# The Beginner’s Guide to Cryptography

Cryptography, or the art and science of encrypting sensitive information, was once exclusive to the realms of government, academia, and the military. However, with recent technological advancements, cryptography has begun to permeate all facets of everyday life.

Everything from your smartphone to your banking relies heavily on cryptography to keep your information safe and your livelihood secure.

And unfortunately, due to the inherent complexities of cryptography, many people assume that this is a topic better left to black hat hackers, multi-billion dollar conglomerates, and the NSA.

But nothing could be further from the truth.

With the vast amounts of personal data circulating the Internet, it is more important now than ever before to learn how to successfully protect yourself from individuals with ill intentions.

In this article, I am going to present you with a simple beginner’s guide to cryptography.

My goal is to help you understand exactly what cryptography is, how it’s, how it’s used, and how you can apply it to improve your digital security and make yourself “hacker-proof.”

Let’s get started.

# 1. Cryptography Throughout History

Since the dawn of human civilization, information has been one of our most treasured assets.

Our species' ability (or inability) to keep secrets and hide information has eliminated political parties, shifted the tide of wars, and toppled entire governments.

Let's go back to the American Revolutionary War for a quick example of cryptography in practice (https://en.wikipedia.org/wiki/Intelligence_in_the_American_Revolutionary_War).

Suppose that a valuable piece of information regarding the British Army's plan to attack an American encampment was intercepted by local militia.

Since this is 1776 and therefore pre-iPhone, General Washington couldn't just shoot a quick text to the commanding officers at the encampment in question.

He would have to send a messenger who would either transport some form of written correspondence, or keep the message locked away in their head.

And here's where the Founding Fathers would have hit a snag.

The aforementioned messenger must now travel through miles and miles of enemy territory risking capture and death in order to relay the message.

And If he *was* intercepted? It spelled bad news for team USA.

The British captors could have simply killed the messenger on sight, putting an end to the communication.

They could have "persuaded" him to share the contents of the message, which would then render the information useless.

Or, if the messenger was a friend of Benedict Arnold's, they could have simply bribed the messenger to spread false information, resulting in the deaths of thousands of American militia.

However, with the careful application of cryptography, Washington could have applied an encryption method known as a cipher (more on this in a second) to keep the contents of the message safe from enemy hands.

*A Replica of Thomas Jefferson's cylinder Cipher in the National Cryptologic Museum*

Assuming that he entrusted the cipher to only his most loyal officers, this tactic would ensure that even if the message *was* intercepted, the messenger would have no knowledge of its contents. The data would therefore be indecipherable and useless to the enemy.

Now let's look at a more modern example, banking.

Every day, sensitive financial records are transmitted between banks, payment processors, and their customers. And whether you realize it or not, all of these records have to be stored at some point in a large database.

Without cryptography, this would be a problem, a very *big* problem.

If any of these records were stored or transmitted without encryption, it would be open season for hackers and your bank account would quickly dwindle down to $0.

However, the banks know this and have gone through an extensive process to apply advanced encryption methods to keep your information out of the hands of hackers and food on your table.

So now that you have a 30,000-foot view of cryptography and how it has been used, let's talk about some of the more technical details surrounding this topic.

# 2. Understanding Ciphers: The Basis of All Cryptography

**Note: For the purposes of this article, I will refer to messages in an easily readable format as "plaintext" and encrypted or unreadable messages as "ciphertext". Please note that the words "encryption" and "cryptography" will also be used interchangeably"**

Cryptography, at its most fundamental level, requires two steps: encryption and decryption.

The encryption process uses a cipher in order to encrypt plaintext and turn it into ciphertext.

Decryption, on the other hand, applies that same cipher to turn the ciphertext back into plaintext.

Here's an example of how this works.

