

Forum:[Hack Forums](#)

Thread: [Introduce me in cryptography](#)

Niely - July 29, 2014, 2:58 pm

Hello

I want to slightly get more in cryptography. :)

I think it's always a nice skill to have in the back of your head.

But, I have some questions:

Are there good free pdf books about it? Already searched but found nothing.

How do you guys see what kind of encryption is used? I can only recognize Base64. ?

Is it possible to make your own algorithm?

What kind of programs do you use to crack hashes and filter the salt (who also work for Linux).

Anything else? :)

I only know a bit about cryptography now, like public and private keys, know what hash-salts are (salts are some random extra characters given to that hash).

And some basics about bits (not sure if that helps).

That 123.45.72 is 32-bit (IPv4) for example. :)

...

Anyway,

Thanks for reading,

Niely

crazyycast13 - July 29, 2014, 3:02 pm

If you want to take a fast dive into cryptography, go to <http://crypto.stackexchange.com/> and whenever you have a question, search on Google or go to Wikipedia.

<http://cacr.uwaterloo.ca/hac/index.html> <-- that is now your handibook.

<http://www.amazon.com/Beginning-Cryptography-Java-David-Hook/dp/0764596330> This was the first crypto book I got, it's very helpful if you already know Java and teaches you how to use the different crypto algos located inside the bouncycastle API. HOWEVER, do not use the bouncycastle's random number generator as Java made theirs a lot better than expected, and bouncycastle's isn't distributed well on a randomization curve.

If you follow the quest to solve 3301's puzzles, you will learn a lot about steganography, a lot of different algos, magical ciphers, and many, many other things, so it's good to have a look at that too.

Finally, Forezza, Chink3nman, TheDubWubCub, and myself are all good people to pm if you have questions.

Forezza - July 29, 2014, 3:40 pm

It's good to see that you want to learn but cryptography is a massive subject to try cover. There are coursera courses for it but you don't start at the basics and it's quite hard to pick up. The best bet for now is sort by rating in this section and you'll get some semi-decent threads to read (weeds out

most of the crypter shit). I can write a very basic writeup when I get home, but still that is going to take some time.

Regarding your questions though:

-> There are PDF books, but I'm not sure if they really cover the subject that well.

-> Base64 is a type of encoding rather than a way to encrypt data. You can tell this because you don't need any key or additional information to be able to reverse the base64 output. You can't really identify encryption algorithms that well unless they are unique such as have a lot of dots to split data, etc.

-> Yes, you can make your own algorithm but it's not recommended. The current encryption algorithms that are used by most have been tested vigorously for years to become approved as standards.

-> oclHashcat (Requires usage of your graphics card) and Hashcat (CPU-based) is probably the best and most common hash cracking program.

Niely - July 30, 2014, 12:19 am

Thanks all for your help! :)

Will help me further for sure, taking a look at all of them now.

TheDubWubCub - July 30, 2014, 2:37 am

Just saw this thread & rushed to respond, but it looks like Forezza and crazyycast13 beat me too it. Everything they've said is spot on & very informative! I wish there were more people like them and you on this forum!

Below is just some more information that will hopefully help you out in this chaotic world of Cryptography. ?

Wanna make your own code?!:

Spoiler ([Click to View](#))

Even though code making isn't recommended if you plan on securing data with it, feel free to make codes just for fun or to challenge others.

It can defiantly give you & others an awesome learning experience/perspective in the cryptography world.

If you plan on making your own codes, I suggest you go back in time & learn about as many ciphers & codes as you can. (Check my video suggestions)

Learn about how they were made, why/how they were strong/weak, how they were cracked, and just an overall understanding on the cipher/codes.

Now just go crazy & make your own!

(Start small/simple though, the initial point is to learn & just have fun with it! ?)

If you still wish to make your own code to secure data, you should read about [Kerckhoffs' principle](#) first, test your algorithm vigorously, publicize it to be peer-reviewed, Consult multiple certified Cryptographers, revise & repeat, and be prepared for the worst. (Or take the most common route: Stick to the standards, or Secure your data through obscurity & hope for the best lol)

Good luck! ?

Identifying algorithms:

Spoiler ([Click to View](#))

When it comes to identifying codes, a lot of it is just having a large knowledge base of various types of codes along with some educated guesses & some testing.

If you've ever heard about <http://crypto.in.ua/tools/> , here's a thread that shows you how to identify some of the algorithms used on that website: (More recent threads have been made, but idunno where they are haha)

<https://hackforums.net/showthread.php?tid=2495136>

(Or you could just visit the website & input your own data & study their outputs)

Here's a website where you can input your own data & it will hash it with a bunch of hashing algorithms. From there, you can study their outputs to find patterns that are unique to those specific hashing algorithms.

<http://www.insidepro.com/hashes.php> (it's been updated since this post, so just look up hash identifiers)

(Someone should make an updated thread with as much algorithms as they can and then just constantly update it with new submissions/posts of how to identify other certain algorithms! haha ?)

