

Forum:[Hack Forums](#)

Thread: [\[Vb.net\] \[Source\] \[UPDATED\] All 15 Crypto.com Encryptions Cracked/Leaked](#)

pr0t0typ3 - September 11, 2010, 11:11 am

Hi Guys

Today I spend my time Cracking the Encryptions on Crypto.com

The source code is protected so I couldn't directly convert it but with a little trick I was able to get the javascript source.

I converted this and manually extracted the Key for each Encryption/Ciphers

I DO know that there are a few bugs in the functions, but I have no intention to rewrite the functions, sorry.

Encryptions/Ciphers you'll find in this thread are:

- AER-256
- OKTO3
- EZIP-64
- ARMON-64
- ZARA-128 (I fixed the bug)
- BASE-64 (I know that it is a Encoding not a Encryption)
- FERON-74
- GILA-7
- ATOM-128
- TIGO-3FX
- TRIPO-5
- ZONG-22
- HAZZ-15
- ESAB-46

And here you go:

<http://pastebin.com/LfH6qxPc>

There are only 3 simple Rules:

1. Give Credits
2. Post a Feedback
3. Don't flame/Constructive Criticism is highly appreciated (Yes I mean you Rue)

vag belch - September 11, 2010, 11:12 am

Great work, would you happen to be releasing the trick you used to get the source? :)

Asus - September 11, 2010, 11:13 am

Nice, your coding is getting alot better.

pr0t0typ3 - September 11, 2010, 11:14 am

(Sep 11, 2010 11:12 AM)d4rkk0 Wrote: [\[CITE\]](#) Great work, would you happen to be releasing the trick you used to get the source? :)

No I'm sorry I can't tell you as it would be bad for all owners of websites who want to protect their codes

pr0t0typ3 - September 11, 2010, 11:33 am

(Sep 11, 2010 11:30 AM)Zer0Fact0r Wrote: [\[CITE\]](#) Because I don't code in VB.NET.

I find it hypocritical how you refuse to release your "secret" method because you want to "protect" people's intellectual property yet here you are releasing their shit. All I want to do is prevent skidds from going to other websites and stealing shit ...

This was a Encryption method everyone uses so I see no reason why I should not post it ..

but if you tell them how to decrypt the javascript they can go to a website c&p it on their own and claim it as their own ...

With the code I posted they can't because it is limited to only 1 site

DEADLYGIRL - September 11, 2010, 11:34 am

This will come in handy pr0t0typ3,

may use some of your source's (I'll give credit of course) :]

pr0t0typ3 - September 11, 2010, 11:40 am

(Sep 11, 2010 11:35 AM)Zer0Fact0r Wrote: [\[CITE\]](#) Noobs don't know enough to be able to translate JS to VB.

However there is nothing stopping people from copying and pasting YOUR code (which was ripped from Crypto.com) and claiming it as their own. That is true ... Okay if I think about it it was not a good idea to call the method secret but I still think it is better to keep it with the content of 1 page instead of 100

P.S. My code was not ripped in anyway it was only the idea of the encryption ... You can't really convert JS to VB so my code is very different from theirs

bloodqman - September 11, 2010, 11:41 am

(Sep 11, 2010 11:12 AM)d4rkk0 Wrote: [\[CITE\]](#) Great work, would you happen to be releasing the trick you used to get the source? :)

while ago i've managed to download the full Crypto website, with all of its' contents...if u want i can send u the file.. ?

pr0t0typ3 - September 11, 2010, 11:43 am

(Sep 11, 2010 11:41 AM)bloodqman Wrote: [\[CITE\]](#) while ago i've managed to download the full Crypto website, with all of its' contents...if u want i can send u the file.. ? The content is encrypted/encoded so you won't have luck with that

flAmingw0rm - September 11, 2010, 12:17 pm

Very useful, thanks a lot! ?

