Cryptography For Ethical Hackers

Learn about cryptography, one of the most important tools in modern cybersecurity, and how it's related to Ethical Hacking.

What Is Cryptography

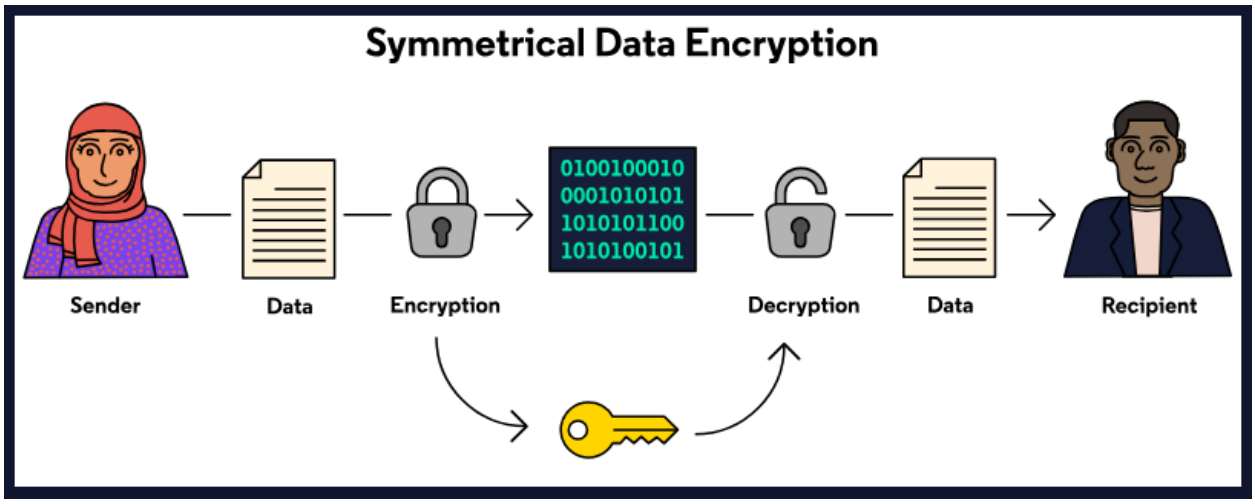
Since before even the Roman Empire, humans needed to preserve the confidentiality of information, and one way we do that is by using cryptography. Broadly speaking, **cryptography** is the process of encrypting and decrypting data using algorithms known as ciphers. Ciphers vary broadly in their complexity, ranging from simple substitution ciphers that can be solved for fun by children to complex mathematical functions designed to resist the most powerful supercomputers we have.

The ciphers we use in modern cybersecurity are much closer to the latter than the former, but it's often much easier to explain concepts using simple algorithms.

Key Concepts

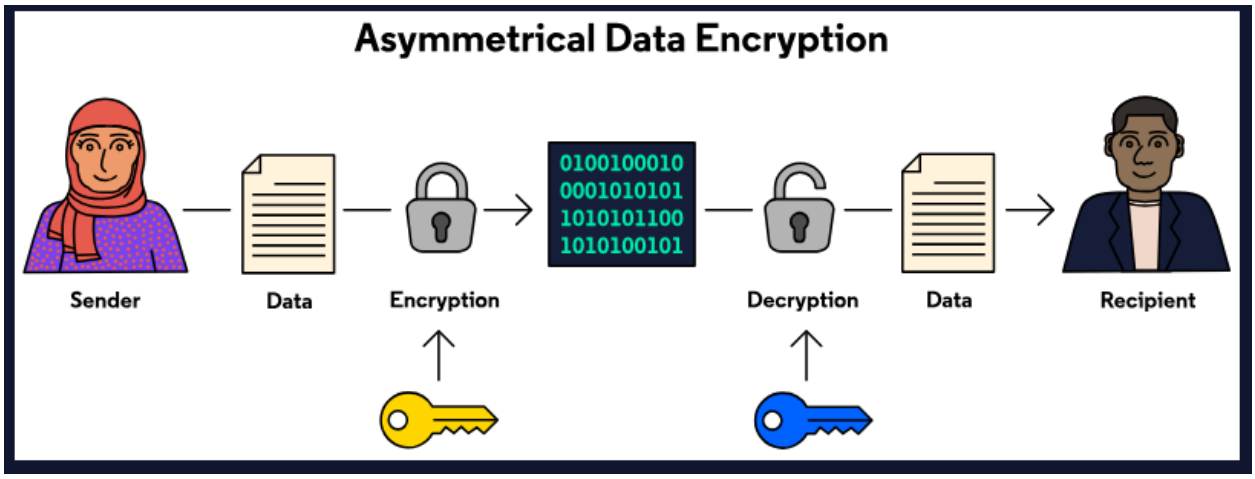
Symmetric Vs. Asymmetric Encryption

Symmetric encryption uses the same key to encrypt and decrypt data. Symmetric encryption is faster than asymmetric encryption, but if someone is able to obtain the key from symmetric encryption, they can read and secretly modify any data they intercept.



