007FF7EFB8EE9	mov	PCX. Pax
00007FF7FF88FF9	1 shr	rcx, 21h
00007FF7FF88FF9	R YOF	PCY PAY
00007FF7EFB8FF9	Bmov	rax, rdx
00007FF7EFB8FF9	Eshr	rax, 21h
00007FF7EFB8FFA	2 xor	rax, rdx
00007FF7EFB8FFA	5 add	CAX. CCX
00007FF7EFB8FFA	8 add	CCX. CAX
00007FF7FFB8FF4	B mov	[rbp+8C0h+var 280], ray
00007FF7EFB8FFB	2 mov	[rbp+8C0h+var_278], rcv
00007FF7EFB8FFB	test	r12d, r12d
00007FF7EFB8FFB	ile	loc 7FF7EFB8EF93

Decryption Round Two

00007FF7EFB71880 00007FF7EFB71880 loc 7FF7EFB71880: 00007FF7EFB71880 mov rcx, cs:gword 7FF7EFDB2D78 r8, 87C37B91114253D5h 00007FF7EFB71887 mov 00007FF7EFB71891 imul rcx, r8 00007FF7EFB71895 rol rcx, 1Fh 00007FF7EFB71899 mov rdx, 4CF5AD432745937Fh 00007FF7FFB718A3 imul nex, ndx 00007FF7FFB718A7 xor rcx, 48F73C39h 00007FF7EFB718AE rol rcx, 1Bh 00007FF7EFB718B2 mov rax, 18FB11446h 00007FF7EFB718BC add rax, rcx 00007FF7EFB718BF lea rdi, [rax+rcx*4] 00007FF7EFB718C3 mov rax, cs:gword 7FF7EFDB2D80 00007FF7EFB718CA imul rax, rdx 00007FF7EFB718CE rol rax, 21h 00007FF7EFB718D2 imul rax, r8 00007FF7FFB718D6 xor rax, 48F73C39h 00007FF7EFB718DC rol rax, 1Fh 00007FF7EFB718E0 add rax, 0B41DEF1h 00007FF7EFB718E6 add rax, rdi 00007FF7EFB718E9 lea rcx, [rax+rax*4] 00007FF7EFB718ED xor rcx, 10h 00007FF7FFB718F1 xor rdi, 10h 00007EE7EE8718E5 add rdi, rcx 00007FF7EFB718F8 mov rax, rdi 00007FF7EFB718FB shr rax, 21h 00007FF7EFB718FF xor rax, rdi 00007FF7EFB71902 mov r8, 0FF51AFD7ED558CCDh 00007FF7EFB7190C imul rax, r8 00007FF7EFB71910 mov rdx, rax 00007FF7EFB71913 shr rdx, 21h 00007FF7FFB71917 xor rdx, rax 00007FF7EFB7191A mov r9, 0C4CEB9FE1A85EC53h 00007FF7EFB71924 imul rdx, r9 00007FF7EFB71928 lea rax, [rcx+rdi] 00007FF7EFB7192C mov rcx, rax 00007FF7EFB7192F shr rcx, 21h 00007FF7EFB71933 xor rcx, rax 00007FF7EFB71936 imul rcx, r8 00007FF7EFB7193A mov rax, rcx 00007FF7EFB7193D sh rax, 21h 00007FF7EFB71941 xor rax, rcx 00007FF7EFB71944 imu] rax, r9 00007FF7EFB71948 mov rcx, rax 00007FF7EFB7194B sh rcx, 21h 00007FF7EFB7194F xor rcx, rax 00007FF7EFB71952 mov rax, rdx 00007FF7EFB71955 shr rax, 21h 00007FF7EFB71959 xor rax, rdx 00007FF7EFB7195C add rax, rcx 00007FF7EFB7195F add rcx, rax 00007FF7EFB71962 mov [rbp+117C0h+var 1C8], rax 00007FF7EFB71969 mov [rbp+117C0h+var 1C0], rcx 00007FF7EFB71970 mov ebx, r14d 00007FF7EFB71973 test r15d, r15d loc 7FF7EFB71A38 00007FF7EFB71976 jle

🚺 🚄 🖾

🚺 🛃 🔛

00007FF7FFB71A77 xor edi. 8 00007FF7EFB71A7A mov eax, edi 00007FF7EFB71A7C shr eax, 10h 00007FF7EFB71A7F xor eax, edi ecx, eax, 85EBCA6Bh 00007FF7EFB71A81 imul 00007FF7EFB71A87 mov eax, ecx 00007FF7EFB71A89 shr eax, 0Dh 00007FF7EFB71A8C xor eax, ecx 0007FF7EFB71A8E imul ecx. eax. 0C2B2AE35h 00007FF7FFB71A94 mov edi. ecx 00007FF7EFB71A96 shr edi. 10h 00007FF7EFB71A99 xor edi, ecx 00007FF7EFB71A9B mov rax, r15 00007FF7EFB71A9E cgo 00007FF7EFB71AA0 sub rax, rdx 00007FF7EFB71AA3 sar rax, 1 00007FF7EFB71AA6 mov r14, rax 00007FF7EFB71AA9 mov [rsp+118C0h+lpParameters], [00007FF7EFB71AAE mov rcx, rax 00007FF7EFB71AB1 call malloc wrapper 00007FF7EFB71AB6 mov rbx, rax 00007FF7EFB71AB9 mov rsi, r12 00007FF7EFB71ABC mov rax, 50107E74251C8553h 00007FF7EFB71AC6 imul rdi 00007FF7EFB71AC9 sub rdx, rdi 00007FF7EFB71ACC sar rdx, 9 00007FF7EFB71AD0 mov rcx, rdx 00007FF7EFB71AD3 shr rcx, 3Fh 00007FF7EFB71AD7 add rdx, rcx 00007FF7EFB71ADA imul rax, rdx, 2E9h 00007FF7EFB71AE1 add rdi, rax 00007FF7EFB71AE4 mov eax. 1 00007FF7EFB71AE9 cmovz rdi. rax 00007FF7EFB71AED xorps xmm0, xmm0 00007FF7EFB71AF0 cvtsi2ss xmm0, rdi xmm0, cs:dword 7FF7EFDB4D78 00007FF7EFB71AF5 divss 00007FF7EFB71AFD movss xmm10, cs:dword 7FF7EFDB4D6 00007FF7EFB71B06 subss xmm10, xmm0 00007FF7EFB71B0B xor edi, edi 00007FF7EFB71B0D mov rax, r15 00007FF7EFB71B10 cgo 00007FF7EFB71B12 and edx, 7 00007FF7EFB71B15 add rax, rdx 00007FF7EFB71B18 sar rax, 3 00007FF7EFB71B1C mov r15, rax 00007FF7EFB71B1F test eax, eax 00007FF7EFB71B21 ile loc 7FF7EFB71BCF

