

Forum:[Hack Forums](#)

Thread: [Crystalline Cipher - Testers Required](#)

mmcc - May 12, 2015, 9:24 am

Hi everyone,

I've released a new cipher called Crystalline on CodePlex. So far, the cipher seem incredibly strong but I feel that it needs to go up against people with experience of breaking ciphers.

The reference implementation (in C#) can be found at the link below. If anyone has any questions, comments or suggestions, please feel free to reply.

crystalline (dot) codeplex (dot) com

crazyycast13 - May 12, 2015, 11:49 am

I'll check out the code later today.

mmcc - May 12, 2015, 12:53 pm

(May 12, 2015 11:49 AM)crazyycast13 Wrote: [\[CITE\]](#) I'll check out the code later today.

Thanks very much. I added a little on the theory of operation to the documentation section at Codeplex, so you may want to check it out.

If you want any deeper insights or explanations, just ask. I'll be more than happy to help. I'm still refining the algorithm around the area calculating rounds, at present I just return a hard coded value. This seems to effect the randomness of the output which is critical to its strength. I need to find a robust way of calculating this.

mmcc - May 12, 2015, 1:28 pm

(May 12, 2015 01:17 PM)cyberwebRAT Wrote: [\[CITE\]](#) What makes this a "REAL ADVANCED" crypter?

Who coded it?

I coded it and designed the algorithm and I'm quite good at data analysis. As far as I can tell at this point, there is no mathematical approach to retrieving the key or plaintext.

I've used a different approach with this cipher, in that, it shifts the location of bytes and bits. This erases information about the plaintext, replacing it information about the random sources that perform the relocation.

So, the cipher is based upon information loss, rather than hard to solve mathematics. That why I say there is no mathematical approach to breaking it.

I hope I have explained that well enough, as it is an advanced concept.

crazyycast13 - May 12, 2015, 1:44 pm

(May 12, 2015 01:28 PM)mmcc Wrote: [\[CITE\]](#) I coded it and designed the algorithm and I'm quite good at data analysis. As far as I can tell at this point, there is no mathematical approach to retrieving the key or plaintext.

I've used a different approach with this cipher, in that, it shifts the location of bytes and bits. This

erases information about the plaintext, replacing it information about the random sources that perform the relocation.

So, the cipher is based upon information loss, rather than hard to solve mathematics. That why I say there is no mathematical approach to breaking it.

I hope I have explained that well enough, as it is an advanced concept.
He's spamming this section, ignore him.

DangerZone90 - May 12, 2015, 2:07 pm

lots of infected .exe's

HUGE GIF, sorry for that?

Spoiler ([Click to View](#))[img]http://media.giphy.com/media/3o85xCCvAEEHN7BZ4I/giphy.gif[/img]

mmcc - May 12, 2015, 2:37 pm

(May 12, 2015 02:07 PM)DangerZone90 Wrote: [\[CITE\]](#) lots of infected .exe's

HUGE GIF, sorry for that?

For a second there, I thought you meant Crystalline cipher download. Phew! :)

The only .exe's in that package are builds of the cipher, which you can put through dotPeek to confirm. That's the beauty of C#, you don't need to wonder what code is lurking in the executables.

crazycast13, did you manage to checkout the code?

(May 12, 2015 11:49 AM)crazyycast13 Wrote: [\[CITE\]](#) I'll check out the code later today.
How didyou get on? Any issues?

crazyycast13 - May 15, 2015, 5:01 pm

(May 12, 2015 02:37 PM)mmcc Wrote: [\[CITE\]](#) How didyou get on? Any issues?

First of all, most people in this section never even do legit ciphers with good keys, and bastardize them, so automatic props to you.

I'm looking at your writeup and it looks pretty good, I don't see any strong bruteforce attacks from a couple of passovers but give me a little bit more time.

BTW HxD ftw

As far as the rounds go, well you can't make that random. Well you could, and then present the user with x amount outputs and let them decide, but that's just screwy. I tried that with one algo I did but eh it doesn't increase randomness by that much and instead just makes the user have more problems.