Video Content:

Spoiler ([Click to View](#))

Ok, I probably have too many video suggestions... nahhh haha

Some of them, if not all, are really worth checking out!:

(Intro/warm-up)

Encryption Part I: Introduction to Encryption 1 (12 videos)

<https://www.youtube.com/watch?v=vCDe14NxSY0>

Cryptography 101 - The Basics

<https://www.youtube.com/watch?v=fNC3jCCGJ0o>

Gambling with Secrets:

<https://www.youtube.com/watch?v=llCOtR078Gw&list=PLB4D701646DAF0817>

The Science Of Secrecy Pt1:

https://www.youtube.com/watch?v=_ZTWLAqYf9c

The Science of Secrecy Pt2:

https://www.youtube.com/watch?v=oR0_LPbWxe4

Modern Marvels - A Brief History of Cryptography:

<https://www.youtube.com/watch?v=H9Cu36Qj3dQ>

A brief history of Cryptography with Akamai:

<https://www.youtube.com/watch?v=alpnKaPoUZ8>

(Ciphers)

25 Famously Unsolved Ciphers And Codes That You Won't Be Able To Break:

<https://www.youtube.com/watch?v=RVYtxrm9yRA>

Caesar Cipher:

<https://www.youtube.com/watch?v=sMOZf4GN3oc>

Vigenère Cipher:

<https://www.youtube.com/watch?v=47BHvzLdPxw>

Playfair Cipher:

<https://www.youtube.com/watch?v=quKhvu2tPy8>

I would recommend getting this book to learn a little more about different ciphers:

<http://www.amazon.com/Super-Little-Giant-Book%C2%AE-Secret/dp/1402737394>

I have it & can give you a few samples of the book to see if you'll like it. ?

(Enigma/WWII stuff)

158,962,555,217,826,360,000 - Numberphile:

https://www.youtube.com/watch?v=G2_Q9FoD-oQ

Flaw in the Enigma Code - Numberphile:

<https://www.youtube.com/watch?v=V4V2bpZlqx8>

Code Breakers - The Rise of The Enigma:

https://www.youtube.com/watch?v=5vC5f_Pwmdw&list=PL04ABB8A86B3A2222

World War II Code Breakers:

<https://www.youtube.com/watch?v=9hAzmh6XSr8&list=PL458B94A560A6D0C6>

World War II Mind of a Code Breaker:

<https://www.youtube.com/watch?v=-ITPAbYScIw&list=PLAD3BB14F42437555>

Station X - The codebreakers of Bletchley Park:

<https://www.youtube.com/watch?v=T-Q3Zv582Q0&list=PL969A3150AB13812A>

Secrets of World War II: The Enigma Secret 1998:

https://www.youtube.com/watch?v=RcK_9wyxLNM

(Not so much crypto, but still informative)

Decimal, Binary, Octal & Hexadecimal:

<https://www.youtube.com/watch?v=5sS7w-CMHkU>

Binary Numbers in 60 Seconds:

<https://www.youtube.com/watch?v=qdFmSIFojlw>

Don't encrypt passwords:

https://www.youtube.com/watch?v=FYfMZx2hy_8

(Modern Encryption)

Modern Cryptography:

<https://www.youtube.com/watch?v=8CluknrLeys&list=PLP6PHJ8SLR6AA93UEXGaDFUDc8paCCsiD>

Encryption and HUGE numbers - Numberphile:

<https://www.youtube.com/watch?v=M7kEpw1tn50>

Prime Adventure:

<https://www.youtube.com/watch?v=zCh4q-XoTP0&list=PLbg3ZX2pWlgKZ0eR9lviOkeagDuSPI89K>

Intro to AES Encryption:

https://www.youtube.com/watch?v=dIS5_qfxAss&list=PLDCC9179604F435AB

AES - a Conceptual Review:

<https://www.youtube.com/watch?v=liKXtikP9F0>

Prime Numbers & Public Key Cryptography

<https://www.youtube.com/watch?v=56fa8Jz-FQQ>

SSL Explained:

<https://www.youtube.com/watch?v=SJJmoDZ3il8>

What is HTTPS:

<https://www.youtube.com/watch?v=JCvPnwpWVUQ>

Hashing Algorithms and Security - Computerphile

<https://www.youtube.com/watch?v=b4b8ktEV4Bg>

The Fathers of Quantum Cryptography:

<https://www.youtube.com/watch?v=0fr-N-Kf2qU>

Introduction to Quantum Cryptography & Tokyo QKD Network:

<https://www.youtube.com/watch?v=tG9ZiMLanhE>

Quantum Cryptography: A Tale of Secrets Revealed Through the Laws of Physics:

<https://www.youtube.com/watch?v=NejFo5hKcOg>

Advances in quantum cryptography for free-space communications:

<https://www.youtube.com/watch?v=ovQuFWA2BbU>

Check out these 4 Youtube channels:

<https://www.youtube.com/user/kirankuppa>

<https://www.youtube.com/user/TheIACR>

<https://www.youtube.com/user/ArtOfTheProblem>

<https://www.youtube.com/user/khanacademy>

(Stanford Cryptography Videos)

Not in order, but here's the playlist:

https://www.youtube.com/watch?v=WjdJ4426eE0&list=PLXIdE02sTBD-DkOmnxKX6fU6tArIMP_mv&

[index=41](#)

I think here is a good place to stop haha, but yea I hope you enjoy the content! ?