					¥ —		
		📕 🚄 🖼					
		00007FF7EF	B71B27	movsd	xmm9,	cs:qword_7FF7EFDE	34D90
_					5		
L	A						
L		<u></u>					
L	00007F	F7EFB71B30					
L	00007F	F7EFB71B30	loc_7F	F7EFB71	830:		
L	00007F	F7EFB71B30	movss	xmm8,	dword	ptr [rsi]	
L	00007F	F7EFB71B35	movss	dword	ptr [r	bp+117C0h+var_117	C8],
L	00007F	F7EFB71B3B	movss	xmm7,	dword	ptr [rsi+4]	
L	00007F	F7EFB71B40	add	rsi,	8		
L	00007F	F/EFB/1B44	addss	xmm/,	xmm10		
L	000071	F7EFB71B49	movss	dword	ptr [r	op+11/C0n+var_11/	C8+4
L	000075	F/EFB/1B4E	movaps	xmmø,	xmm /	; X	
L	000075	F7EFB71851	Call	COST			
L	000075	F7EFD71D50	movaps	xiiiiio,	xmm7		
L	00007	E7EEP71055	movaps cpl1	cinf.	XIIIII /	, ^	
L	00007F	F7EFB71B61	movane	vmm7	vmmQ		
L	00007F	F7EFB71B64	mulee	vmm6	vmm8		
L	00007F	F7EFB71B69	VOCDE	vmm1	vmm1		
L	00007F	F7FFB71B6C	cvtss2	sd xmm1	. xmm6		
L	00007F	F7FFB71B70	andns	vmm1.	ymm9		
L	00007F	F7EFB71B74	cvtpd2	os xmm0	. xmm1		
L	00007F	F7EFB71B78	call	round	f		
L	00007F	F7EFB71B7D	movaps	xmm6.	xmm0		
L	00007F	F7EFB71B80	mulss	xmm7,	xmm8		
L	00007F	F7EFB71B85	xorps	xmm1,	xmm1		
L	00007F	F7EFB71B88	cvtss2	sd xmm1	, xmm7		
L	00007F	F7EFB71B8C	andps	xmm1,	xmm9		
L	00007F	F7EFB71B90	cvtpd2	ps xmm0	, xmm1		
L	00007F	F7EFB71B94	call	round	f		
L	00007F	F7EFB71B99	cvttss	2si rax	, xmm6		
L	00007F	F7EFB71B9E	mov	word	ptr [rs	p+118C0h+var_1186	8],
L	00007F	F7EFB71BA3	cvttss	2si rax	, xmm0		
L	00007F	F7EFB71BA8	mov	word	ptr [rs	p+118C0h+var_1186	8+2]
L	00007F	F7EFB71BAD	movsxd	rax,	edi		
L	00007F	F7EFB71BB0	lea	rcx,	[rbx+ra	x*4] ; Dst	
L	00007F	F7EFB71BB4	mov	r8d, 4	4	; Size	
L	00007F	F7EFB71BBA	lea	rdx,	[rsp+11	.8C0h+var_11868] ;	Sno
L	00007F	F7EFB71BBF	call	memmo	ve		
I	00007F	F7EFB71BC4	inc	edi			
	00007F	F7EFB71BC6	cmp	edi,	r15d		
	00007F	F/EFB71BC9	JT	10C_7	FF7EFB7	1830	
L							

Encryption Round Two is Not Symmetric

Address	He	ĸ															ASCII
000002206499A6F0	B 3	02	5D	47	3D	85	10	40	ED	A4	52	47	78	7D	12	40	*.]G=@1¤RGx}.@
000002206499A700	8A	FD	95	47	9E	50	2D	40	4B	51	5 F	47	2F	42	1F	40	.ý.G.P-@KQ_G/B.@
000002206499A710	90	49	18	47	20	AE	2C	40	FO	1D	60	47	22	EF	38	40	.I.G ◎,@ð.`G"ï8@
000002206499A720	E4	A1	68	47	30	F6	50	40	5E	93	7D	47	0A	D9	56	40	ä;hGOÖP@^.}G.ÙV@
000002206499A730	22	F7	90	47	F4	80	3F	40	39	0E	98	47	1F	6B	33	40	"÷.Gô.?@9G.k3@
000002206499A740	8D	B1	5D	47	A1	E1	40	40	D5	7C	32	47	B9	E3	3D	40	.±]Giá@@Õ 2G'ã=@
000002206499A750	3C	53	67	47	92	10	3F	40	D9	6C	79	47	21	B5	1C	40	<sgg?@ùĺyg!µ.@< td=""></sgg?@ùĺyg!µ.@<>
000002206499A760	03	A3	91	47	3F	BO	39	40	84	1B	9C	47	30	DF	34	40	.£.G?°9@G0B4@
000002206499A770	OB	E2	46	47	F4	87	10	40	34	23	83	47	E2	B7	49	40	.âFGÔ@4#.Gâ·I@
000002206499A780	28	65	2E	47	D8	23	49	40	4A	18	B6	46	FA	EC	42	40	(e.GØ#I@J.¶FúÌB@
000002206499A790	33	94	9B	47	BE	E7	3F	40	15	4A	9C	47	33	FB	37	40	3. G4C?@ J.G3û7@
000002206499A7A0	44	34	F2	46	92	D2	12	40	3A	27	9F	47	50	DC	30	40	D40F.0.@:'.GPU0@
000002206499A7B0	42	2D	AD	46	93	00	ЗA	40	76	EE	0E	47	4F	F3	1F	40	BF:@vî.GQÓ.@
000002206499A7C0	9C	Ε1	83	46	B5	CF	12	40	DF	47	82	46	60	B2	2A	40	.á.FµÏ.@ßG.F`⁼*@
000002206499A7D0	BF	17	64	47	BO	49	37	40	E6	EF	23	47	7B	9D	0E	40	∠_dG°I7@æï#G{@
000002206499A7E0	2F	F4	13	47	56	21	55	40	55	Α9	AB	46	B2	78	43	40	/Ô.GV!U@U@«F=xC@
000002206499A7F0	AD	8E	21	47	AA	F3	38	40	67	2B	27	47	A3	0C	19	40	!Gª08@g+'G£@
000002206499A800	31	85	66	47	8A	AB	63	40	65	Β4	C6	46	4A	A2	65	40	1 fG «c@e ÆFJ¢e@
000002206499A810	B4	63	7E	47	F3	27	2D	40	F9	72	ЗA	47	C5	C1	47	40	c~Go'-@ur:GAAG@
000002206499A820	2B	F8	51	47	60	93	63	40	78	A3	ЗE	47	1B	65	48	40	+øQG c@x£>G eH@
000002206499A830	8F	33	0A	47	60	75	0C	40	EB	12	4E	46	39	B6	OD	40	.3.G u.@ē.NF9¶.@
000002206499A840	3E	2F	18	47	F1	Ε1	0E	40	CE	8F	0F	47	75	32	32	40	>/.Gna.@IGu22@
000002206499A850	5B	5E	69	47	7D	81	OD	40	DF	23	7B	47	56	CA	60	40	[^iG}@B#{GVE`@
000002206499A860	82	07	85	47	OB	8F	24	40	81	4F	EE	46	73	32	21	40	G\$@.01Fs2!@
000002206499A870	CB	75	57	47	9B	0F	14	40	56	82	9F	47	8E	2B	35	40	EuWG@VG.+5@
000002206499A880	13	3E	1B	47	C9	4C	38	40	D5	F2	6A	47	12	D2	4E	40	.>.GEL8@OojG.ON@
Game Plan

- Peel off one layer of encryption at a time:
 - "encrypt" third round via symmetric encryption.
 - "decrypt" second round.
 - Hope for hardcoded constants, no time related secrets.
 - "encrypt" first round via symmetric encryption.