Sorry it took so long for me to respond I had to fix my computer before I could take a look.

Demoralise - May 15, 2015, 5:20 pm

I'll be willing to test this for you OP.

mmcc - May 15, 2015, 6:27 pm

(May 15, 2015 05:01 PM)crazyycast13 Wrote: [\[CITE\]](#) First of all, most people in this section never even do legit ciphers with good keys, and bastardize them, so automatic props to you.

I'm looking at your writeup and it looks pretty good, I don't see any strong brute force attacks from a couple of passovers but give me a little bit more time.

BTW HxD ftw

As far as the rounds go, well you can't make that random. Well you could, and then present the user with x amount outputs and let them decide, but that's just screwy. I tried that with one algo I did but eh it doesn't increase randomness by that much and instead just makes the user have more problems.

Sorry it took so long for me to respond I had to fix my computer before I could take a look. No worries on the late reply, I've been working around the clock myself so I wouldn't have had much time to reply. I don't like short keys, computed keys or passphrases either, I like to have a good margin of safety built in.

It's great to hear that you have found no obvious weaknesses from the tests you have run. That's a good sign at this early stage of the analysis. I was thinking of making the rounds a function of the key and salt within a defined range just to make it that little bit harder. The reason why I didn't do that was because I noticed that chi-squared tests were picking up order on different values and I need to explore the root of that. I didn't want to brush it under the carpet. I don't think it is anything serious, it just may be picking up the oscillation in the TRNG. I am writing R scripts at the minute that will explore this.

I'm having another conversation with Karl-Uwe-Frank over at DevShed and we've been discussing methods of testing this cipher. Whilst randomness tests are useful, I want to hit it with some serious machine learning techniques. I described a few of them here:

[forums\[dot\]devshed\[dot\]com/security-cryptography/969138-crystalline-cipher-testers-required-post2956397.html#post2956397](http://forums[dot]devshed[dot]com/security-cryptography/969138-crystalline-cipher-testers-required-post2956397.html#post2956397)

It's basically a death of a thousand cuts and it will reveal exactly how strong this cipher is. I suspect, given the methodology, that this will be an on-going assessment as new techniques are added. It might be an interesting exercise to make this in such a fashion that it can attack any cipher and pool the capabilities of everyone involved in cryptanalysis into some form of open-source/SaaS project that anyone can use. I don't know how popular that will be, but we'll see in time.

Keep attacking it from every angle you can think of and let me know if you spot anything. Even little things, like a pattern in the output, that you notice could be very important.

Hopefully, everyone will get to benefit from a cipher that we know with a very high confidence that no one can break.

Would you mind if I linked to this thread from the CodePlex homepage for Crystalline so that people can come and discuss attacking the cipher and/or read more?

(May 15, 2015 05:20 PM)Demoralise Wrote: [\[CITE\]](#) I'll be willing to test this for you OP. Please do. Any help you can provide will be much appreciated. If you have questions, comments or suggestions just post them and I will discuss it with you.

crazyycast13 - May 15, 2015, 6:31 pm

(May 15, 2015 06:27 PM)mmcc Wrote: [\[CITE\]](#) No worries on the late reply, I've been working around the clock myself so I wouldn't have had much time to reply. I don't like short keys, computed keys or

passphrases either, I like to have a good margin of safety built in.

Its great to hear that you have found no obvious weaknesses from the tests you have run. That's a good sign at this early stage of the analysis. I was thinking of making the rounds a function of the key and salt within a defined range just to make it that little bit harder. The reason why I didn't do that was because I noticed that chi-squared tests were picking up order on different values and I need to explore the root of that. I didn't want to brush it under the carpet. I don't think it is anything serious, it just may be picking up the oscillation in the TRNG. I am writing R scripts at the minute that will explore this.