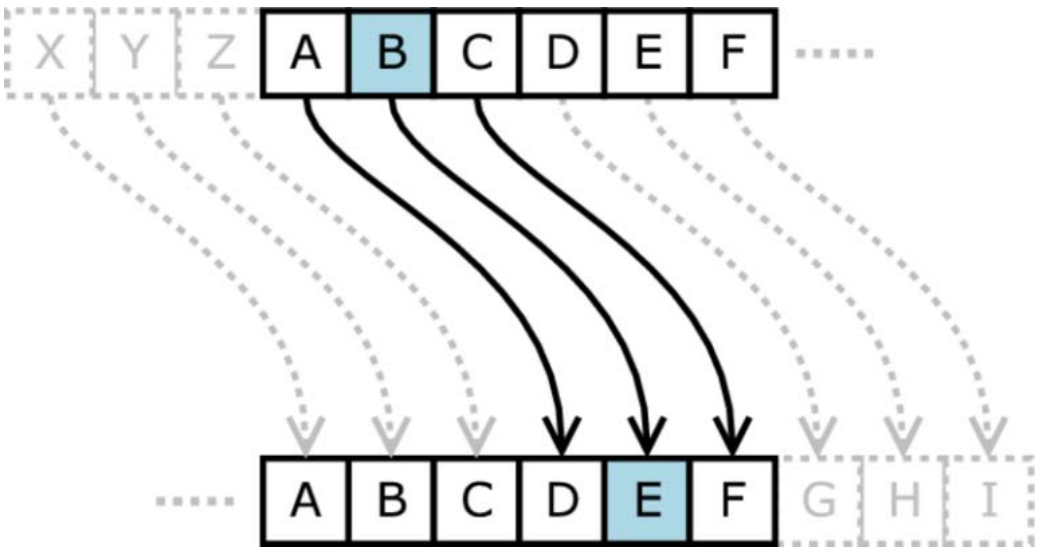
Let's say that you wanted to encrypt a the simple message, "Hello".

So our plaintext (message) is "Hello".

We can now apply one of the simplest forms of encryption known as "Caesar's Cipher (https://learncryptography.com/classical-encryption/caesar-cipher)" (also known as a shift cipher) to the message.

With this cipher, we simply shift each letter a set number of spaces up or down the alphabet.

So for example, the image below shows a shift of 3 letters.



Meaning that:

- A = D
- B = E
- C = F
- D = G
- E = H
- F = I
- And so on.

By applying this cipher, our plaintext “Hello” turns into the ciphertext “Khoor”

To the untrained eye “Khoor” looks nothing like “Hello”. However, with knowledge of Caesar’s cipher, even the most novice cryptographer could quickly decrypt the message and uncover its contents.

**A Brief Word on Polymorphism**

Before we continue, I want to touch on a more advanced topic known as polymorphism (https://www.wilderssecurity.com/threads/polymorphic-cipher.321583/).

While the intricacies of this topic stretch far beyond the realm of this guide, its increasing prevalence mandates that I include a brief explanation.

Polymorphism is basically a cipher that changes itself with each use. Meaning that each time it is used, it produces a different set of results. So, if you encrypted the *exact same set of data* twice, each new encryption would be different from the previous one.

Let’s go back to our original example with the plaintext “Hello.” While the first encryption would result in “Khoor”, with the application of a polymorphic cipher, the second encryption could result in something like “Gdkkn” (where each letter is shifted down a rung of the alphabet)

Polymorphism is most commonly used in cipher algorithms to encrypt computers, software, and cloud-based information.

# 3. Why Does Cryptography Matter?

I want to preface the rest of this article with a warning.

Throughout the rest of this article, I will be explaining exactly how cryptography works and how it is applied today. In doing so, I will have to employ a significant amount of technical jargon that may feel tedious at times.

But bear with me and pay attention. Understanding how all of the pieces fit together will ensure that you are able to maximize your personal security and keep your information out of the wrong hands.

So before I go full blast, explaining symmetric and asymmetric cryptography, AES, and MD5, I want to explain, in Layman's terms, why this matters and why *you* should care.

For starters, let's discuss the only real alternative to cryptography, obfuscation. Obfuscation is defined as "*The act of making something unclear, obscure, or unintelligible".* It means that, in order to transmit a secure message, you must hold back some of the information required to understand the message.