Other info:

Spoiler [\(Click to View\)](#)

Not a bunch of info here, but just little things that you might like. ?

Wanna participate in some challenges?!

Feel free to PM me & I'll notify you when I host some challenges (there's prizes most of time?).

OR check out this amazing site where they have tons of challenges!

<https://www.mysterytwisterc3.org/en/>

Just in case your curious, here's a thread on how to encode/decode Base64 via paper & pen:

<https://hackforums.net/showthread.php?tid=3331128>

Considering the learning potential, you should also check out:

<http://s13.zetaboards.com/Crypto/index/>

It's a nice Crypto forum and you might learn something from there, and if you do and don't see that it's been posted about here, then go ahead & make thread about it to share the knowledge. ?

I have various books & ebooks on cryptography, none programming related though ./, if you're interested then just PM me.

Here's one recommended by chick3nman:

<http://cacr.uwaterloo.ca/hac/>

There's so much more to learn about, but I think we've scratched a good surface so far. :P

If you actually take all of this information in that we all have provided & retain it, then you'll be good to go and be able to dive deeper into the vast world of cryptography... without any floaties.. ?

Niely - July 30, 2014, 2:45 am

^Thank you very much for the reply! :D

Was also very helpful, will also use those URLS for sure!

TheDubWubCub - July 30, 2014, 2:47 am

(Jul 30, 2014 02:45 AM)Niely Wrote: [\[CITE\]](#) ^Thank you very much for the reply! :D

Was also very helpful, will also use those URLS for sure!

Sounds good! Like crazyycast13 said, If you need anything then just contact one of us. ?

crazyycast13 - July 30, 2014, 2:57 am

(Jul 30, 2014 02:47 AM)TheDubWubCub Wrote: [\[CITE\]](#) Sounds good & if you need anything, just contact one of us. ?

Where the hell have you been? You disappeared from this section for at least two months, if not four.

But he's right, we're all open to help. What do you want to do with cryptography though? Make crypters? (please don't say that) Make your own crypto algos? Crack hashes using attacks other than the standard bruteforce/dict attack? Work on implementing security into websites? Make it so that an application is less likely broken by adding Run Time Encryption?

There are a lot of things you can do.

TheDubWubCub - July 30, 2014, 3:03 am

(Jul 30, 2014 02:57 AM)crazyycast13 Wrote: [\[CITE\]](#) Where the hell have you been? You disappeared from this section for a month or two.

But he's right, we're all open to help. What do you want to do with cryptography though? Make crypters? (please don't say that) Make your own crypto algos? Crack hashes using attacks other than the standard bruteforce/dict attack? Work on implementing security into websites? Make it so that an application is less likely broken by adding Run Time Encryption?

There are a lot of things you can do.

haha I've still been here, I just haven't been posting.

I've spent most of the time at that other [forum](#). ?

You've been doing an awesome job in this section though! ?

I got a contest coming up soon, you wanna be notified when it starts? :]

Niely - July 30, 2014, 3:06 am

(Jul 30, 2014 02:57 AM)crazyycast13 Wrote: [\[CITE\]](#) Where the hell have you been? You disappeared from this section for at least two months, if not four.

But he's right, we're all open to help. What do you want to do with cryptography though? Make crypters? (please don't say that) Make your own crypto algos? Crack hashes using attacks other than the standard bruteforce/dict attack? Work on implementing security into websites? Make it so that an application is less likely broken by adding Run Time Encryption?

There are a lot of things you can do.

I do want to make crypters (not those vb.NET things but real C++ ones).

But that's not why I want to learn cryptography.

I want be able to crack hashes, and learn those algorithms and be able to decrypt them.

Also, I want be able to secure my data when communicating with other's (public and private keys). :)

Unauthenticated - July 30, 2014, 9:31 pm

Well I've just found this crazyycast123, I can start over here, ignore my pm

Niely - July 31, 2014, 9:01 am

I installed OclHashcat, but it won't open (Linux).

I tried the bin, exe, and app. :)

Unauthenticated - July 31, 2014, 9:35 am

Niely I don't know what you tried to install but if you're trying to install something in linux look up for the ".tar" files

Niely - July 31, 2014, 10:12 am

^The installation was successful. :)

I have a folder including Hashcat but the file won't open.

PoHem - *December 30, 2014, 4:32 pm*

This is just a beautiful thread for someone just getting into cryptography! Thank you guys!

dendrobates - *November 3, 2015, 11:20 pm*

neily i can help u install hashcat. pm me if u still need help