I'm having another conversation with Karl-Uwe-Frank over at DevShed and we've been discussing methods of testing this cipher. Whilst randomness test are useful, I want to hit it with some serious machine learning techniques. I described a few of them here:

[forums\[dot\]devshed\[dot\]com/security-cryptography/969138-crystalline-cipher-testers-required-post2956397.html#post2956397](http://forums[dot]devshed[dot]com/security-cryptography/969138-crystalline-cipher-testers-required-post2956397.html#post2956397)

Its basically a death of a thousand cuts and it will reveal exactly how strong this cipher is. I suspect, given the methodology, that this will be an on-going assessment as new techniques are added. It might be an interesting exercise to make this in such a fashion that it can attack any cipher and pool the capabilities of everyone involved in cryptanalysis into some form of open-source/SaaS project that anyone can use. I don't know how popular that will be, but we'll see in time.

Keep attacking it from every angle you can think of and let me know if you spot anything. Even little things, like a pattern in the output, that you notice could be very important.

Hopefully, everyone will get to benefit from a cipher that we know with a very high confidence that no one can break.

Woud you mind if I linked to this thread from the CodePlex homepage for Crystalline so that people can come and discuss attacking the cipher and/or read more?

Please do. Any help you can provide will be much appreciated. If you have questions, comments or suggestions just post them and I will discuss it with you.

You have to realize, the amount of people in this forum who can do legit crypto is a handful, if that. Are you doing this for a university project or are you doing this just because?

Serious props either way. Serious props.

BTW <http://crypto.stackexchange.com/> is a great place with a lot of smart people who could answer some questions better than I could, same goes for <http://www.reddit.com/r/crypto>

mmcc - May 15, 2015, 8:34 pm

(May 15, 2015 06:31 PM)crazyycast13 Wrote: [\[CITE\]](#) You have to realize, the amount of people in this forum who can do legit crypto is a handful, if that. Are you doing this for a university project or are you doing this just because?

Serious props either way. Serious props.

BTW [crypto stackexchange com](http://crypto.stackexchange.com) is a great place with a lot of smart people who could answer some questions better than I could, same goes for

www.reddit.com/r/crypto

I understand that the majority of users here will have an interest but not necessarily the skillset to support that interest. I think they will find this fascinating as I will share the techniques behind how we analyse the cipher and various cutting-edge approaches to breaking them. I will use R and R Studio, which everyone can download for free, for most of this and I'll share the scripts. Hopefully, some users will pick it up as I go along. I'll start simple enough so that they can pick up the language, how to use RStudio, etc., then introduce more complex analysis into the mix. I come from a Matlab background, so I'll be using this as a way to broaden my skillset.

No, its not for University. I already hold an honours degree in Computer Science. This emerged from a very simple question I had over 5 years ago, why do most ciphers preserve the order of the plaintext in the ciphertext? I saw this as a form of leakage that provided a reference point from which cryptanalysis could begin. My only reason for doing this is because I find it interesting and that it provides good subject matter for further experimentation with machine learning and statistical tools. Crosswords and Suduko just don't hold the same appeal I suppose.

I have been to Stack Exchange, however, they are seeking focused questions that its user base can provide definitive answers for. I asked 'How secure is the Crystalline Cipher?' which is a very broad question, too broad to be answered in such a format. They placed the question on hold and requested that I reword it to narrow the focus. I will probably do that now and ask about something related to information loss. Hopefully I will be able to use the responses in the analysis in some way.

I didn't know Reddit had a crypto section. I will take a look and see what form of topics they will accept. Thanks.

TheDubWubCub - May 16, 2015, 2:04 pm

Very interesting work mmcc! ?

It's unfortunate that I lack the skills and knowledge to be able to fully comprehend and properly assist with your project, but I appreciate it immensely and wish you the best of luck towards the extensive evaluation of Crystalline. ??

From what I can tell, Crystalline already seems to do a good job at stumping people with basic crypto skills/knowledge (depending on incentives).