Which, by default, means it would only take one person with knowledge of the original message to divulge the missing pieces to the public.

With cryptography, a specific key and numerous calculations are required. Even if someone knew the encryption method used, they wouldn't be able to decrypt the message without the corresponding key, making your information much more secure.

To understand why cryptography *really* matters you need look no further than something we all know and love, the Internet.

By design, the Internet was created to relay messages from one person to another, in a similar manner to the postal service. The Internet delivers "packets" from the sender to the recipient, and without the various forms of cryptography that we will discuss in a moment, *anything* that you sent would be visible to the general populace.

Those private messages you meant to send to your spouse? The whole world could see them. Your banking information?

Anybody with a router could intercept your funds and redirect them to their own account. Your work emails discussing sensitive company secrets? You might as well package those up and ship them to your competitors.

Luckily, we *do* have cryptographic algorithms that actively protect almost all of our personal data.

However, this does not mean that you are completely secure.

You need to look no further than recent attacks on companies like AdultFriendFinder and Anthem Inc. to realize that large corporations do not always implement the necessary systems required to protect your information.

Your personal security is *your* responsibility, no one else's.

And the sooner that you can develop a strong understanding of the systems in place, the sooner you will be able to make informed decisions about how you can protect your data.

So with that out of the way, let's get to the good stuff.

# 4. Types of Cryptography

There are four primary types of cryptography in use today, each with its own unique advantages and disadvantages.

They are called hashing, symmetric cryptography, asymmetric cryptography, and key exchange algorithms.

1. **Hashing**

Hashing is a type of cryptography that changes a message into an unreadable string of text for the purpose of verifying the message's contents, *not* hiding the message itself.

This type of cryptography is most commonly used to protect the transmission of software and large files where the publisher of the files or software offers them for download. The reason for this is that, while it is easy to calculate the hash, it is extremely difficult to find an initial input that will provide an exact match for the desired value.

For example, when you download Windows 10, you download the software which then runs the downloaded file through the same hashing algorithm. It then compares the resulting hash with the one provided by the publisher. If they both match, then the download is completed.

However, if there is even the slightest variation in the downloaded file (either through the corruption of the file or intentional intervention from a third party) it will drastically change the resulting hash, potentially nullifying the download.

Currently, the most common hashing algorithms are MD5 and SHA-1 (https://crypto.stackexchange.com/questions/18612/how-is-sha1-different-from-md5), however due to these algorithm's multiple weaknesses, most new applications are transitioning to the SHA-256 (http://www.xorbin.com/tools/sha256-hash-calculator) algorithm instead of its weaker predecessors.

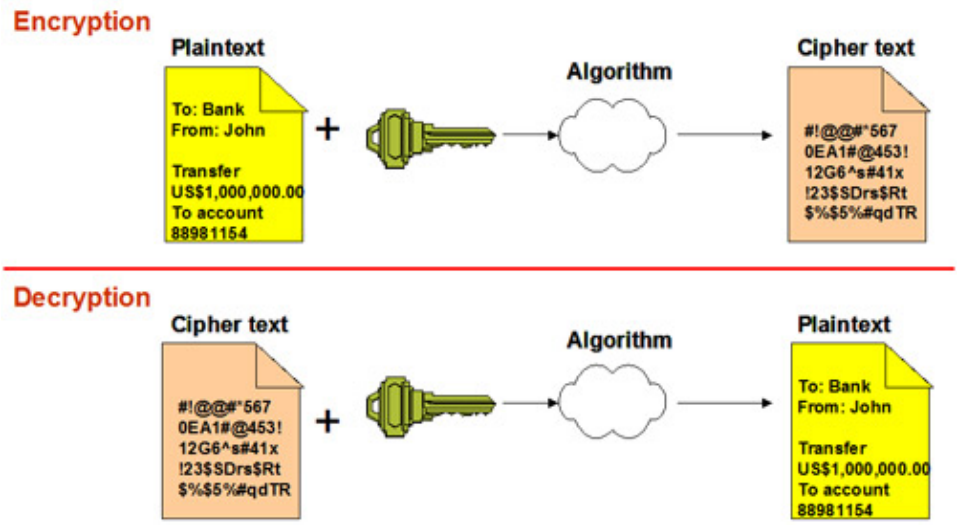
2. **Symmetric Cryptography**

Symmetric Cryptography, likely the most traditional form of cryptography, is also the system with which you are probably most familiar.