Joler1302 - September 11, 2010, 12:46 pm

I know this guy, hes a great coder. Keep posting stuff like this, HQ member :) And thanks :)

pr0t0typ3 - September 11, 2010, 1:06 pm

(Sep 11, 2010 12:46 PM)Joler1302 Wrote: [\[CITE\]](#) I know this guy, hes a great coder. Keep posting stuff like this, HQ member :) And thanks :)

Thank you for your Feedback...

Banana_ - September 11, 2010, 3:36 pm

Would it be okay if I use these Encryptions to make a program? Basically it will be a text encoder/decoder.

Krex Productions™ - September 11, 2010, 4:05 pm

This is great mate! thanks for the share.

Svens0n - September 11, 2010, 4:07 pm

another great release from our cryptokiller :D
gr8 job

pr0t0typ3 - September 12, 2010, 1:35 am

(Sep 11, 2010 03:36 PM)FuzzyBanana92 Wrote: [\[CITE\]](#) Would it be okay if I use these Encryptions to make a program? Basically it will be a text encoder/decoder.

If you give credits it would be no problem... I'll later fix the little bug in the zara-128 decoder but then you can use all of them

Guru Security Klan - September 12, 2010, 3:39 am

could be useful, thanks :)

pr0t0typ3 - September 12, 2010, 3:45 am

(Sep 12, 2010 03:39 AM)Guru Security Klan Wrote: [\[CITE\]](#) could be useful, thanks :)

No problem.. I'm glad you like it ... I'll post the other 4 later as I'm currently writing them... The encryption is ready but the decryption needs some more work

d3c0mpil3r - September 12, 2010, 4:14 am

lol .. nice leak dude :D

I might use them later ..

Kris` - September 12, 2010, 4:44 am

Nice share man :)

toshort

Hli4S - September 12, 2010, 4:55 am

thnxxx !!! Someday these will be very usefull for me :P

drizzy_effect - September 12, 2010, 5:27 am

Awsome Nice coding hope to see more from you

WhizKidz - September 12, 2010, 6:10 am

This really great appreciated thanks prototype

pr0t0typ3 - September 12, 2010, 10:07 am

All 4 remaining Encryptions cracked and added .. Have Fun

The Weeknd. - September 12, 2010, 10:34 am

Eheh, you're so quick :D

Thank you for adding those 4!

Mr steve - September 12, 2010, 3:47 pm

Very Awesome dude!

Very cool that you figured out those 5 I've pm'd you about, I'll mos def give credits in my project ^_^

Bitwin - September 12, 2010, 3:49 pm

Good work.

Might take a look later (I don't see any use of this yet xD)

Mr steve - September 12, 2010, 4:29 pm

Just found a problem;

In the AER encryption, you can't encrypt results from a previous encryption

(like double clicking encrypt on crypto)

the error was "Cannot convert String H& to type double" or something along those lines

The method I sent you earlier does it, but I can respect you making your own code ^_^

just giving some feedback

TurokPD - September 12, 2010, 9:13 pm

thanks a lot, will look at them and probably rewrite to C# for me ...

pr0t0typ3 - September 12, 2010, 9:56 pm

(Sep 12, 2010 04:29 PM)Mr steve Wrote: [\[CITE\]](#) Just found a problem;

In the AER encryption, you can't encrypt results from a previous encryption

(like double clicking encrypt on crypto)

the error was "Cannot convert String H& to type double" or something along those lines

The method I sent you earlier does it, but I can respect you making your own code ^_^

just giving some feedback This is only a minor Problem in mine but your code was not dynamic in anyway and much different from the original.... For example : You always make $i+=5$ steps while the original code makes $i+= \text{key.length} / 2$ steps and many things more

Mr steve - September 12, 2010, 10:02 pm

(Sep 12, 2010 09:56 PM)pr0t0typ3 Wrote: [\[CITE\]](#) This is only a minor Problem in mine but your code was not dynamic in anyway and much different from the original.... For example : You always make $i+=5$ steps while the original code makes $i+= \text{key.length} / 2$ steps and many things more

Well the key is always A256-CRYPO, which divided by 2 would equal five for length.. so I just hardcoded the 5 in.

and I can tell you are a lot better at this than I am, but I did my best to make it as logically equal to the original code as possible.