Seeing how you're striving for more though, "Crystalline hopes to set a new standard in security", then I suggest you keep on doing what you're doing and openly share it with the world. ?

Do you have a primary purpose for Crystalline or was it just designed with the intent for universal purposes?

Also, how are you able to incorporate 'randomness' within a cipher/encryption system? I would think that would affect its ability to decode/decrypt properly unless you're somehow storing the 'random info' within the ciphertext or something.?

Lastly, why'd you name it 'Crystalline'??

mmcc - May 16, 2015, 4:44 pm

(May 16, 2015 02:04 PM)TheDubWubCub Wrote: [\[CITE\]](#) Very interesting work mmcc! ?

It's unfortunate that I lack the skills and knowledge to be able to fully comprehend and properly assist with your project, but I appreciate it immensely and wish you the best of luck towards the extensive evaluation of Crystalline. ??

Thanks. I'm actually taking the analysis step-by-step over a Devshed if you want to learn or just watch how it is done. Karl identified an issue in the random output of the cipher but beyond output from randomness testing tools he didn't have anything concrete to demonstrate the source of the issue. I was in the process of creating code in R that could produce output suitable for machine learning when I obtained a really clear image of the repeating structure that Karl's tests were finding. Right now, that appears to be a harmonic, most likely a bias introduced by the plaintext as the frequency distribution would be off a little. So, I don't think it is anything to worry about.

Have a read:

[forums devshed com/security-cryptography-17/crystalline-cipher-testers-required-969138.html](https://forums.devshed.com/security-cryptography-17/crystalline-cipher-testers-required-969138.html)

(May 16, 2015 02:04 PM)TheDubWubCub Wrote: [\[CITE\]](#) From what I can tell, Crystalline already seems to do a good job at stumping people with basic crypto skills/knowledge (depending on incentives).

Yes, so far, no one has reported break or even provided a general methodology as to how one may be achieved other than brute force. That's a very promising sign and after I have dug a little deeper, it will be ready for analysis by some seasoned professionals and academics.

(May 16, 2015 02:04 PM)TheDubWubCub Wrote: [\[CITE\]](#) Seeing how you're striving for more though, "Crystalline hopes to set a new standard in security", then I suggest you keep on doing what you're doing and openly share it with the world. ?

That's the general idea. If a strong cipher emerges, fantastic. I'm sure people will use it. If not, everyone involved in the analysis will have added to a body of knowledge around assessing the strength of ciphers. So, there is no downside to this.

(May 16, 2015 02:04 PM)TheDubWubCub Wrote: [\[CITE\]](#) Do you have a primary purpose for Crystalline or was it just designed with the intent for universal purposes?

There is no primary purpose for the cipher. It is for general usage where security is paramount.

(May 16, 2015 02:04 PM)TheDubWubCub Wrote: [\[CITE\]](#) Also, how are you able to incorporate 'randomness' within a cipher/encryption system? I would think that would affect its ability to decode/decrypt properly unless you're somehow storing the 'random info' within the ciphertext or something.?

Its because the cipher does not encrypt data in a conventional manner. It scrambles the locations of bits and bytes using random input in a way that can be reversed. That input being the key and salt. I can reverse the process because it is performed as one long chain of bit/byte swaps.

(May 16, 2015 02:04 PM)TheDubWubCub Wrote: [\[CITE\]](#) Lastly, why'd you name it 'Crystalline'??

In a word, structure. Because the cipher changes the locations of bits/bytes in a chain, it reminded me of crystals growing. Snowflakes, quartz, the phase change between ice and water, etc. The name seemed apt.

TheDubWubCub - May 16, 2015, 5:08 pm

Quote:Thanks. I'm actually taking the analysis step-by-step over a Devshed if you want to learn or just watch how it is done. Karl identified an issue in the random output of the cipher but beyond output from randomness testing tools he didn't have anything concrete to demonstrate the source of the issue. I was in the process of creating code in R that could produce output suitable for machine learning when I obtained a really clear image of the repeating structure that Karl's tests were finding. Right now, that appears to be a harmonic, most likely a bias introduced by the plaintext as the frequency distribution would be off a little. So, I don't think it is anything to worry about.