This type of cryptography uses a single key to encrypt a message and then decrypt that message upon delivery.

Since symmetric cryptography requires that you have a secure channel for delivering the crypto key to the recipient, this type of cryptography is all but useless for transmitting data (after all, if you have a secure way to deliver the key, why not deliver the message in the same manner?).

As such, its primary application is the protection of resting data (e.g. Hard Drives and data bases)

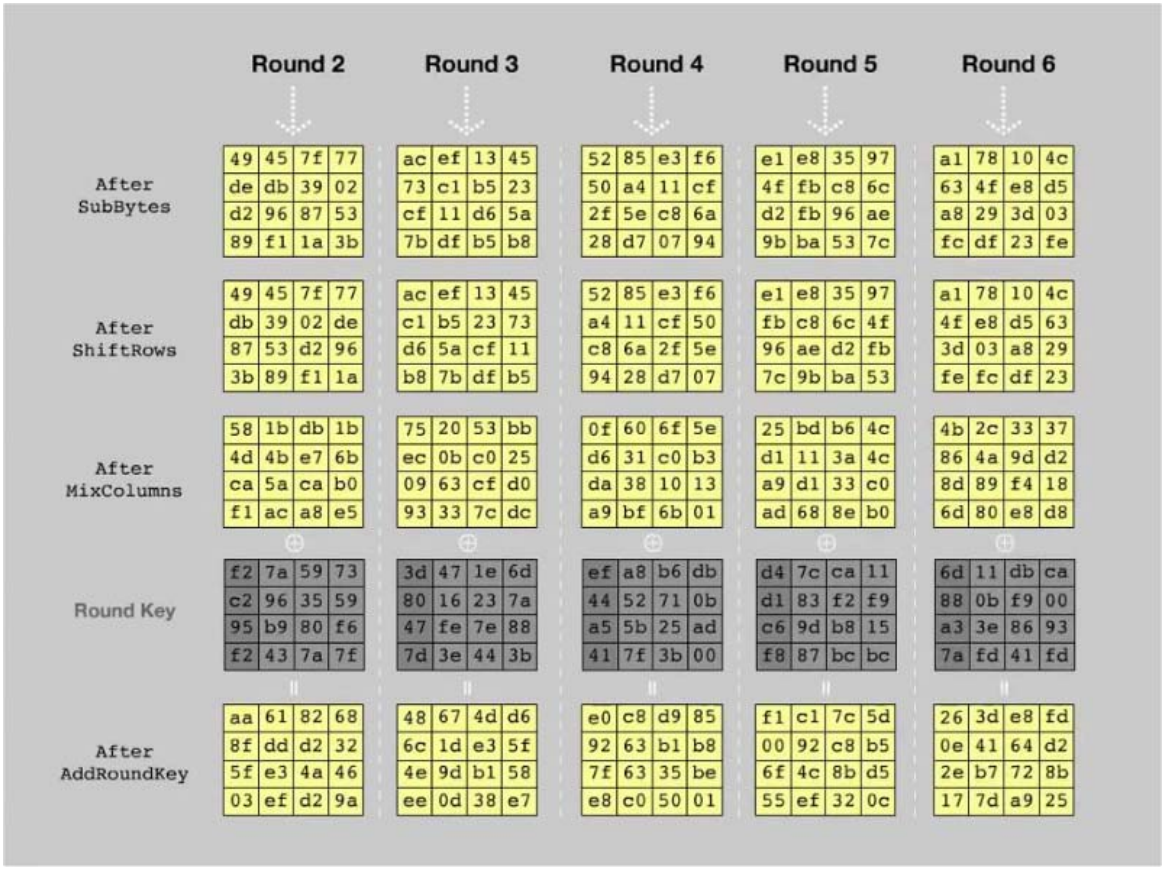



In the Revolutionary War example that I mentioned earlier, Washington's method for transmitting information between his officers would have relied on a symmetric cryptography system. He and all of his officers would have had to meet in a secure location, share the agreed upon key, and then encrypt and decrypt correspondence using that same key.