Extracting Ciphertext, Third Round of Encryption

Test.x	Challer	ige5_	V1.7	.х														
Offs	et	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000	000	9E	0A	66	89	0D	16	30	14	FE	B6	AO	59	EA	7E	D4	12	žf‰ 0 þ¶ Yê~Ô
00000	016	AF	24	51	89	0D	16	30	14	DD	B 6	AO	59	EB	7E	D4	12	¯\$Q‰ 0 ݶ Yë~Ô
00000	032	C4	1C	3D	36	DE	95	51	C6	7E	61	D8	68	D7	6A	A0	FB	Ä =6₽•QÆ~aØh×j û
00000	048	DC	ЗD	20	8 F	39	DF	BE	27	13	Α4	65	DD	F9	A 8	87	E7	Ü= 98¾' ¤eÝù∵‡ç
00000	064	E5	FC	75	48	3B	24	77	FC	09	10	28	71	47	FA	40	CE	åüuH;\$wü (qGú@Î
00000	080	9C	5E	43	48	40	1A	0D	E1	5A	31	86	46	51	12	4B	CA	œ^CH@ áZl†FQ KÊ
00000	096	В4	90	C2	D6	85	5A	C7	6D	FO	FC	4A	DF	4E	9C	71	CF	ÂÖZÇmðüJBNœqÏ
00000	112	1D	AC	C9	8C	E8	6E	C4	1B	0B	73	87	A 2	15	BD	8C	49	¬ÉŒènÄ s‡¢ ₩EI
00000	128	C0	23	B6	79	FC	DD	FB	A 2	8A	36	AA	17	BA	1F	E4	BE	À #¶ yüÝû¢Š6ª ° ä¾
00000	144	96	53	C2	BA	F2	90	07	39	56	06	F6	9D	B2	AD	1B	38	-S°ò 9V ö ⁼- 8
00000	160	91	CD	2F	2B	38	7E	Α4	09	21	BB	57	40	C4	9F	91	08	`Í/+8~¤ !≫W@ÄŸ`
00000	176	2C	9B	90	D6	Fl	C9	FE	B0	87	87	4D	A0	67	09	1F	7A	,≻ÖñÉþ°‡‡Mg z
00000	192	BB	7A	21	B 3	F6	FD	13	9E	9A	A 5	DE	2B	10	DO	E9	1E	»z!"öý žš¥⊉+ Đé
00000	208	CE	7D	AC	68	88	DA	AB	4C	07	C1	7C	26	6E	23	5B	AF	Ï}¬h^Ú«L À &n#[
00000	224	64	D2	A4	A 8	C9	FD	1F	0B	E5	E9	27	BB	8B	D8	AA	16	dÒ¤∵Éý åé'≫<ت
00000	240	28	5E	57	A2	01	95	1F	21	81	02	B1	23	7F	07	D7	71	(^₩¢ • ! ±# ×q
00000	256	B6	21	53	77	A2	C1	99	2F	C5	EF	DE	46	8A	24	8B	49	¶!Sw¢Å™/ÅïÞFŠ\$ <i< td=""></i<>
00000	272	40	BB	36	2D	4D	96	68	A 2	87	F4	ЗD	8E	22	43	02	45	0≫6-M-h¢‡ô=Ž"C E
00000	288	E4	42	78	9A	97	7F	EB	AB	F9	DA	C8	EE	C2	56	FE	8E	äBxš— ë«ùÚĖîĀVþŹ
00000	304	СВ	ЗF	0E	9C	12	DA	28	46	37	94	39	54	94	94	93	BO	Ë? œ Ú(F7"9T"""°
00000	320	79	6D	05	06	42	6E	15	08	3F	C1	08	5B	6A	B6	0D	44	ym Bn ?À [j¶ D
00000	336	B5	F9	7F	E9	95	E8	85	8C	B3	7D	4D	29	32	AC	DF	CD	µù é•è…Œ³}M)2⊣BÌ
00000	352	48	EE	5A	D9	E2	E4	37	6E	90	CD	E3	FA	2C	40	57	E4	HîZÛâä7n İãú,@Wä
00000	368	В9	0E	FF	AA	24	C6	53	5B	78	El	F3	0C	91	CC	23	F3	'ÿ*\$ÆS[xáó `Í#ó
00000	384	C4	5D	FB	1A	CA	Α4	BO	22	49	Α7	8D	CD	8C	88	CD	0A	Ä]û ˤ°"IŞ İŒ^İ
00000	400	90	DD	14	8B	DD	A 4	9F	16	14	5C	72	85	04	AF	89	84	Ý «Ý¤Ý \r ‰,
00000	416	9A	8E	BB	Cl	00	FO	76	02	53	F8	Α6	DB	B3	2C	BA	AA	šŹ»Á ðv Sø¦Ü³,°ª
00000	432	7C	4E	67	AC	13	83	86	79	43	Fl	0E	1D	1D	91	D7	Cl	Ng¬ ftyCñ `×A
00000	448	7F	D6	FD	68	D5	Β4	A2	6E	8B	5E	B9	EF	59	F9	4D	23	ÖýhÖ′¢n<^¹ïYùM#
00000	464	A0	36	BA	15	0E	42	8B	6E	DE	67	6A	79	6E	11	9A	F9	6° B <n₽gjyn td="" šù<=""></n₽gjyn>
00000	480	F5	1E	41	AD	E1	1D	D7	D2	30	91	C5	27	B5	E8	D3	49	õ A-á ×00'A'µèOI
00000	496	07	15	29	AO	77	3F	A0	81	53	12	E6	3E	C2	9F	E1	7B) w? Sæ>AYá{
00000	512	17	3B	B7	25	9F	DB	BF	DF	AD	0F	F3	1F	21	9C	30	CB	; %YU¿B− ó !œOE
00000	528	76	07	74	EA	89	D2	8C	44	D3	EC	EE	C8	DF	3D	4B	7F	v te%OEDOiïEB=K
00000	544	02	AF	17	D3	F9	OF	D1	A 8	F5	9D	9F	BF	A2	06	21	15	Ou N 8 Y20 !
00000	560	C6	19	22	A'/	02	81	D2	715	88	81	96	8E	5D	00	10	DA	AC "S O " - Z] U
00000	576	5E	98	73	41	F4	89	AC	OF	57	CO	BB	11	D7	59	4B	21	^SAO‰¬ WA≫ ×YK!
00000	592	20	A4	FC	TE	AD	IF	B6	BA	51	BE	70	01	78	A5	72	52	Hu - 9°0% X¥rR
00000	608	90	40	67	00	4E	FE	31	70	19	98	20	58	A2	6E	20	59	LGANDI >-[on Y
00000	624	90	02	19	03	89	CI RC	89	80	36	64	E/	BC	18	88	21	56	00 -A- 60ÇIX /V
000000	640	/3	20	35	Dr	AD C7	EO	20	51	10	D3 CC	30	DC	11	90	7A	DE	SESDWAR-QN-<+10 ZP
00000	656	8A OF	30	80	92	20	19	43	96	E3	00	20	09	64	E /	06	88	S=€rçuc-al ÷ ,
00000	672	OL	71	11	23	AD	90	20	21	AL	93	43	20	CA	74	7.0	2A	**D'97220 @21 >** ~
000000	000	Cr 07	25	42	98	21	69	03	12	20	10	/A DD	37	D3	00	09	C2	168301 q- 27000A
00000	704	0 / E E	71	EA F7	22	21	D9	00	10	24	21	24	11	AP	30	22	ED FF	+ eo:oA x:» "y
00000	726	SE 24	71	27	70	70	20	20	10	34	62	A4	51	20	25	07	11	QC»vien4aA/> Vy
00000	750	24	70	0.0	A9	93	60	30	CH CO	ED oF	93	10	C2	30	20	0A 01	90	CIN AN A TOTARY
00000	760	70	14	99	12	92	DC	11	09	DC	26	LE NO	DE P2	A9	CF	57	DA	1 3 3D+1/06 373W-
00000	794	33	14 14	07	13	0A 22	Cl	09	5.9	DF	20	Ad	D3	08	DF	5/	C2	3 Γ μηλ·ΝΡή α 953
00000	800	33	AC.	21	R2	20	05	54	DD	42	82	37	BF	97	80	18	E2	300: - TVH 7: - F S
000000	816	58	D2	AL.	75	50	12	57	3D	20	82	D1	47	50	24	12	82	0
000000	030	32	51	CP	28	51 FD	13	90	20	26	50	DE	0 C	SE	21	76	02	202+10HarVG -
00000	032	33	21	CB	20	20	01	99	MA	20	29	08	00	20	CA	10		SQL+10 AND DEU