Have a read:

[forums devshed com/security-cryptography-17/crystalline-cipher-testers-required-969138.html](https://forums.devshed.com/security-cryptography-17/crystalline-cipher-testers-required-969138.html)

Oh I see, I'll have a look! Thanks. :]

Quote:Yes, so far, no one has reported break or even provided a general methodology as to how one may be achieved other than brute force. That's a very promising sign and after I have dug a little deeper, it will be ready for analysis by some seasoned professionals and academics.

I shall try one thing and see if I get anywhere with it, (doubt it haha), but yea that'll be awesome if you can get it reviewed from them!

Quote:That's the general idea. If a strong cipher emerges, fantastic. I'm sure people will use it. If not, everyone involved in the analysis will have added to a body of knowledge around assessing the strength of ciphers. So, there is no downside to this.

Very true! :]

Quote:There is no primary purpose for the cipher. It is for general usage where security is paramount.

Even better haha good luck!

Quote:Its because the cipher does not encrypt data in a conventional manner. It scrambles the locations of bits and bytes using random input in a way that can be reversed. That input being the key and salt. I can reverse the process because it is performed as one long chain of bit/byte swaps. Okay gotcha, never mind then. :)

Quote:In a word, structure. Because the cipher changes the locations of bits/bytes in a chain, it reminded me of crystals growing. Snowflakes, quartz, the phase change between ice and water, etc. The name seemed apt.

haha awesome, and have you made other crypto systems before? and for what purpose? (little or small? for fun or work?)

mmcc - May 16, 2015, 5:13 pm

(May 16, 2015 05:08 PM)TheDubWubCub Wrote: [\[CITE\]](#) haha awesome, and have you made other crypto systems before? and for what purpose? (little or small? for fun or work?)

Would you believe me if I said it was my very first attempt? :)

TheDubWubCub - May 16, 2015, 6:54 pm

(May 16, 2015 05:13 PM)mmcc Wrote: [\[CITE\]](#) Would you believe me if I said it was my very first attempt? :)

lol, what's your usual type of work? Nice first try haha. :D

mmcc - May 16, 2015, 7:17 pm

(May 16, 2015 06:54 PM)TheDubWubCub Wrote: [\[CITE\]](#) lol, what's your usual type of work? Nice first try haha. :D

Distributed computing, machine learning, artificial general intelligence and cloud-based systems. More recently, cloud based e-commerce systems. The cipher is just something toy with during my free time, transfer my Matlab skillset to R, improve my machine learning skillset on extracting knowledge from noisy data and, of course, maintain my skillset in distributed computing. All the techniques are transferable, so its a good way to keep on top of things.

How about yourself? What line of work are you in?

TheDubWubCub - May 16, 2015, 8:36 pm

(May 16, 2015 07:17 PM)mmcc Wrote: [\[CITE\]](#) Distributed computing, machine learning, artificial general intelligence and cloud-based systems. More recently, cloud based e-commerce systems.

The cipher is just something to play with during my free time, transfer my Matlab skillset to R, improve my machine learning skillset on extracting knowledge from noisy data and, of course, maintain my skillset in distributed computing. All the techniques are transferable, so it's a good way to keep on top of things.

How about yourself? What line of work are you in?

Very nice man, and no wonder your first cipher is doing so well haha.

Currently unemployed and just going to school. :P

Here on HF, I host little crypto contests and do what I can within the 'crypto' community haha.

All of this techie/crypto stuff is more of a hobby for me mainly because I have no clue which direction I want to pursue; which makes progression difficult at times. :P

Anyways, welcome to HF & hope your stay is awesome possum. :D

mmcc - May 17, 2015, 3:57 am

(May 16, 2015 08:36 PM)TheDubWubCub Wrote: [\[CITE\]](#) Very nice man, and no wonder your first cipher is doing so well haha.

