

Forum:[Hack Forums](#)

Thread: [Introductory Cryptographic Concepts](#)

lwristz - September 30, 2017, 10:13 pm

Disclaimer ([Click to View](#)) Greetings friends, I've done a lot of reading and really appreciate the resources this forum has to offer. This section is filled with so much potential, but instead of complaining about how it can be better, I will try and contribute a little to it. I was told that I could implement more detail, however, I had a difficult time finding the sweet spot between more info and the character limit I found. Please do not think I was lazy, I would have much preferred to include said information.

What is encryption and why should I care?

Code In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

~Integrity~

Code The concept of integrity insures that data has not been modified. We use "hashing" to ensure that integrity is retained. What is a hash? A hash is a number that is derived from performing a calculation on the data. Hashing cannot be reversed, which is why it is used so commonly in assuring integrity. (Take every absolute in technology with a grain of salt.) Safer practice to say, "in theory, hashing cannot be reversed."

Think of hashing like a glass window. If I threw a stone and shattered a glass window, you wouldn't be able to put it back together perfectly. With hashing, if I modify any part of a file, the hash will not return the same as the original hash.

Hashes are used for...Verifying the integrity of files or messages

Password verification

Proof-of-work

File or data identifier

Pseudorandom generation and key derivation

Popular hash functions...

MD5

SHA-1

SHA-256

RIPEMD

Click [here](#) to see all the hash functions side by side.

~Confidentiality~

Code When we talk confidentiality which is for intended audiences only, we are talking about ensuring the secrecy of certain content. This is where ENCRYPTION comes in.

Encryption scrambles/ciphers data to make it unreadable if intercepted. It heavily uses algorithm/keys.

There are two main forms of encryption. Asymmetric and symmetric.

~Let's take a look at Asymmetric Encryption.~

Spoiler ([Click to View](#))

Compared to the asymmetric encryption.

Spoiler ([Click to View](#))

~What's more secure?~

[Click here to find out](#). Asymmetric schemes seem to be more secure, but what are we measuring? Algorithmic encryption strength by itself? Mathematical involvement? The way keys are published?

~Types of Asymmetric Encryption~

Asymmetric Encryption involves a public key/private key. If you're keeping up with this concept, that means there are TWO keys. The public key is as the name implies, publicly published where the private key is maintained in secrecy again, as implied by the name.

~Asymmetric Encryption is often used for confidentiality and can be seen implemented in digital signatures.~

Code Anyone with the public key is able to encrypt a message, providing confidentiality, and then only the person in possession of the private key is able to decrypt it.

~Asymmetric Algorithms~[DSA](#)

[Elliptic curve cryptography](#)

[RSA](#)

[Diffie-Hellman key exchange](#)

[Key Serialization](#)

[X25519 key exchange](#)

~Symmetric-Key Algorithm~

Code Are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

~Several ways of encryption.~

~Block Ciphers~

Code Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits were commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001, and the GCM block cipher mode of operation use 128-bit blocks.

~Stream Ciphers~

Code Stream ciphers encrypt the digits (typically bytes) of a message one at a time.

I've found two diagrams that best describe this concept.

Block Ciphers ([Click to View](#))

Stream Ciphers ([Click to View](#))

~Symmetric Implementations~

[Twofish](#)

[Serpent](#)

[AES](#)

[Blowfish](#)

[CAST-128](#)

[Kuznyechik](#)

[RC4](#)

[3DES](#)

Targus - September 30, 2017, 10:26 pm

Most of the examples you've mentioned are all contemporary instead of diving down to the very basics like Caesar Cipher (ROT), Vignere Cipher, Substitution Cipher, and so on for symmetric encryption (this doesn't apply for asymmetric). Not trying to say that it's wrong, but IMO you should use something simple as a starting point and go deeper from there.

Also, your thread formatting is a bit of a pain to my eye. The combination of those small-sized fonts along with several bright colours doesn't bode well. You might want to use special formatting for text that deserves special attention from the rest.

Cagey - September 30, 2017, 10:28 pm

Very HQ thread thank you for contributing, posting so I can read later though

lwristis - September 30, 2017, 10:29 pm

(Sep 30, 2017 10:26 PM)Targus Wrote: [\[CITE\]](#) Most of the examples you've mentioned are all contemporary instead of diving down to the very basics like Caesar Cipher (ROT), Vignere Cipher, Substitution Cipher, and so on for symmetric encryption (this doesn't apply for asymmetric). Not trying to say that it's wrong, but IMO you should use something simple as a starting point and go deeper from there.