Extracting Ciphertext, Second **Round Decryption**

																					00007FF 00007FF	-63BAA -63BAA	1A2F 1A32	~ 0	9:FF0	「設出」
																			1P		00007FF	FG3BAA	1A3D	4	8:C70	🛛 🖸 ர
		-		~		-			· · ·		~ ~			1						•	00007FF	FG3BAA	1A44	C	F1F40	
Address	He	x															ASCII			٠	00007FF	F63BAA	1A48	0	F1F84	WZG
000002377830FDF0	AE	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	AB	~~~~~~~~~~~~~	0		[>	00007FF	F63BAA	1A50	6	98499	He
000002377830FE00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					00007F	CODAA	1AEE	2	100 0	
000002377830FE10	EE	FE	EE	FE	EE	FE	EE	FE	4F	C5	72	81	9F	59	00	3C	îþîþîþîþ0ÅrY.	<			00007F	EG3RAA	1464		359	D0 7
000002377830FE20	B3	02	5D	47	3D	85	10	40	ED	A4	52	47	78	7D	12	40	*.]G=@i¤RGX}.(8			00007F	EG3BAA	1466	ē	107 0	5F 7
000002377830FE30	8A	FD	95	47	9E	50	2D	40	4B	51	5 F	47	2F	42	1F	40	.ý.G.P-@KQ_G/B.0	8			00007FF	F63BAA	1A69	8	107	FC D
000002377830FE40	90	49	18	47	20	AE	2C	40	FO	1D	60	47	22	EF	38	40	.I.G ◎,@ð. G"180	8		•	00007FF	F63BAA	1AGF	8	D3CBF	111 1
000002377830FE50	E4	- A1	68	47	30	F6	50	40	5E	93	7D	47	0A	D9	56	40	a;hGOOP@^.}G.UVO	8		•	00007FF	F63BAA	1A72	4	8:FFC	10/0
000002377830FE60	22	F7		47	F4		3F	40	39			47	1F	6B	33	40	"÷.Gö.?@9G.k30	8		i@	0000751	CODAA	1470	× 7	r na	20 0
000002377830FE70	BD 8D	B1	5D	47	A1	E1	40	40	D5	7C	32	47	B9	EB	ЗD	40	.±]G;a@@O[2G'a=0				<					AC
000002377830FE80	30	53	67	47	92	10	31	40	09	6C	/9	47	21	85	10	40	<sgg?@ulyg!µ.0< td=""><td>e</td><td>edi=ED99CBA1</td><td></td><td></td><td></td><td></td><td></td><td></td><td>A1 6</td></sgg?@ulyg!µ.0<>	e	edi=ED99CBA1							A1 6
000002377830FE90	103	AB	91	47	3F	BO	39	40	84	18	90	47	30	DF	34	40	. £. G?* 9@ GOIS40									9B 8
000002377830FEA0		. 12	03	47	89	05	OB	40	108	7 B	97	47	SE	02	34	40	1G.U.@01.G>.40									1E A
000002377830FEB0		. C3	37	47	AB	10	20	40	LOC	93		46	6A	AU	327	40	nard .[@z.YF] A	ŧ ا •	text:00007FF63	BAA1A38	3 timelo	ck.ex	e:\$11/	A38 #	10E38	75 9
000002377830FEC0		00	SP CA	47	102	10	10	40	LCC.	74	AD	47	40	OF DA	27	40	9.160.20.34«GH.70									36 E
000002377830FED0	20			40	1 E C	E7	60	40	64	10	20	47	40 D4	04	25	40	->xxEr@@g.GH~PC		-					_		07 5
000002377830FEE0	20	90	EO	46	35	23	1E	40	43	01	DS	45	15	6F	10	40	-0.2F0+ @0 (00.7%)		😓 Dump 1 🛛 🚛	Dump 2	😓 Du	mp 3	😓 Dr	ump 4		39 1
000002377830FF00	15	76	68	47	DA	8A	43	40	7D	4F	18	47	81	CA	1F	40	.vhGÚ.C@}0.G.Ê.(Address	LIAV		-		-		3A 4
000002377830FF10	20	68	6A	47	37	26	65	40	86	77	10	47	D6	52	45	40	.kiG7&e@.w.GÖRE@		000002202884207	10.20	0 0 0 20	20.02	00.0		CA DC	E7 2
000002377830FF20	36	7E	EC	45	95	6F	34	40	77	91	62	47	7C	92	20	40	6~1E.04@w.bG . (00000220388A207		1 B6 38	20 02	00 0		00 00	80 /
000002377830FF30	1A	FE	3D	47	F2	92	4C	40	2F	39	85	46	D5	53	6A	40	.þ=Gò.L@/9.FÔSj0	١ŏ	00000220388A209	0 80 81	B5 38	20 02	00 0	O AB	AB AB	66 5
000002377830FF40	60	11	71	47	E2	77	36	40	9D	CB	ЗE	47	EO	17	4F	40	`.qGâw6@.Ë>Ga.O	١ŏ	00000220388A20A	AB AB	AB AB	AB AB	AB A	BEE	FE EE	77 E
000002377830FF50	DO	70	3B	47	EA	13	56	40	F7	3C	4F	47	AC	A4	53	40	D ;Gê.V@÷ <og¬¤so< td=""><td>0</td><td>00000220388A20B</td><td>0 00 00</td><td>00 00 0</td><td>00 00</td><td>00 0</td><td>0 00</td><td>00 00</td><td>96 2</td></og¬¤so<>	0	00000220388A20B	0 00 00	00 00 0	00 00	00 0	0 00	00 00	96 2
000002377830FF60) 5 F	78	ЗA	47	E3	4F	1A	40	B9	AB	BD	46	1F	53	28	40	_x:GãO.@'«½F.S(0	0	00000220388A20C	00 00	00 00 0	00 00	00 00	0 AF	F2 BA	68 0
000002377830FF70	FC	D7	5 B	47	34	AC	29	40	44	C4	AF	46	2D	32	36	40	ü×[G4¬)@DÄ [¯] F−260	8 0	00000220388A20D	0 66 78	3 B3 B7	19 OC	25 5	2 DF	8C 2E	3F 0
000002377830FF80) 1E	11	. 4D	47	63	10	16	40	9A	8C	19	47	BO	ЗF	5 F	40	MGC@G°?_0		00000220388A20E	0 50 87	7 81 OC	4E 4D	9A 6) F9	AF BC	
000002377830FF90	67	05	4F	47	BE	FA	1B	40	EB	63	E8	45	E8	97	63	40	g.OG¾ú.@êcêEê.co)0000220388A20F	0 86 10	O CB 37	E1 9D	92 B	1 E7	5D F2	80 6
000002377830FFA0	49	F9	67	47	7A	BD	07	40	5C	B8	91	47	EE	4C	4A	40	IugGz½.@\GiLJ0		J0000220388A210	0 C6 95	5 27 8E	43 2C	2A 0	F B1	D7 C9	C6 0
000002377830FFB0	39	EA		46	CF	2F	5C	40	99	2B	76	47	A2	A5	69	40	9ë.FI/\@.+vG¢¥10		J0000220388A2110	0 44 37	55 AU	D6 96	67 6	1 29	B1 28	66 1
000002377830FFC0	AC	37	9B	47	2A	92	32	40	EF	9F	99	47	02	2F	35	40	¬7.G*.2@îG./50		00000220388A2120	1B 11	1 C1 52	65 EB		E 03	68 41	00 0
																			00000220388A214	BE FE	08 A8	AA 4E	C5 2	BEZ	13 38	
																		lõ	00000220388A215	07 60	E8 48	9C 76	C5 D	7 4F	09 7A	
																		0	00000220388A216	D E5 48	E D5 72	77 4A	93 4	4 9C	3D 62	Keep
																		0	00000220388A217	BO 30	2E C2	1C 61	1F 5	4 3F	78 C2	
																		0	00000220388A218	01 CE	3 DD 29	95 GC	41 10	C 41 (C7 D6	17114
																		0	10000220388A219	E9 01	18 56	58 7E	1E A	E 83	78 A7	0B 56 F