Most modern symmetric cryptography relies on a system known as AES or Advanced Encryption Standards.

While the traditional DES models were the industry norm for many years, DES was publicly attacked (https://www.sans.org/reading-room/whitepapers/vpns/day-des-died-722) and broken in 1999 causing the National Institute of Standards and Technology to host a selection process for a stronger and more updated model.

After an arduous 5-year competition between 15 different ciphers, including MARS from IBM, RC6 from RSA Security, Serpent, Twofish, and Rijndael, the NIST selected Rijndael as the winning cipher (http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf).




It was then standardized across the country, earning the name AES or Advanced Encryption Standards. This cipher is still widely used today and is even implemented by the NSA for the purposes of guarding top secret information.

3. **Asymmetric Cryptography**

Asymmetric cryptography (as the name suggests) uses two different keys for encryption and decryption, as opposed to the single key used in symmetric cryptography.

The first key is a public key used to encrypt a message, and the second is a private key which is used to decrypt them. The great part about this system is that only the private key can be used to decrypt encrypted messages sent from a public key.

While this type of cryptography is a bit more complicated, you are likely familiar with a number of its practical applications.

It is used when transmitting email files, remotely connecting to servers, and even digitally signing PDF files. Oh, and if you look in your browser and you notice a URL beginning with “https://”, that’s a prime example of asymmetric cryptography keeping your information safe.

4. **Key Exchange Algorithms**

Although this particular type of cryptography isn’t particularly applicable for individuals outside of the cyber-security realm, I wanted to briefly mention to ensure you have a full understanding of the different cryptographic algorithms.

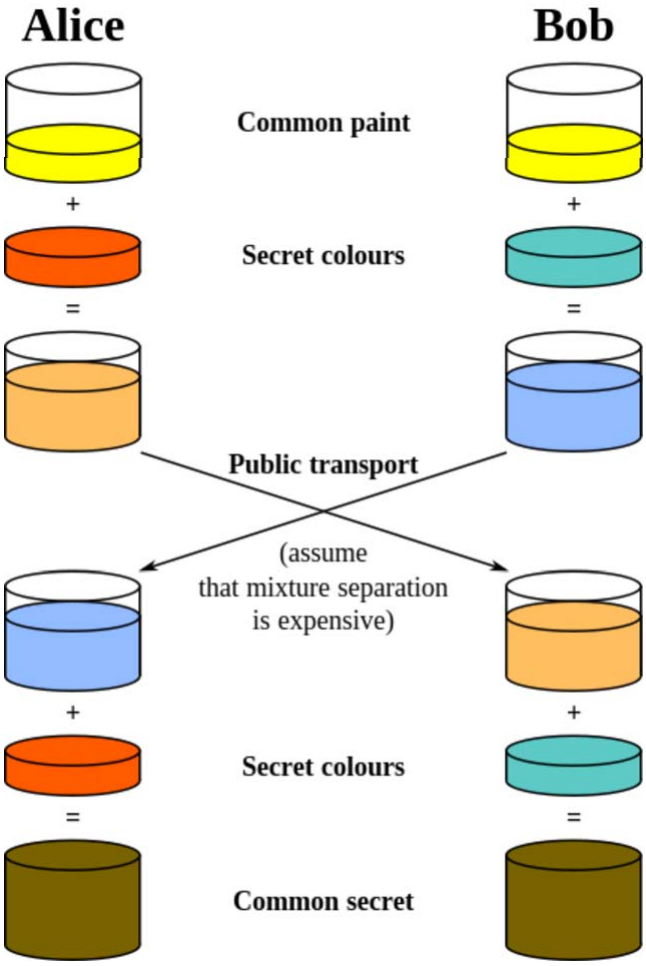
A key exchange algorithm, like Diffie-Hellman, is used to safely exchange encryption keys with an unknown party.