Anywho, major Kudos to you for figuring it all out in such a short time frame ^_^

TurokPD - September 13, 2010, 4:19 am

is ARMON-64 really working with your code? Looks to me, that your algorithm is using fixed 4 decimal places (is default), but the online crypter somehow computes the number of decimal places.

and another comment, do you know, that e.g. "6.5" rounded with `Math.Round(6.5)` is 6 and not 7? You should use it like this `Math.Round(6.5, MidpointRounding.AwayFromZero)` to get the proper output (7). End therefor when crypting with ARMON-64 and the default key, your main cycle is getting more iterations than it is suppose to.

pr0t0typ3 - September 13, 2010, 4:43 am

(Sep 13, 2010 04:19 AM)TurokPD Wrote: [\[CITE\]](#) is ARMON-64 really working with your code? Looks to me, that your algorith is using fixed 4 decimal places (is default), but the online crypter somehow computes the number of decimal places.

and another comment, do you know, that e.g. "6.5" rounded with Math.Round(6.5) is 6 and not 7? You should use it like this Math.Round(6.5, MidpointRounding.AwayFromZero) to get the proper output (7). End therefor when crypting with ARMON-64 and the default key, your main cycle is getting more iterations than it is suppose to.

The Key is choosen by you .. the Key that is on the Encryption only page is only a example... My Code does the exact same as the original code .. They also use Round and it always works... The Number of decimal places is not that important as it is rounded in the End (I tested it with many different keys/messages)

TurokPD - September 13, 2010, 7:06 am

(Sep 13, 2010 04:43 AM)pr0t0typ3 Wrote: [\[CITE\]](#) The Key is choosen by you .. the Key that is on the Encryption only page is only a example...

My Code does the exact same as the original code .. They also use Round and it always works... The Number of decimal places is not that important as it is rounded in the End (I tested it with many different keys/messages)

well, i just copy-pasted your code into VB.net 4.0, and input "mamicka" with the default key is encrypted to 24115047656.0672+8.22688867737457, what is totally different from the online crypter. the input size is 7, so when "Do While x < Message.Length", there should be only 1 iteration of the while loop. the size of the key is 13, but because "x += Math.Round(key.Length / 2)" = "x += Math.Round(13 / 2)" is 6, not 7, it will iterate once more.

sorry if i am bothering you

littlepinuin - September 13, 2010, 8:05 am

Nice ;D

Can u find Tiger and Whirpool encryption method?

Great post ^^

TurokPD - September 13, 2010, 10:11 am

Code Public Function ARMON64_Encrypt(ByVal message As String, Optional ByVal key As String = "ARMON64-CRYPO") As String

Dim out As New System.Text.StringBuilder

If key.Length < 3 Then Return message

Dim intkey() As Byte = System.Text.Encoding.UTF8.GetBytes(key)

Dim x As Integer

Do While x < message.Length

Dim hextemp As String = ""

Dim y As String = ""

If x > 0 Then y = "+"

For i As Integer = x To Math.Round(key.Length / 2)

If i < message.Length Then hextemp += Hex(Asc(message(i)))

Next

Dim thenum As Double = "&H" & hextemp

If Information.IsNumeric(thenum) = False Then Return message

For z As Integer = 0 To key.Length - 1

Dim operation As Integer = z Mod 4

Select Case operation

Case 0

thenum += intkey(z)

```

Case 1
thenum /= intkey(z)
Case 2
thenum -= intkey(z)
Case 3
thenum *= 0.01 * intkey(z)
End Select
Next
out.Append(y & thenum)
x += Math.Round(key.Length / 2)
Loop
Return out.ToString.Replace(",", ".")
End Function

```

You are not using Round method for the output at all, so it's always rounded to the default 4 decimals, on the other hand, the online crypter apparently somehow computes the number of decimal places. They differ pretty much for each input. Aren't you forgetting something?