•	00007FF63BAA1A2F 49:FF0	」」「設迅靋説蕚∷旫、記{盞''貧@鉃∧脯ៃ舔゚超時心醫趁助垰鈮针瞳籐閲甄曉
·•	00007FF63BAA1A32 ^ OF85 5	
RIP	00007FF63BAA1A38 BF 372	🙀 LITE-8
•	00007FF63BAA1A3D 48:C70	• 011-0
•	00007FF63BAA1A44 0F1F40	
•	00007FF63BAA1A48 0F1F84	WZGQQf@6 QF2?\@QQ GK @QQ GQQE@QQ\$GQQA@Qg~G
>•	00007FF63BAA1A50 698499	
	00007FF63BAA1A5B C1C0 C	Hex:
	00007FF63BAA1A5E 69C8 9	
	00007FE63BAA1A64 33E9	D0 7C 3B 47 EA 13 56 40 F7 3C 4F 47 AC A4 53 40
	0000755628441466 0107 0	5F 78 3A 47 E3 4F 1A 40 B9 AB BD 46 1F 53 28 40
	00007FF63BAA1A60 81C7 1	FC D7 5B 47 34 AC 29 40 44 C4 AF 46 2D 32 36 40
	00007FF63BAA1A65 81C7	1E 11 4D 47 63 10 16 40 9A 8C 19 47 B0 3F 5F 40
	00007FF63BAAIA6F 0DSCBF	67 05 4F 47 BE FA 1B 40 EB 63 E8 45 E8 97 63 40
•	00007FF63BAA1A72 48:FF0	49 F9 67 47 7A BD 07 40 5C B8 91 47 FF 4C 4A 40
L@	00007666204414761 . 76 00	39 FA 88 46 CE 2E 5C 40 99 28 76 47 42 45 69 40
	<	AC 27 98 47 2A 92 22 40 55 85 99 47 02 25 56 40
edi=ED99CBA1		AC 37 36 47 2A 32 32 40 19 16 35 47 02 2F 33 40
Cur-Ebbbebai		AI 62 62 46 64 24 65 40 18 10 87 46 AE 64 56 40
		98 87 6D 47 C5 AF 48 40 93 0A 90 47 98 9E 35 40
tout.000075563844443	n timeleck eventsings anorse	1E A3 8E 47 8D 94 3C 40 EE 8B 91 47 B4 3C 47 40
.LEX1:0000/FF63BAAIA3	s timefock.exe:\$11A38 #10E38	75 9C 33 47 7A 4C 25 40 D5 34 51 46 47 C9 2F 40
		36 BF 66 47 04 46 36 40 4B 2B 1B 47 46 D4 63 40
1		07 51 71 47 8C E8 2B 40 FF 25 8D 47 ED 90 40 40
Dump 1 Dump 2		39 11 44 47 C7 14 55 40 C7 88 91 47 6F 6F 27 40
alla Dump z	🚛 Dump 3 👹 Dump 4 😽	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40
Address Hex	Ump 3 Ump 4 Ump 4	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40
Address Hex 00000220388A2070 10 2	0 8A 38 20 02 00 00 C0 64 86	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 BS E6 46 D4 C1 1B 40
Address Hex 00000220388A2070 10 2 00000220388A2080 C0 6	0 8A 38 20 02 00 00 C0 64 B6	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 88 E6 46 D4 C1 18 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40
Address Hex 00000220388A2070 10 2 00000220388A2080 00 8	Q mp Dump 3 Q mp Dump 4 Q mp 0 0 8A 38 20 02 00 00 CO 64 B6 4 B6 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40
Address Hex 00000220388A2070 10 2 00000220388A2080 00 6 00000220388A2090 80 80 80 80 80 80 80 80 80 80 80 80 80	High Dump 3 High Dump 4 High Dump 4 0 8A 38 20 02 00 00 CO 64 B6 4 B6 38 20 02 00 00 00 00 00 00 1 B5 38 20 02 00 00 AB AB AB 1 B5 38 20 02 00 00 CF FF FF	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40
Address Hex 00000220388A2070 10 2 00000220388A2080 CO 6 00000220388A2090 80 8 00000220388A2090 80 8 00000220388A2090 80 8	High Dump 3 High Dump 4 High Dump 4 0 8A 38 20 02 00 00 C0 64 B6 4 B6 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40
Address Hex 0000022038842070 10 2 0000022038842080 00 00 0 0000022038842080 80 80 90 0000022038842080 80 80 90 0000022038842080 00 00 90 90	Image: Window Constraints Image: Constraints	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 BS E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 40 43 40 08 2F 9B 47 RC 19 44 40
Address Hex 00000220388A2070 10 2 00000220388A2080 C0 6 00000220388A2080 S0 8 00000220388A2080 00 0 00000220388A2080 00 0 00000220388A2080 00 0 00000220388A2080 00 0	High Dump 3 High Dump 4 High Dump 4 0 8A 38 20 02 00 00 CO 64 B6 4 B6 38 20 02 00 00 00 00 00 01 1 B5 38 20 02 00 00 A8	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 18 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 80 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 25 09 74 77 54 70 80 75 47 53 A0 47 70 80 75 47 78 94 66 40
Address Hex Address Hex 00000220388A2070 10.2 00000220388A2080 00.6 00000220388A2080 80.8 00000220388A2080 80.8 00000220388A2080 00.0 00000220388A2080 06.7	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 80 57 5A 47 88 94 66 40
Address Hex 00000220388A2070 0.2 00000220388A2080 0.0 00000220388A2080 0.6 00000220388A2080 0.5	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00 00 CO 64 B6 4 86 38 20 02 00 00 00 00 10 1 B5 38 20 02 00 00 00 00 10 1 B5 38 20 02 00 00 00 00 00 00 00 10 11 15 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 80 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 36 7C 91 46 32 3F 5C 40 8D 48 FF 1E 47 C4 88 9C 40 36 7C 91 46 32 3F 5C 40 8D 48 FF 1E 47 C4 88 9C 40
Address Hex 00000220388A2070 10 2 00000220388A2080 00 0 0 00000220388A2080 66 7 0 00000220388A2080 50 8 1	High Dump 3 High Dump 4 High Dump 4 0 8A 38 20 02 00 <t< td=""><td>B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 82 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF FE 40 E3 BE 46 C1 18 40 80 AF E6 46 E7 84 40 E5 AC 45 9 C3 7 40 66 58 06 47 73 40 80 AF 58 AC 47 9 63 42 24 40 96 20 80 46 58 40</td></t<>	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 82 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF FE 40 E3 BE 46 C1 18 40 80 AF E6 46 E7 84 40 E5 AC 45 9 C3 7 40 66 58 06 47 73 40 80 AF 58 AC 47 9 63 42 24 40 96 20 80 46 58 40
Address Hex 00000220388A2070 10 2 00000220388A2080 CO 6 00000220388A2080 80 00 00000220388A2080 00 0 00000220388A2080 66 7 00000220388A2080 66 7 00000220388A2080 66 7 00000220388A2080 66 7 00000220388A2080 86 1 00000220388A2080 66 7 00000220388A2080 86 1	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00 00 CO 64 B5 4 86 38 20 02 00 00 00 00 00 1 B5 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 3E 40 41 CD 5C 47 60 72 69 40 80 AF DE 4E FE 40 E3 8E 64 C1 18 40 80 AF DE 4E FE 40 E3 8E 64 C1 18 40 80 AF DE 46 CE 81 74 0 80 2C 65 FA 21 40 96 20 80 46 58 FF 06 40 C6 A4 71 47 73 24 22 40 68 66 75 47 53