Unlike other forms of encryption, you are not sharing information during the key exchange. The end goal is to create an encryption key with another party that can later be used with the aforementioned forms of cryptography.

Here’s an example from the Diffie-Hellman wiki (https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange) to explain exactly how this works.

Let’s say we have two people, Alice and Bob, who agree upon a random starting color. The color is public information and doesn’t need to be kept secret (but it does need to be different each time). Then Alice and Bob each selects a secret color that they do not share with anyone.

Now, Alice and Bob mix the secret color with the starting color, resulting in their new mixtures. They then publicly exchange their mixed colors. Once the exchange is made, they now add their own private color into the mixture they received from their partner, and the resulting in an identical shared mixture.




# 5. The 4 Types of Cryptographic Functions

So now that you understand a little bit more about the different types of cryptography, many of you are probably wondering how it is applied in the modern world.

There are four primary ways that cryptography is implemented in information security. These four applications are called “cryptographic functions”.

1. **Authentication**

When we use the right cryptographic system, we can establish the identity of a remote user or system quite easily. The go-to example of this is the SSL certificate (https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/) of a web server which provides proof to the user that they are connected to the right server.

The identity in question is *not* the user, but rather the cryptographic key of that user. Meaning that

the more secure the key, the more certain the identity of the user and vice versa.

Here's an example.

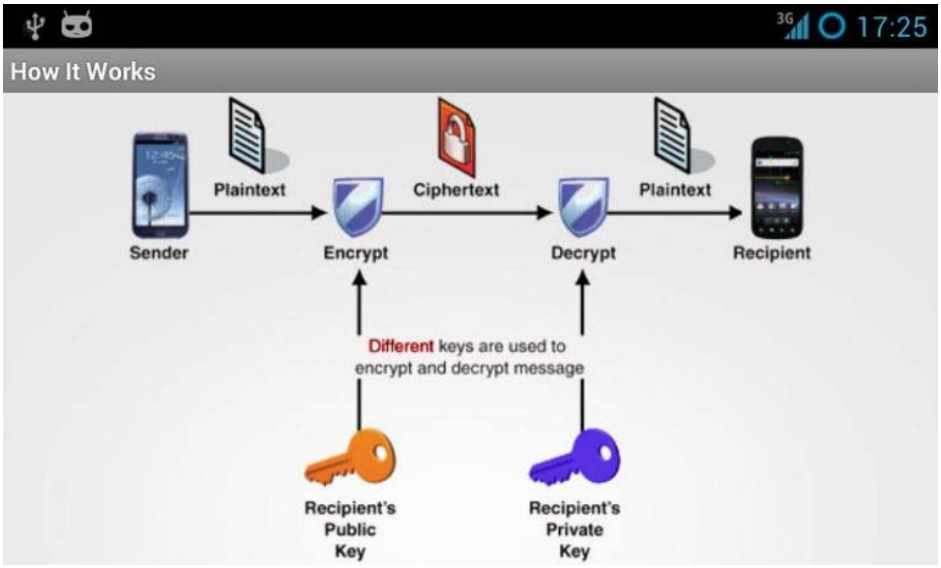
Let's say that I send you a message that I have encrypted with my private key and you then decrypt that message using my public key. Assuming that the keys are secure, it is safe to assume that I am the actual sender of the message in question.

If the message contains highly sensitive data, then I can ensure a heightened level of security by encrypting the message with my private key and *then* with your public key, meaning that you are the only person who can actually read the message and you will be certain the message came from me.

The only stipulation here is that the public keys are both associated with their users in a trusted manner, e.g. a trusted directory.