pr0t0typ3 - September 13, 2010, 10:42 am

(Sep 13, 2010 10:11 AM)TurokPD Wrote: [\[CITE\]](#) You are not using Round method for the output at all, so it's always rounded to the default 4 decimals, on the other hand, the online crypter apparently somehow computes the number of decimal places. They differ pretty much for each input. Aren't you forgetting something?The mod is not setting the Decimal Places or anything ... It is just for choosing the current arithmetic Function.. It does not modify the Output at all and if you would have understood the Function you would see that the Round is only needed in the Decrypt and is only used to Round Deciamls which are a little bit bigger then the wanted value (for example 1,0001233423 instead of 1)

The values are not like 1,8 or smth. there are only very small after point decimal values...

adiiforu - September 13, 2010, 10:48 am

nice one prototype!!

cools!!

i didnt mean the s bt the msg is f***ing shrt!!

TurokPD - September 13, 2010, 11:04 am

(Sep 13, 2010 10:42 AM)pr0t0typ3 Wrote: [\[CITE\]](#) The mod is not setting the Decimal Places or anything ... It is just for choosing the current arithmetic Function.. It does not modify the Output at all and if you would have understood the Function you would see that the Round is only needed in the Decrypt and is only used to Round Deciamls which are a little bit bigger then the wanted value (for example 1,0001233423 instead of 1)

The values are not like 1,8 or smth. there are only very small after point decimal values...

you probably don't understand what i am talking about. first of all, i know what mod is and its function in the crypting fuction.

as another member pointed here, your Rounding isn't working right, because rounding in JS and .net differs in special occasions. now, try to crypt message "mamicka" with your code and compare it with the online crypter output.

your code output: 24115047656,0672+8,22688867737457

online crypter output: 24115047656.06717

so, as you see, your code iterates through the main loop one more time than it's suppose to

(because the wrong rounding), therefore the "+8,22688867737457" part of your output string adding another parameter to Math.Round method like this
Math.Round(doublegoeshere, MidpointRounding.AwayFromZero) should solve this problem

another problem, is your constant default rounding (i know you are not rounding the output at all) to 4 decimals, therefor you get .0672 instead of .06717

here i am attaching a pic of debugging your code, so you see i am not kidding you
[img]http://www.chelsea.sk/hf/ARMON.JPG[/img]

PS: no offense, just trying to get it right in C# ... ?

Ironside - September 13, 2010, 11:17 am

So basically, these are functions, which you can call and parse a string to them, and it will return the encrypted string?

This is great indeed!

pr0t0typ3 - September 13, 2010, 11:21 am

Alright.. Now I get your Point... I tried it with shorter strings... and it was no problem.. I'm currently having a look at it ... btw. I fixed the Rounding of the Keylength so that is correct now...

Black-Blood™ - October 10, 2010, 12:38 am

Some decrypt functions doesn't work for me. Still good I like it =)

µnKn0wn_H4CK3r - October 10, 2010, 4:01 am

Hi!

Thanks, useful!

I think I'll translate it in C++ when I have the time.

And congratulations for Ub3r ? ! You deserve it ? .

pr0t0typ3 - October 10, 2010, 4:08 am

Thank you very much !

2 short

Kotei - November 21, 2010, 8:13 pm

Yeah, i hate to say it but most of the decrypt functions don't work.

Rotana - November 21, 2010, 8:31 pm

Great job,

Btw the keys you got in the source are that the default keys from crypto.com?

Keep on the good work

pr0t0typ3 - November 21, 2010, 9:59 pm

(Nov 21, 2010 09:13 PM)Xypher Wrote: [\[CITE\]](#) Yeah, i hate to say it but most of the decrypt functions don't work.I know there are some bugs but I simply got no time to fix them...

Kotei - November 21, 2010, 10:14 pm

(Nov 21, 2010 10:59 PM)pr0t0typ3 Wrote: [\[CITE\]](#) I know there are some bugs but I simply got no

time to fix them...