Asymmetric encryption uses separate keys to encrypt and decrypt data. Asymmetric encryption is slower than symmetric encryption, but it's harder for an attacker to read or modify intercepted communications. Asymmetric

encryption can also be used to verify identity as well as verify the authenticity of documents.



Hashing

When we encrypt something, we usually want to be able to decrypt it later. **Hashing** throws that concept out the window. Unlike encryption algorithms, hashing algorithms *aren't designed to be reversible*. This is useful for situations where we want to be able to check if one piece of information matches another without actually knowing what either piece of information is. An example of such a situation is password storage.

Hashing algorithms usually also have two other properties:

1. Their output is a *fixed* size, while their input can be *any* size.
2. Changing the input a *little* will change the output *a lot*.

Hashing algorithms are deterministic, which means that the same input results in the same output *every time*. In a well-designed hashing algorithm, the only way to figure out what input created a given output is by repeatedly making guesses and running those guesses through the correct hashing algorithm until you get the same output.

If a hashing algorithm has more potential inputs than potential outputs, it is mathematically inevitable that there will be some inputs that produce the same output. This is known as a **hash collision**, and most modern hashing algorithms, such as SHA256, deal with this by having a very large number of possible outputs, so collisions are rare. SHA256 has more possible outputs than the estimated number of atoms in the Milky Way.

Ephemeral Keys

Ephemeral keys are keys that are generated, used once (or for a short time), and then discarded. This means that even if an attacker is able to obtain the key, it won't be useful to them for long! For example, TLS 1.3 uses symmetric, ephemeral keys created simultaneously on both the client and server, without the key itself ever being transmitted over the internet. As is the case with most modern cryptography, the exact details of how this works are very complicated and involve a lot of math.

Cryptography In The World Of An Ethical Hacker

As advanced cryptography can be, it is important to know that it can be broken and have vulnerabilities. That said, it is helpful for ethical hackers to be able to exploit cryptographic algorithms in use. By exploiting the algorithm in use, an ethical hacker can analyze the algorithm to identify if any vulnerabilities exist.

Here are some non-exhaustive ways that an ethical hacker can exploit cryptographic vulnerabilities:

- Key Management

Secured communication between two parties often occurs using secret keys. These secret keys are only known between the two authorized parties. However, your cryptographic system is only as good as your key management system. In other words, if your key management systems contain weak and reusable passwords, your cryptographic system is weak. An ethical hacker can obtain the encryption key for your cryptography system and bypass your cryptographic protections.

- Insecure Encryption Algorithms

Insecure encryption sounds a bit weird, but it exists. An encryption algorithm can be insecure if it is weak, outdated, broken, or isn't used correctly. Those insecurities mentioned allows for vulnerabilities within a system waiting to be exploited. As an ethical hacker, one of your jobs is to identify and exploit those vulnerabilities before a malicious actor does. That said, an ethical hacker might research encryption algorithm vulnerabilities to identify its weaknesses.

- DIY Algorithms/Protocols

As difficult as cryptographic encryption is, many individuals attempt to create their own to make it better than the standard. This is dangerous and opens a whole world of possible vulnerability issues. An ethical hacker can reverse engineer the encryption algorithm to identify its vulnerabilities and exploit them. If an ethical hacker can do this, so can a malicious hacker. If a malicious hacker successfully reverse-engineers the system's custom encryption, the malicious hacker will now have access to your system.

This list of ways that hackers can exploit cryptographic vulnerabilities is not exhaustive. There are several more ways to exploit cryptographic vulnerabilities, and they will continue to be so as technology develops.

Conclusion

Cryptography is a useful tool for preserving confidentiality and integrity, as well as providing means of authentication and non-repudiation. However, cryptography, through the mean encryption algorithms, is not free from vulnerabilities. It is up to the ethical hacker to identify, exploit, and resolve those vulnerabilities before a malicious hacker identifies and exploits them.