In order to address this weakness, the community created an object called a certificate which contains the issuer's name as well as the name of the subject for whom the certificate is issued. This means that the fastest way to determine if a public key is secure is to note if the certificate issuer also has a certificate too.

An example of this type of cryptography in action is Pretty Good Privacy, (https://en.wikipedia.org/wiki/Pretty_Good_Privacy) or PGP, a software package developed by Phil Zimmerman that provides encryption and authentication for email and file storage applications.




This software package provides users with message encryption, digital signatures, data compression, and email compatibility.

Although Zimmerman ran into some legal problems with the initial software which used an RSA for

key transport, MIT PGP versions 2.6 and later are legal freeware for personal use, and Viacrypt 2.7 and later versions are legal commercial alternatives.

2. **Nonrepudiation**

This concept is especially important for anyone using or developing financial or e-commerce applications.

One of the big problems that e-commerce pioneers faced was the pervasive nature of users who would refute transactions once they had already occurred. Cryptographic tools were created to ensure that each unique user had indeed made a transaction request that would be irrefutable at a later time.

For example, let's say that a customer at your local bank requests a money transfer to be paid to another account. Later in the week, they claim to have never made the request and demand the full amount be refunded to their account.

However, as long as that bank has taken measures to ensure non-repudiation through cryptography, they can prove that the transaction in question was, in fact, authorized by the user.

3. **Confidentiality**

With information leaks and a seemingly endless number of privacy scandals making the headlines, keeping your private information,, well, private is probably one of your biggest concerns. This is the exact function for which cryptographic systems were originally developed.

With the right encryption tools, users can guard sensitive company data, personal medical records, or just lock their computer with a simple password.

4. **Integrity**

Another important use of cryptography is to ensure that data is not viewed or altered during transmission or storage.

For example, using a cryptographic system to ensure data integrity ensures that rivaling companies cannot tamper with their competitor's internal correspondence and sensitive data.

The most common way to do accomplish data integrity through cryptography is by using cryptographic hashes to safeguard information with a secure checksum.

# 6. Cryptography for the Everyday Joe and Jane

So, now that we have gone through the basics of what cryptography is, how it's used, it's different applications, and why it matters, let's have a look at how you can apply cryptography in your everyday life.

And I want to start this section by pointing out that you *already* rely on cryptography each and every day to keep yourself secure!

Have you used a credit card recently? Played a Blu-ray movie? Connected to wifi? Visited a website?

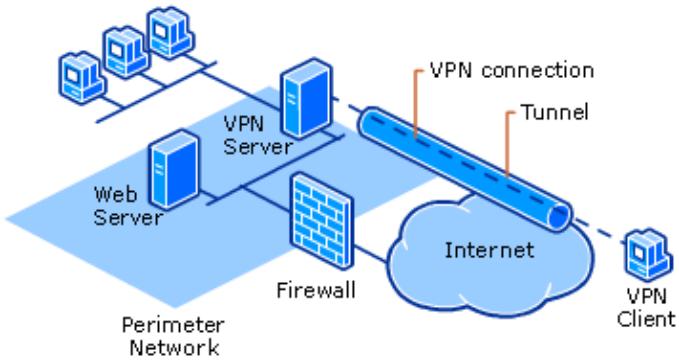
All of these actions rely on cryptography to ensure that your information and assets are secure.

But for those of you who want an extra layer of protection, here are a couple of ways that you can implement even more encryption into your life.

1. **Download a VPN to Protect Your**

A VPN or Virtual Private Network (https://thebestvpn.com/what-is-vpn-and-how-it-works/) allows you to create a secure connection to another network over the public Internet.

These are highly versatile tools that allow you to access restricted websites, hide your browsing activity from the eyes on public wifi, and remotely access your private servers.




Here are a few examples of how they are used.

Let's say that you are a C-level executive at a large company. You are away on business meetings and want to login to your private corporate network remotely.