Also, your thread formatting is a bit of a pain to my eye. The combination of those small-sized fonts along with several bright colours doesn't bode well. You might want to use special formatting for text that deserves special attention from the rest.

Thank you for the feedback. You're correct. I tried to keep it to more contemporary forms of encryption. Would you like to work together on a thread that goes into the basic implementations? Also, I will fix the colors as we speak. :) Really appreciate it.

Targus - September 30, 2017, 10:39 pm

(Sep 30, 2017 10:29 PM)oxid Wrote: [\[CITE\]](#) Thank you for the feedback. You're correct. I tried to keep it to more contemporary forms of encryption. Would you like to work together on a thread that goes into the basic implementations? Also, I will fix the colors as we speak. :) Really appreciate it. Sure. If you have XMPP, do send me your contact information through PM.

lwristis - September 30, 2017, 10:41 pm

(Sep 30, 2017 10:39 PM)Targus Wrote: [\[CITE\]](#) Sure. If you have XMPP, do send me your contact information through PM.

I have a discord which I will now relay to you.

Not Your Average Orange - October 1, 2017, 8:36 am

Thanks for the tutorial. What would be the best free crypter to crypt my rat? I need it to be undetectable for 3 days.

/s

But in all seriousness, it's a good in depth tutorial.

lwrists - October 1, 2017, 8:40 am

(Oct 1, 2017 08:36 AM)Not Your Average Orange Wrote: [\[CITE\]](#) Thanks for the tutorial. What would be the best free crypter to crypt my rat? I need it to be undetectable for 3 days.

In California, trolling Internet posts will get you EXECUTED.

The.Businessman - October 1, 2017, 10:15 am

Great Thread :)

Amazing Thread, Great Thread Layout BTW

lwrists - October 1, 2017, 10:36 am

(Oct 1, 2017 10:15 AM)The.Businessman Wrote: [\[CITE\]](#) Great Thread :)

Amazing Thread, Great Thread Layout BTW

Much appreciated! I hope people are able to use it as a reference.

Soulmate~?? - October 1, 2017, 10:37 am

Nice thread, covers the basics pretty well.

lwrists - October 1, 2017, 10:38 am

(Oct 1, 2017 10:37 AM)Soulmate~?? Wrote: [\[CITE\]](#) Nice thread, covers the basics pretty well.

?

Approval from you makes me cream my panties.

theBallistic - October 1, 2017, 10:40 am

Nice thread! I'm trying to get into cryptography and hashing and all that fun stuff, and this is a great start! Thanks OP, I'll take out my notebook now :)

lwrists - October 1, 2017, 10:42 am

(Oct 1, 2017 10:40 AM)theBallistic Wrote: [\[CITE\]](#) Nice thread! I'm trying to get into cryptography and hashing and all that fun stuff, and this is a great start! Thanks OP, I'll take out my notebook now :)

Certainly. I am working with Tarus to release a co-op'd thread for the introductory implementations. I will hit him up today.

M?xim - October 1, 2017, 3:03 pm

Congratulations on the Sticky Man award! @oxid

lwrists - October 1, 2017, 3:15 pm

(Oct 1, 2017 03:03 PM)Maxim Wrote: [\[CITE\]](#) Congratulations on the Sticky Man award! @oxid

Thanks! The admin forgot to pin the thread haha! You have 4 of these badges?!

M?xim - October 1, 2017, 3:17 pm

(Oct 1, 2017 03:15 PM)oxid Wrote: [\[CITE\]](#) Thanks! The admin forgot to pin the thread haha! You have 4 of these badges?!

It's suppose to not be pinned. To respect the ones who have paid to have their thread stickied. But yeah, lol.

/wrists - October 1, 2017, 3:21 pm

(Oct 1, 2017 03:17 PM)Maxim Wrote: [\[CITE\]](#) It's suppose to not be pinned. To respect the ones who have paid to have their thread stickied.

But yeah, lol.

Oh! Okay, how do I PM the admin. I accidentally told him that he forgot to pin it.

Metallic Silver - October 1, 2017, 3:30 pm

Good work on this thread even though we rough eachothers jimmies.