Currently unemployed and just going to school. :P

Here on HF, I host little crypto contests and do what I can within the 'crypto' community haha.

All of this techie/crypto stuff is more of a hobby for me mainly because I have no clue which direction I want to pursue; which makes progression difficult at times. :P

Anyways, welcome to HF & hope your stay is awesome possum. :D

We've all been there at some point. Actually, in the IT world you will find that it can happen multiple times. Sometimes people follow a certain career path and simply get bored with it, only to return to study and follow a different one. If you enjoy your career and can make a decent living pursuing it, that's all that matters I suppose. What are you studying at the minute?

TheDubWubCub - May 17, 2015, 10:47 am

(May 17, 2015 03:57 AM)mmcc Wrote: [\[CITE\]](#) We've all been there at some point. Actually, in the IT world you will find that it can happen multiple times. Sometimes people follow a certain career path and simply get bored with it, only to return to study and follow a different one. If you enjoy your career and can make a decent living pursuing it, that's all that matters I suppose. What are you studying at the minute?

I'll pm you so that this thread doesn't get too bogged down with our conversation haha.

mmcc - May 17, 2015, 6:37 pm

(May 17, 2015 10:47 AM)TheDubWubCub Wrote: [\[CITE\]](#) I'll pm you so that this thread doesn't get too bogged down with our conversation haha.

I can't reply to PMs yet. I'm still a new user.

I have uploaded an RStudio project at DevShed which I will be using as the primary testing tool to analyse Crystalline. If anyone wants to join in, learn a little and play around. Then download a copy of RStudio, R and the project and join in. RStudio and R can be downloaded for free. I have kept this generic enough so that it can be used to analyse any cipher, so in time it will become a very useful tool to have around.

The RStudio project can be found here:

forums devshed

com/security-cryptography/969138-crystalline-cipher-testers-required-post2956486.html#post2956486

TheDubWubCub - May 23, 2015, 4:24 pm

Hello again! :D

I've converted the C# project to vb so I and any others can understand and work with it a bit easier. Just pm me for the converted project if you need it.

I plan on trying a couple of things to see if any distinct critical patterns or anything really shows up, I'll keep ya updated. :]

mmcc - May 23, 2015, 7:11 pm

Actually, I am in the middle of rewriting the cipher for the Beta 3 release. The core algorithm remains the same, but there are extensive changes around keys, salts, IVs, etc., to support multiple byte arrays. I also changed how the circular buffers function, rather than looping from 0 to EOF for the plaintext, repeating the key and salt, I have created a type of randomly driven gearbox. There is no point in analysing the current code for patterns as this new functionality will drastically change the output.

I've also added functionality to automate the production of test output suitable for analysis. The eventual hope is to import the JSON description of the output into the RStudio project and automate the entire analysis stage.

I'm hoping to get this out sometime tomorrow (probably late tomorrow), so you will be able to update your VB code then.

TheDubWubCub - May 23, 2015, 7:22 pm

(May 23, 2015 07:11 PM)mmcc Wrote: [\[CITE\]](#) Actually, I am in the middle of rewriting the cipher for the Beta 3 release. The core algorithm remains the same, but there are extensive changes around keys, salts, IVs, etc., to support multiple byte arrays. I also changed how the circular buffers function, rather than looping from 0 to EOF for the plaintext, repeating the key and salt, I have created a type of randomly driven gearbox. There is no point in analysing the current code for patterns as this new functionality will drastically change the output.

I've also added functionality to automate the production of test output suitable for analysis. The eventual hope is to import the JSON description of the output into the RStudio project and automate the entire analysis stage.

I'm hoping to get this out sometime tomorrow (probably late tomorrow), so you will be able to update your VB code then.

I see, could you elaborate on the 'randomly driven gearbox'? :D

Oh nice, haha good luck with it.

Ok cool, just post it when you can & I'll do so. ?