Title: The Science of Secrets
Author: satoshi_notmemoto
Created 2022-03-16 21:02:40 UTC
Permalink: /r/DDintoGME/comments/tft34l/the_science_of_secrets/
Url: https://www.reddit.com/r/DDintoGME/comments/tft34l/the_science_of_secrets/

GLVEKMKMGNMPXPWDFBXPABKFPZYCDMEPXTWCGMCEKYASZXUZZVYSGLEGGGCI

Do you see the string of characters above? Wonder what it means? I bet you do, but, unfortunately, unless I made a mistake, tell you, or give you the key, you will never know the true meaning of the above. Kinda cool, isn't it? That's just one of the things cryptography can be used for. Cryptography is the reason we get to have nice things in our ever-growing digital world(s). I'm talking about everything. From the last item you ordered from GameStop to state secrets. Even the creation of computers themselves has cryptography to thank.

Up until recently, cryptography has primarily remained in the background. Cryptography has been gaining more attention with blockchain, cryptocurrencies, NFTs, and other decentralized technologies. As we know, GameStop's future with NFTs, blockchain, and things of the sort is definite. Therefore, it's good to have a basic idea of the tools used to build these new technologies. I plan to go into more depth about each specific technology and how it relates to GameStop and the bigger picture in other posts. However, they will require some basic knowledge of cryptography. This post aims to serve as a foundation for upcoming posts. Also, I wanted to dedicate my first "real" post to cryptography because, if my username hasn't already given it away, I'm an enormous crypto enthusiast. I genuinely believe this GameStop saga is only the beginning act of whatever it is we're participating in right now. Crypto and decentralized technologies are what's going to take us all the way.

This post is intended as an overview. If you want more info on anything, you can always reach out to me. Or use Wikipedia. I know your teachers didn't want you to, but our chairman clearly does. With that, let's learn about the crypto in crypto.

The Basics of Cryptography

There are three main goals in cryptography. They are to provide confidentiality, ensure data integrity, and establish authenticity. These goals are accomplished using low-level algorithms called primitives. Calm down you apes. I'm not calling you primitive. Although, you all would probably see that as a compliment anyway.

Many of you may have familiarity with confidentiality. It is the most well-known of the three. It allows for information to be transferred between multiple parties such that only the intended parties have access to the true nature of it. The message at the beginning of this post is an example. Confidentiality is achieved through encryption. The two types of encryption are symmetric and asymmetric. (I used a particular type of symmetric encryption for the message at the being of the post called a one-time pad if anyone is interested.) Symmetric encryption uses the same key for encryption and decryption. In contrast, asymmetric encryption uses a different key for encryption, commonly referred to as the public key and, a different key for decryption, commonly referred to as the private key. As the names imply, public keys are meant to be shared and private keys are meant to be, well, not shared. Symmetric encryption typically uses a cipher alongside the key to encrypt/decrypt. On the other hand, asymmetric encryption is most commonly achieved through the keys in conjunction with complicated math problems such as prime number factorization. Keys are like passwords but much more random and longer. Keys need high entropy so that no one can guess them. Hunter2 isn't gonna cut it.

Data integrity makes sure the data being sent and received is the same and not tampered with. It is achieved using "one-way" functions known as hash functions. When we say "one-way" function, we are talking about a function that is easy to compute but hard to find an inverse. It is unclear if a true one-way function, i.e. a function where an inverse cannot be found, exists. If you happen to find one, you will become rich and famous. Amongus nerds at least. Besides being one-way, it should be practically

impossible to find a collision for a hash function to be considered good. A collision happens when two different inputs result in the same output, often referred to as the digest. If a good hash function is used and the digest of the data matches, you can remain confident in the integrity of the data. For example, there is a SHA3-256 hash of this post at the end. If you run this post through the same algorithm, you should get the same digest as below. I've linked a walkthrough of it at the end. Fun fact: If you ever wondered what exactly crypto mining is. It's basically computing a bunch of hashes until the digest looks a certain way.