Mkay, time for me to get to work on them then. ^^

Theoc - November 22, 2010, 2:27 am

Thanks a lot dude

all credits go to you :)

phoobos - November 24, 2010, 7:34 pm

Great work, would you happen to be releasing the trick you used to get the source? :)

--

GodWall - November 24, 2010, 8:43 pm

Wow this is a gr8 share thanks

enK - November 26, 2010, 1:25 pm

I <3 you for this.

VERY MUCH <3

:D

Mr. Anderson - November 26, 2010, 1:30 pm

:d pr0t0type!

I was decrypting the javascript of the page awhile back, but I gave up :p

thanks for the awesome functions!

SIM-209986 - November 26, 2010, 1:58 pm

Thank you for these. Will be using in my project and give creds to you.

xartermate - December 18, 2010, 7:40 am

greate share prototype !!!

all encrypt but only some of those dont decrypt a very nice share of one of hf best coders.

xeers mate keep up.

made an application with all codes preety usefull for strong passwords and strings encrypting.

?Demon - December 25, 2010, 10:02 am

Thank you for this (: - Still too short -

-VeX- - December 26, 2010, 11:58 pm

hope all these still work...going to try to convert them to C# and i'll have a hard enough time if they DO work, haha. Let alone if they don't =X

nice share either way ^^

N3oNight - January 3, 2011, 2:38 pm

thank you very much for this...

this will help me a lot....

MOD3M - January 3, 2011, 4:50 pm

Very Nice. Will definitely use for an Application I'm coding. Will of Course give Credits.

Meth - January 3, 2011, 6:00 pm

(Dec 27, 2010 12:58 AM)-xPloit Wrote: [\[CITE\]](#) hope all these still work...going to try to convert them to C# and i'll have a hard enough time if they DO work, haha. Let alone if they don't =X

nice share either way ^^

Why would they stop working.

fredde_jason - January 22, 2011, 4:52 pm

Could you provide the javascripts too? :)

d3adz3r0 - February 17, 2011, 9:58 am

very useful.. thnx mate. u r gr8 :)

?Kreedz? [™] - February 17, 2011, 10:41 am

Nice release very useful thanks !

gandy3451 - February 17, 2011, 10:45 am

thanks very usefull release

infomiho - February 17, 2011, 12:19 pm

I'm going to use this someday..

So thanks !

:*

You're great :D

devil0angel - February 17, 2011, 12:33 pm

Thanks for this, if I use it somewhere will sure give you credit for it!

___R___ - March 16, 2011, 5:37 pm

thanks a lot. it really helped

Tuxx95 - March 16, 2011, 6:23 pm

Yess

Ive been looking for this!

great share so helpful

TheBarret - May 26, 2011, 4:04 pm

This looks like a very good share but i was looking at the encryptions until i noticed every (encryption) function

was the same but with a different key.

Can someone explain me what is different on the encryption other then a different key?

TheDubWubCub - May 26, 2011, 4:31 pm

OMG! I LOVE YOU SO MUCH! who ever doesnt give credits is messed up!

DragQueen - May 26, 2011, 4:45 pm

<http://www.mediafire.com/?a8pcga3i767cg67>

i can still it too :P

JL33T - May 26, 2011, 6:49 pm

My detection went lower. Thanks man!

???1zz - October 29, 2011, 8:26 pm

I can just :* you...

You helped me alot

Coleak - October 29, 2011, 8:41 pm

(Oct 29, 2011 08:26 PM)???1zz Wrote: [\[CITE\]](#) I can just :* you...

You helped me alot

You just felt the need and had to this didnt you...

razor199 - December 2, 2011, 11:10 pm

How do i use this?

```
Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
    HAZZ15_Encode(TextBox1.Text)
End Sub
```

Dont work ;(

i95swervin - December 2, 2011, 11:40 pm

lol nice job bro ..off to pastebin I go thanks again

T - December 2, 2011, 11:51 pm

(Dec 3, 2011 12:10 AM)razor199 Wrote: [\[CITE\]](#) How do i use this?

```
Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
    HAZZ15_Encode(TextBox1.Text)
End Sub
```

Dont work ;(

It works, just as you have it there. You're just not showing your encrypted text. Try:

```
Code Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
    Dim encoded as String = HAZZ15_Encode(TextBox1.Text)
    MessageBox.Show(encoded)
End Sub
```

Resident - December 3, 2011, 2:26 am

Thanks this is a great source to learn from!

pekopon321 - December 30, 2011, 11:50 pm

where should we give credits? to you or to crypto.com??