Address Hex 00000220388A2070 10 00000220388A2080 00 00000220388A2080 65 00000220388A2080 65 00000220388A2080 66 00000220388A2080 68 00000220388A2080 68 00000220388A2080 68 00000220388A2080 64 00000220388A2100 66 00000220388A2104 44	understand understand <thunderstand< th=""> understand understa</thunderstand<>	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 3E 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 3E 40 E4 E8 E4 40 E1 B8 E6 46 C1 18 40 80 AF E6 45 B4 E5 84 40 E5 B4 64 26 13 F 40 66 58 04 77 72 18 40 85 84 C4 73 740 66 40 C6 A4 71 47 63 24 22 40 44 40 36 75 74
Address Hex Address Hex 00000220388A2050 10.2 00000220388A2080 00.6 00000220388A2080 00.0 00000220388A2080 00.0 00000220388A2080 00.0 00000220388A2080 00.0 00000220388A2080 00.0 00000220388A2080 66.7 00000220388A2080 66.7 00000220388A2080 66.1 00000220388A2080 66.1 00000220388A2100 66.2 00000220388A2100 64.3 00000220388A2100 43.3 00000220388A2100 44.3	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00 00 C0 64 B6 4 B6 38 20 02 00 00 00 00 01 1 B5 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 3E 40 41 CD 5C 47 60 72 69 40 80 AF DE 4E FS 40 E3 8E 64 C1 18 40 80 AF DE 4E FS 40 E3 8E 64 C1 18 40 80 AF DE 40 PS BA C2 C4 71 40 77 78 F5 46 C5 F0 40 40 8A C2 45 FA 14 40 96 20 80 46 57 A4 78 94 66 40 46 40
Address Hex 00000220388A2070 10 00000220388A2080 CD 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2080 66 00000220388A2080 66 00000220388A2100 66 00000220388A2104 43 00000220388A2120 36A 00000220388A2120 34 00000220388A2120 34	Here Dump 3 Here Dump 4 Here 0 8A 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD SC 47 60 72 69 40 E7 28 80 47 EF 3E 40 41 CD SC 47 60 72 69 40 E7 28 80 47 EF 3E 40 E4 DE SE 86 46 C1 18 40 85 86 46 41 18 40 85 86 46 41 18 40 85 86 46 40 14 40 86 60 40 66 46 26 40 40 84 40 82 96 47 87 40 80 82 49 44 40 47 73 40 80 57 58 47 40 83
Address Hex Address Hex 00000220388A2050 10 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2080 66 00000220388A2080 66 00000220388A2080 66 00000220388A2100 66 00000220388A2100 66 900000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 64 000000220388A2100 64	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00 00 00 00 00 1 B5 38 20 02 00 00 00 00 00 01 1 B5 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 3E 40 41 CD 5C 47 60 72 69 40 80 AF E F3 40 E4 E3 86 46 C4 11 84 0 85 AC 47 39 9C 37 40 77 E8 F5 46 C5 87 06 40 A6 A7 39 9C 37 40 96 20 80 46 58 87 60 60 60 A4 71 47 63 24 22 40 68 66 75 47 53 A0 43 00 82 29 47 <
Address Hex 00000220388A2070 10 00000220388A2080 C0.6 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2060 66 00000220388A2100 67	H = Dump 3 H = Dump 4 H = Dump 4 0 8A 38 20 02 00 00 00 00 00 00 00 00 1 B5 38 20 02 00 00 00 00 00 00 00 00 1 B5 38 20 02 00 00 00 AB AB AB AB AB AB AB AB AB AB AB AB AB	B8 F1 1F 47 8A DF 37 40 SE AC DS 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD SC 47 60 72 69 40 E7 28 80 47 EF 3E 40 41 CD SC 47 60 72 69 40 E7 28 80 47 EF 5E 40 E3 BE 46 C1 18 40 80 AF D E4 B5 84 0 A5 AF D <ca< td=""> 46 2C 61 3F 40 66 58 06 40 C6 A4 24 55 A4 27 90 37 40 96 20 80 46 58 FF 06 40 08 22 45 EF A2 14 40 36 70</ca<>
Address Hex 00000220388A2050 10 2 00000220388A2050 00 80 8 00000220388A2050 00 0 2 00000220388A2050 00 0 0 00000220388A2050 00 0 0 00000220388A2050 00 0 0 00000220388A2050 66 7 0 00000220388A2050 50 8 1 00000220388A2100 66 7 0 00000220388A2100 64 3 0 00000220388A2100 64 4 3 00000220388A2100 64 4 3 00000220388A210 16 1 4 00000220388A210 18 1 6 00000220388A210 18 1 7 00000220388A215 07 6 1	understand understand <thunderstand< th=""> understand understa</thunderstand<>	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 067 54 75 3A 0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 B4 EF 1E 47 C4 B8 0C 40 AC AF 03 47 BB F3 45 40 8A 02 24 47 B3 A3 41 40 80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40 C6 07 63 47 2E 4D 51 40 E2 EE 6B 47 94 EA 13 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00 00
Address Hex 00000220388A2070 10 00000220388A2080 C0.6 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 14 00000220388A2100 18 00000220388A2150 07 00000220388A2150 07 00000220388A2160 E5	Image: Constraint of the state of	B& F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 BE 64 60 4C 11 B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 84 C1 24 7 B3 A3 41 40 80 67 63 47 2E 4D 51 40 C2 83 47 2D 8E 30 40 C6 07 63 47 2E 4D 51 40 E2 EE 6B 47 94 EA 13 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00
Address Hex 00000220388A2070 10 2 00000220388A2080 C0.6 6 00000220388A2080 00 0 00000220388A2080 66 7 00000220388A2080 66 7 00000220388A2080 66 7 00000220388A2100 66 7 00000220388A2100 C6 9 00000220388A2100 C6 9 00000220388A2100 C6 9 00000220388A2100 C6 9 00000220388A2130 18 1 00000220388A2140 EF 6 00000220388A2150 C6 5 00000220388A2160 E5 4 00000220388A2170 B0 3	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00	B8 F1 1F 47 8A DF 37 40 SE AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD SC 47 60 72 69 40 E7 28 80 47 EF 3E 40 41 CD SC 47 60 72 69 40 80 47 EF 3E 40 EF 40 E3 8E 46 H 11 80 80 47 E4 EF 8E 40 E3 FD AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 06 40 B8 A22 45 EF A2 14 40 96 20 80 46 55 A0 40 08 27 54 47 37 40 82 44 44 40