Well written

/wrists - October 1, 2017, 3:32 pm

(Oct 1, 2017 03:30 PM)Metallic Silver Wrote: [\[CITE\]](#) Good work on this thread even though we rough eachothers jimmies.

Well written

Thanks for support and I hope you've learned something! :)

Aura - October 2, 2017, 3:56 pm

so hq, much wow, very gud

/wrists - October 2, 2017, 4:16 pm

(Oct 2, 2017 03:56 PM)Aur? Wrote: [\[CITE\]](#) so hq, much wow, very gud thanks for THEE support.

U5sqqA6EnveZDnz2Vr5W - October 2, 2017, 6:10 pm

The first reply to this thread is right, this is not an introduction to cryptography, the semantics are not quite right and the thread does not actually explain anything, it is rather represented as a list.

It would be better if you started by the step-by-step explanation of the construction of a simple encryption algorithm like the first reply specifies, explaining the behinds of RSA can be a really good example, RSA is simple, easy to implement (even if not recommended unless you make sure that it is audited by a community of experts), and really straight forward to understand.

Cryptography is not about what exists today, it is about changing data around with an algorithm that cannot (or at least, keep cryptographers busy for long enough) be re-engineered to be faster. (not talking about computers here but math)

There is as well interesting benefits when it comes to certain schemes such as asymmetric encryption, making exchange of confidential data actually private (or at least, until proven otherwise).

A shorter path is what you want to avoid, common way of finding attacks involve data analysis on similarities, repeated sequences or associations in the different inputs of the algorithm, like the keys and data, and the outputs. There's generic ways to uncover anomalies on encryption algorithms. Sometimes the flaw is hidden so well that it can keep a whole community of cryptographers busy for decades, it is why cryptography is not so reliable at the end because most of humans don't understand cryptography (or at least, don't try to), and that a malicious actor could easily make up a vulnerable but secure-looking algorithm for everyone to use and feel private with, but for the malicious actor to spy on.

You can show examples of what has been done using cryptography but in my opinion, it is out of scope to expand for a tutorial about cryptography, cryptography is about understanding, making and breaking encryption algorithms.

/wrists - October 2, 2017, 6:34 pm

(Oct 2, 2017 06:10 PM)U5sqqA6EnveZDnz2Vr5W Wrote: [\[CITE\]](#) The first reply to this thread is right,

this is not an introduction to cryptography, the semantics are not quite right and the thread does not actually explain anything, it is rather represented as a list.

It would be better if you started by the step-by-step explanation of the construction of a simple encryption algorithm like the first reply specifies, explaining the behinds of RSA can be a really good example, RSA is simple, easy to implement (even if not recommended unless you make sure that it is audited by a community of experts), and really straight forward to understand.

Cryptography is not about what exists today, it is about changing data around with an algorithm that cannot (or at least, keep cryptographers busy for long enough) be re-engineered to be faster. (not talking about computers here but math)

There is as well interesting benefits when it comes to certain schemes such as asymmetric encryption, making exchange of confidential data actually private (or at least, until proven otherwise).

A shorter path is what you want to avoid, common way of finding attacks involve data analysis on similarities, repeated sequences or associations in the different inputs of the algorithm, like the keys and data, and the outputs. There's generic ways to uncover anomalies on encryption algorithms. Sometimes the flaw is hidden so well that it can keep a whole community of cryptographers busy for decades, it is why cryptography is not so reliable at the end because most of humans don't understand cryptography (or at least, don't try to), and that a malicious actor could easily make up a vulnerable but secure-looking algorithm for everyone to use and feel private with, but for the malicious actor to spy on.

You can show examples of what has been done using cryptography but in my opinion, it is out of scope to expand for a tutorial about cryptography, cryptography is about understanding, making and breaking encryption algorithms. Correct, this is a reference. We will be coming out with a more detailed implementation guide soon. If you read the title, you would understand why. I was unupgraded at the time and my maximum character was 8000, I believe.

CODEHACKER4U - *October 15, 2017, 11:05 am*

wow that is greate am really new to cryptographic... i have learnt something

SIM-2564555 - *November 13, 2017, 1:23 am*

Good thread and a lot of efforts thank you Bro

predatorvj - *November 14, 2017, 10:21 am*

Splendid. Enjoyed every word of the this thread