Authenticity is achieved using digital signatures. Essentially, authenticity ensures that the person is who they claim to be. Authenticity is usually combined with data integrity and/or confidentiality. As such, digital signatures rely on keys, ciphers, and/or complicated math problems. The exact implementation depends on which scheme you are using. The most prevalent implementations use a public/private key system. As long as your private key remains confidential and your identity is associated with a public key, nobody can claim to be you. Although, you have to be a little careful for the very same reason. Once you sign something and share it, you can't take it back. The inability to refute a signature is known as non-repudiation. Some people consider it the fourth goal of cryptography, but I think it just ties in with authenticity. A good authentication scheme will have non-repudiation built-in. I have included my signature of this post and a link to a walkthrough at the end.

For anyone wondering just how secure these systems are. The security of these systems is measured in bits. If all the world's computing power was combined it would still take approximately a billion years to break a 128-bit secure system. A 256-bit system would take longer than the age of the universe. (I've linked a table for reference)

Key Management

If you take away anything from this post I think this section is the most important. Another important part of cryptography is key management. It doesn't matter how secure a system is if something is wrong with the key. You can let someone else worry about the cryptography part, but you must be responsible for your keys. That being said, I'm going to be honest with you. It would be great if everyone took their security into their own hands, became experts in cryptography/key management, and did everything themselves. However, that's just not going to happen. For the most part, as long as you are not doing something sensitive or high-value, you should be fine using an open-source, peer-reviewed system. But, be sure to know best practices. Anyways, with key management, we aim for secure use, exchange, and storage of keys.

When it comes to key usage, you have to keep in mind two things. The first is to make sure there are no onlookers when a key is being used and the second is to change keys after multiple uses. It is preferable to only use a key offline and alone. As for you changing your keys, there is no set time. You should probably rekey sooner if you use the keys often and you can get away without rekeying longer if you are careful or don't use your keys often.

Exchanging keys can be done offline or online. Offline key exchanges happen when a key is exchanged offline i.e the physical world. This could be done by all parties being present during the creation of the keys, mail, or some super spy shit. Thanks to asymmetric encryption though, offline key exchanges are becoming less common. Asymmetric encryption lets keys be shared online by encrypting the key using a person's public key, and allowing them to decrypt it using their private key.

The final part of key management is key storage. This part is relatively straightforward. ALWAYS store keys or keyword phrases offline or in some sort of cold storage. If you can't store them offline for some reason, keep them in an isolated environment on your machine. This may seem like common sense, but even the "world-class" Bittrex hackers, who were sitting on billions in Bitcoin, stored their keys in the cloud.

On the next episode of …

That covers the basics of cryptography, hope ya'll found it somewhat interesting. For the next post, I will be talking about smart contracts. I'm sure you've heard of 'em, but it's time you get to know 'em. Also, I know there is a concern of communication issues if something should ever happen to Reddit or the Gangnam Style video on YouTube. Not to mention the threat of censorship regardless of the platform. I think there is

a team working on some sort of decentralized Reddit. Still, for the time being, I wanted to share an uncensorable and decentralized way to communicate should the need arise. Nothing fancy but it works. Spoiler… It involves smart contracts.

Puzzle

Hmph. Seems I lack common sense. Maybe I should listen to my own advice.

Below is the hash and signature of the post above. This link will provide an overview of how that works.

https://github.com/satoshinotmemoto/Reddit/blob/main/The%20Science%20of%20Secrets/hash%26sign.pdf

hash: 964046743a22216f5b6bfcb761a68a3bb7fe16d37b78b6b4a8d2039a937d288f

signature: 0ab03516804cc4b454af2289c18c5bbbf94f186afa11db1427e6e2a7b556a87a5175048b920484be94dcc9408e464ea8167554b97e4192bb50c6f836baeceaaa1b