Address Hex 00000220388A2070 10 00000220388A2080 C0.6 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2080 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 67 00000220388A2100 65 00000220388A2100 65 000000220388A2100 65 <	H = Dump 3 H = Dump 4 H = Dump 4 0 8A 38 20 02 00 <t< td=""><td>B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 3E 40 5E 46 C3 85 64 61 18 40 80 AF D6 46 F8 4E 58 40 5A AF CA 46 2C 61 3F 40 77 E8 F5 46 C5 86 40 40 80 82 245 EF 21 40 96 20 80 46 58 64 40 80 82 29 47 70 23 40 82 245 EF A2 40 40 80 67 57 A7 74 40 82 58 47 83 44</td></t<>	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 3E 40 5E 46 C3 85 64 61 18 40 80 AF D6 46 F8 4E 58 40 5A AF CA 46 2C 61 3F 40 77 E8 F5 46 C5 86 40 40 80 82 245 EF 21 40 96 20 80 46 58 64 40 80 82 29 47 70 23 40 82 245 EF A2 40 40 80 67 57 A7 74 40 82 58 47 83 44
Address Hex 00000220388A2070 10 00000220388A2080 C0.6 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2080 66 00000220388A2080 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2120 64 00000220388A2120 64 00000220388A2120 64 00000220388A2120 67 00000220388A2120 67 00000220388A2120 67 00000220388A2130 18 00000220388A2150 07 00000220388A2160 65 00000220388A2170 80 00000220388A2180 01 00000220388A2180 01 00000220388A2180 01 000000220388A2180 01 <	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 BE 646 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 84 EF 1E 47 C4 88 0C 40 AC AF 03 47 BB F3 45 40 8A C0 24 47 B3 A3 41 40 80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00 00
Address Hex 00000220388A2070 10 00000220388A2080 C0 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2080 66 00000220388A2080 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 67 00000220388A2100 67 00000220388A2160 67 00000220388A2160 65 00000220388A2180 07 00000220388A2180 01 00000220388A2180 01 00000220388A2180 01 00000220388A2190 65 00000220388A2180 01 00000220388A2180 88	High Dump 3 High Dump 4 High Dump 4 High Dump 4 0 8A 38 20 02 00 <td>B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 58 FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 B4 EF 1E 47 C4 B8 0C 40 AC AF 03 47 BB F3 45 40 8A 02 24 45 EF A2 14 40 80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40 C6 07 63 47 2E 4D 51 40 E2 EE 6B 47 94 EA 13 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00 00 Keep Size</td>	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 B8 E6 46 D4 C1 1B 40 80 AF D6 46 F8 4E 58 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 58 FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 B4 EF 1E 47 C4 B8 0C 40 AC AF 03 47 BB F3 45 40 8A 02 24 45 EF A2 14 40 80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40 C6 07 63 47 2E 4D 51 40 E2 EE 6B 47 94 EA 13 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00 00 Keep Size
Address Hex 00000220388A2070 10 00000220388A2080 C0 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 00 00000220388A2080 66 00000220388A2080 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 66 00000220388A2100 65 00000220388A2130 18 00000220388A2140 85 00000220388A2150 07 00000220388A2160 65 00000220388A2170 80 00000220388A2180 01 00000220388A2180 01 00000220388A2180 15 00000220388A2180 15 00000220388A2180 15 00000220388A2180 15 00000220388A2180 15 00000220388A2180 15 000000220388A2180 15 <tr< td=""><td>unders unders <thunders< th=""> <thunders< th=""> <thunders< td="" th<=""><td>B& F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 BE 64 60 4C 11 B 40 80 AF D6 46 F8 4E 53 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 84 EF 1E 47 C4 88 0C 40 AC AF 03 47 BB F3 45 40 8A C0 24 47 B3 A3 41 40 80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00 00 Keep Size</td></thunders<></thunders<></thunders<></td></tr<>	unders unders <thunders< th=""> <thunders< th=""> <thunders< td="" th<=""><td>B& F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 BE 64 60 4C 11 B 40 80 AF D6 46 F8 4E 53 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 84 EF 1E 47 C4 88 0C 40 AC AF 03 47 BB F3 45 40 8A C0 24 47 B3 A3 41 40 80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00 00 Keep Size</td></thunders<></thunders<></thunders<>	B& F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 3A 4A 3E 47 01 48 2A 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EA EF 3E 40 E3 BE 64 60 4C 11 B 40 80 AF D6 46 F8 4E 53 40 5A FD CA 46 2C 61 3F 40 66 58 00 47 77 32 1B 40 BF 5B AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 0C 40 BD 8A 22 45 EF A2 14 40 96 20 B0 46 5B FF 06 40 C6 A4 71 47 63 24 22 40 68 06 75 47 53 A0 43 40 08 2E 9B 47 BC 19 44 40 3F 09 7F 47 9A 47 37 40 B0 57 5A 47 88 94 66 40 36 7C 91 46 32 3F 5C 40 84 EF 1E 47 C4 88 0C 40 AC AF 03 47 BB F3 45 40 8A C0 24 47 B3 A3 41 40 80 67 7E 47 79 6C 0B 40 1C 20 83 47 2D 8E 30 40 66 1B 72 47 57 57 07 40 C3 25 69 47 B9 1C 16 40 00 00 00 00 Keep Size
Address Hex 00000220388A2070 10 2 00000220388A2080 C0 6 00000220388A2080 00 0 00000220388A2080 66 7 00000220388A2100 66 9 00000220388A2110 44 3 00000220388A2120 36 A 00000220388A2180 18 1 00000220388A2160 67 6 00000220388A2160 16 1 00000220388A2180 01 C 00000220388A2180 10 1 00000220388A2180 10 1 00000220388A2180 10 1 00000220388A2180 10 1 00000220388A2180 88 1 00000220388A2180 88 1 00000220388A2180	understand understand <thunderstand< th=""> understand understa</thunderstand<>	B8 F1 1F 47 8A DF 37 40 5E AC D5 46 36 BC 4E 40 41 CD 5C 40 5E AC D5 46 36 BC 4E 40 41 CD 5C 47 60 72 69 40 E7 28 80 47 EF 8E 40 41 CD 5C 47 60 72 69 40 80 AF D 66 58 60 47 73 218 40 BF 5E AC 47 39 9C 37 40 77 E8 F5 46 C5 8F 06 40 BA A2 24 5E F1 44 40 36 67 57 47 39 40 87 37 40 80 57 54 65 40 66 A4 71 47 32 42 24 40 35 67 71 40 <