Meerkat.? - December 31, 2011, 2:12 am

Thanks a looot! This is certainly going to be helpful in future projects. Ofc with giving credits to you ;D

Spyki - December 31, 2011, 2:28 am

Nice, thanks a lot ! Very useful code.

?DiViN3 - December 31, 2011, 3:09 am

Thank you very much for leaking the code. :)

MILÃn97 - December 31, 2011, 4:08 am

You have error...

I'm coding Crypto - Encrypt / Decrypt (I'll give credits :D)

But I have problem...

See pic

<http://www.dodaj.rs/f/2F/AN/1wEhoanq/greska.jpg>

I was encoded 'Milan97' but program and crypto give diferent output...

XeSxProjects - January 1, 2012, 4:39 pm

Thank You! if i use it i will def. Give You Credit. :)

Cherish Life - January 1, 2012, 7:41 pm

HOLY SHIT. HOLY FUCKING SHIT.

You just got rep from me. This is called contribution people, this is called contribution. good job.

NetDotNet - January 2, 2012, 3:36 pm

thanks, il give you credits (:

where did you found them ??!

ElementalTree - March 24, 2014, 5:18 am

Still working great after 4 years :)

derpin0n - March 24, 2014, 11:12 am

(Mar 24, 2014 05:18 AM)ElementalTree Wrote: [\[CITE\]](#) Still working great after 4 years :)

I don't want to sound like a dick, but if you know this is 4 years old, the last post was in 2012, why are you posting? Let old threads die...

nuk - March 24, 2014, 11:27 am

Holy \$^#%!!! I needed this exact thing and have been searching for months... You are AWESOME!

Thank you so much for this ;)

SIM-1456245 - March 24, 2014, 11:52 am

People come fucking on... How do you find this new sport, Grave Digging or whatever it is called so fun.

Xch4ng3 - March 24, 2014, 6:40 pm

Grave digging isn't against the rules, no need to report it unless it breaks existing site policy.

Server97 - March 25, 2014, 12:57 am

Nice - don't release the source code.

Doctor07 - March 25, 2014, 9:50 pm

(Mar 24, 2014 11:52 AM)Electroalek Wrote: [\[CITE\]](#) People come fucking on... How do you find this new sport, Grave Digging or whatever it is called so fun.

There's nothing wrong with gravedigging, only in certain circumstances is it useless.
But this is a high quality and very useful thread to many people..
It's good that this has cropped up again for people to see.

Only3 - March 25, 2014, 10:06 pm

(Mar 25, 2014 09:50 PM)ViolentReality Wrote: [\[CITE\]](#) There's nothing wrong with gravedigging, only in certain circumstances is it useless.

But this is a high quality and very useful thread to many people..
It's good that this has cropped up again for people to see.
not really most if not all not working well and very bad coding

Doctor07 - March 25, 2014, 10:21 pm

(Mar 25, 2014 10:06 PM)Only3 Wrote: [\[CITE\]](#) not really most if not all not working well and very bad coding

I made an app using these the day they we're posted and they worked fine.

Only3 - March 25, 2014, 11:11 pm

post here ARMON64 or one of the last that work just read the replys and u understand how bad is it

Doctor07 - March 25, 2014, 11:20 pm

(Mar 25, 2014 11:11 PM)Only3 Wrote: [\[CITE\]](#) post here ARMON64 or one of the last that work cust read the replys and u understand how bad is it

I just rebuilt an application and yeah you're right. I'm pretty sure I've got a post on one of the first couple pages complaining tbh, but that was a long time ago :p