This is actually an incredibly easy task. All you need to do is to first connect to the public Internet through an ISP and then launch a VPN connection using the company's VPN server and specific software and Voila! You now have access to your private network.

Or, perhaps you are location independent employee who primarily works out of local coffee shops. Public connections like the networks at your friendly neighborhood Starbucks are notoriously insecure meaning that any hacker worth his salt could easily spy on your activity and steal sensitive data related to your current projects.

However, with a VPN, you can connect to a highly secure network that will shield you from the prying eyes of less than ethical coffee shop hackers.

VPNs can even be used in foreign countries to access region-restricted websites (https://www.howtogeek.com/210614/how-to-access-region-restricted-websites-from-anywhere-on-earth/). For example, if you are travelling in Asia, you are likely aware that the Chinese government has a number of Draconian censorship laws that block public access to applications like Facebook and Instagram.

However, as long as you have a VPN pre-installed on your device, you can quickly connect to a secure network in your hometown and have instant access to all of the websites and platforms you normally use.

While VPNs are a great tool for anyone looking to increase their network security, it's important that you are selective with *which* VPN provider you use.

If you want to compare the cost, security, and speeds of different services, you can check out the rest of our site for a comprehensive review and comparison of the most popular VPNs on the market.

2. **Download HTTPS Everywhere**

HTTPS pages typically use either SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to increase the security of your browsing experience with an asymmetric Public Key Infrastructure.

This type of connection scrambles messages being sent between your computer and the website you are viewing to ensure that you are less susceptible to hackers.

This is *extremely* important whenever you are transmitting sensitive personal information or financial details.

"HTTPS Everywhere (https://www.eff.org/https-everywhere)" is a free open source browser extension compatible with Chrome, Firefox, and Opera. With this extension, any website you visit will be forced to use an HTTPS connection instead of the less secure HTTP connection so long as it's supported.

3. **Install BitLocker (for Windows) or FileVault2 (for Mac)**

If you want to take extra steps (beyond just login password) to ensure that your personal information

is secured on your PC or laptop, then I highly recommend you install BitLocker (https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-overview) or FileVault2 (https://support.apple.com/en-us/HT204837).

These disk encryption devices protect your data by using the AES cryptography algorithm to provide encryption for entire volumes. If you do opt for this software, be sure to write down your credentials and keep them in a secure location. If you lose these credentials, it is almost certain that you will forever lose access to all of your encrypted information.

# 7. Cryptography Isn't Perfect

At this point, I hope that you have developed a concrete understanding of cryptography and its applications for everyday life.

But before I wrap up, I want to leave you with a word of warning.

While cryptography can certainly provide you with *more* security, it cannot provide you with *total* security.

With the plethora of attacks that have happened in recent years including the Tesco Bank (http://www.thisismoney.co.uk/money/saving/article-3930118/Tesco-Bank-hack-happened-protect-account.html), Department of Justice hack (http://www.computerworld.com/article/3030983/security/hackers-breach-doj-dump-details-of-9-000-dhs-employees-plan-to-leak-20-000-from-fbi.html), and AdultFriendFinder (https://www.theverge.com/2016/11/13/13615750/412-million-adultfriendfinder-accounts-exposed-breach) attacks (just to name a few) it's pretty clear that cryptography has its shortcomings.

And while the vast majority of you can sleep soundly knowing that large corporations are working their hardest to ensure the safe and secure transmission and storage of your data, it's important to realize that you are not impervious to a similar attack.

This is not said to dissuade you from using the aforementioned methods of encryption, simply to inform you that even the best cryptographic algorithms were designed by imperfect teams of people and are subject to breach.

So as you go through your daily life, be mindful of this reality and realize that "More Secure" doesn't mean "Totally secure".

## Conclusion

By developing a greater understanding of the common encryption methods and cryptography algorithms in circulation today, you will be better equipped to protect yourself from potential cyber attacks and breaches in data security.

Although cryptography isn't perfect, it *is* necessary to ensure the continued security of your personal information. And with the rapidly evolving landscape of modern data, this topic is more important now than ever before.