Command:

Extracting Ciphertext and First Round of Encryption

00007F72F88C4 00007F72F88EC44 00007F72F88EC44 00007F72F88EC45 00007F77F88EC45 00007F77F88EC55	A1:3001 X0F byte bir ds:[r9],a1 A1:0FBGCA movzx exx,r10b 0FBGCA32 movzx eax,byte btr ds:[rdx+rsi] 888400 40060000 mov byte ptr ds:[rbp+rcx+640],a1 49:FFC2 inc r10 49:FFC1 inc r9 49:FFC1 inc r9				
00007FF7EFB8EC58	OF B Edit data at 000002377D0E0760	1001 000	15-A		
00007FF7EFB8C51 00007FF7EFB8C51 00007FF7EFB8E564 00007FF7EFB8E568	41 41 42 Hex String Copy data	000002377D0E0760 0 000002377D0E0770 0 000002377D0E0780 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00 00 00 00 00 00 00 00 00 00 00 00 00	
00007FF7EFB8EC6F 00007FF7EFB8EC6F	41 48 ASCII	000002377D0E0790 0	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 0 57 65 35 52 65 77 61 72	00 64 Challenge5Reward
00007F7EFB8EC74 00007FF7EFB8EC78	48 48 NÍyv(Àø¦îozMë 3 Xs ±Û`d Ž§Ç ≤7þò,œ¯Á ÆÙØ ÄF:ž dH n;	000002377D0E07B0	E 74 78 74 00 59 6F 7	75 20 68 61 76 65 20 63	6F .txt.You have co
00007FF7EFB8EC7F 00007FF7EFB8EC85 00007FF7EFB8EC8D	41 69 UNICODE: C1	000002377D0E07C0 0 000002377D0E07D0 2	0 63 68 61 6C 6C 65 7	20 54 69 6D 65 4C 6F 63 6E 67 65 20 23 35 20 75	73 challenge #5 us
00007FF7EFB8EC90 00007FF7EFB8EC96	56 59 54 44 50日子・額回線気茶型会発習ロ膀胱漂悦は事業会業留波で工業降型种業ロロ機会支援す会構成の 44	000002377D0E07E0 0 000002377D0E07E0 0	59 6E 67 20 56 31 2E 3 50 20 69 60 70 72 65 7	37 2E OD OA OD OA 49 20 73 73 65 64 20 77 69 74	61 ing V1.7I a 68 m impressed with
00007FF7EFB8EC99 00007FF7EFB8EC99	41 41 😮 UTF-8	000002377D0E0800 2	0 79 6F 75 72 20 73 (6B 69 6C 6C 20 61 6E 64 3	20 your skill and
byte ptr [r9]=[000002377D0E0760]=0	B Xs Qud QQ Q7QDQ QQ QF: Q dH nQc7QQQ YQdYQ	000002377D0E0820 7	73 74 61 6E 64 20 68 0	6F 77 20 79 6F 75 20 61	63 stand how you ac
text:0000755755885630 timelock patched eve	Hex:	000002377D0E0830	53 GF GD 70 GC G9 73 (68 65 64 20 74 68 69 73 1 60 60 65 65 67 65 20 52	21 complished this!
Image: Construction of the second s	55 36 0 A E I 21 10 C F AE 26 F0 F6 53 AA 0A C F B3 53 66 0 A E I 21 10 C F AE 26 F0 F6 53 AA 0A C F B3 53 27 78 36 57 89 57 89 92 78 98 56 53 AD 548 4F PC F0 28 57 76 82 C 79 E4 32 54 87 C 85 56 00 56 E4 A5 00 C E A5 82 90 0A 13 E6 1E C 558 22 55 82 A1 15 A8 6C A0 57 98 C 7 0C 78 9A E0 80 C 55 F8 21 18 99 A0 4E C 17 00 56 25 00 56 E4 A2 28 10 20 55 57 77 52 16 62 10 8 A7 25 56 07 66 43 28 1A 19 P1 08 10 00 87 68 30 80 86 768 38 23 16 57 F2 99 50 65 77 52 16 62 10 8 A7 25 56 07 66 43 28 1A 19 P1 08 12 16 03 30 87 68 38 23 16 57 72 99 50 65 77 52 16 32 53 38 06 52 90 A7 C 53 A9 457 72 03 588 41 12 24 85 53 38 06 52 91 A2 C 77 63 A9 457 72 03 58 41 14 17 76 30 30 83 1C 21 96 A7 C3 A9 457 72 03 58 10 19 F6 15 39 50 A1 C 4 9E E5 27 CC F1 A0 69 54 27 E8 05 19 F6 16 76 A3 52 70 10 08 64 27 C7 A8 30 C 9C 06 11 24 9A 16 78 A6 65 22 60 29 55 1F C F A 40 27 C 70 B8 28 47 69 17 8A 66 52 E0 29 55 16 17 C F A 49 3C 9C 06 11 24 9A 17 8A 66 52 E0 29 55 17 16 0 96 A1 80 64 06 06 88 DC 17 78 36 85 28 60 53 23 28 14 B 30 66 31 40 95 48 <	000002377D0E0850 000002377D0E0850 000002377D0E0850 000002377D0E0870 000002377D0E0880 000002377D0E0880 000002377D0E0880 000002377D0E0880 000002377D0E0880 000002377D0E0880 000002377D0E0880 000002377D0E0880 000002377D0E0890 000002377D0E0910 000002377D0E0910 000002377D0E0920 000002377D0E0920	10 0.0 0.0 0.4 4.3 6.8 6.1 (10 0.0 0.0 0.4 4.3 6.8 0.0 1.0 12 6.7 6.4 3.4 2.0 0.0 1.6 1.6 12 6.6 6.3 2.0 4.1 6.4 0.0 1.6 1.6 12 6.6 6.8 4.2 2.5 4.1 6.4 1.6 1	bc 6C 6C 6S 6E 67 6S 20 52 0A 0D 0A 42 54 43 20 50 64 72 65 73 73 3A 20 0D 39 7A 37 66 62 72 48 76 45 76 43 20 50 74 37 66 62 72 48 76 61 73 73 3A 20 0D 0A 42 32 64 67 43 34 48 34 44 55 53 7A 52 78 50 62 6A 59 58 54 40 69 79 71 34 71 AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB	<pre>bsChallenge Re 75 ward:BTC Pu A blic Address: 47 3NhhBeL927fbrKvG 51 LXQyZRCEvCfDW5nQ 74 TQBTC Privat 73 e Address:L2s 54 bGB3LkFdgC4H4JUT 74 D9DWt40SZRxPbjYZ 36 j5upKGhkTMiyq4q6 AB =G««««««««««««««« FE w«îpîpîpîpîpîpîp 30 îpîpîpîpîpîpîpîp 30 îpîpîpîpîpîpîpîpî 30 îpîpîpîpîpîpîpîpî 90 P .EopJ.}7 90 pJ.}7J.}7</pre>
$\begin{array}{c} 00000237700E0820 & 41 & 41 & 41 & 41 & 41 & 41 & 41 & 4$	64 - 55 - 61 - 00 - 66 - 66 - 76 - 30 - 16 - 72 - 89 - 02 - 65 - 62 - 85 - 37 7 7 8 7 8 7 8 7 9 7 9 7 9 7 10 1 10 1 11 11 12 1 14 1 15 1 16 1 16 1 17 1 18 10 10 1 10 1 10 1 10 1 16 10 17 10 18 10 19 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 </th <th></th> <th></th> <th></th> <th></th>				

Loot #5

Challenge5Reward - Notepad

File Edit Format View Help

You have completed TimeLock challenge #5 using V1.7.

I am impressed with your skill and anxious to understand how you accomplished this!

Challenge Reward:

BTC Public Address: 3NhhBeL9z7fbrKvGLXQyzRCEvCfDW5nQTQ

BTC Private Address: L2sbGB3LkFdgC4H4JUTD9DWt4oSzRxPbjYzj5upKGhkTMiyq4q67

Lessons Learned

Vulnerability found:

- Flawed encryption rounds may as well not be present at all.
- Crypto with hardcoded constants is easy to get around, since there are no variable secrets like time.
- Nesting crypto with different properties to make up for their shortcomings doesn't work when they are each critically flawed.

How to fix:

• Adopt a public – private key encryption scheme, and use a trusted third party to store keys and only provide access to authorised users.

The Case For Hackers In Dev Teams

- Auditing at end of development, right before production is not productive.
 - Its irresponsible and costly.
 - Deep flaws unlikely to be fixed before production.
- Security needs to be present at every step:
 - Early design / architecture planning.
 - Development.
 - Testing.
 - Deployment.
 - Post production.
- Hackers are specifically trained to consider the "big picture" when it comes to complex system interactions and spot small nuisances which are easily overlooked.

What Would a Robust TimeLock Look Like?

- Client and Server model.
- Secrets stored on trusted server.
- Data never leaves the client.
- Communication with public / private encryption systems.
 - Server.priv stored on the server.
 - Server.pub distributed to all clients.

Encryption

- Client wishes to make Lockbox:
 - Client sends Server.pub(hash(password, answers), start, stop)) to Server.
 - Server stores hash(password, answers), start, stop.
 - Server generates new lockbox.priv and lockbox.pub, sends Server.priv(lockbox.pub) to client.
 - Client makes lockbox.pub(data) + enc(answers).

Decryption

- Client wishes to decrypt:
 - Client collects and sends
 Server.pub(lockbox.pub(hash(password, answers))).
 - Server decrypts. Verifies hash and checks time window.
 - If correct, server sends
 Server.priv(lockbox.priv(lockbox.priv)).
 - Client decrypts with lockbox.priv(encdata).

Greetz

- u/cryptocomicon, for the interesting challenges.
- #kiwicon users for the weekday banter.
 - I am captianyipe, btw.
- NSA for making Ghidra public and FOSS.
 - Ghidra is the biggest thing to happen in reverse engineering for quite some time...

About Me

- Sustaining Engineer at Canonical.
 - Fixing Linux kernel gremlins in Ubuntu kernels.
 - Come find me and chat about Linux or reversing =)
- Read my blog:

https://ruffell.nz matthew@ruffell.nz