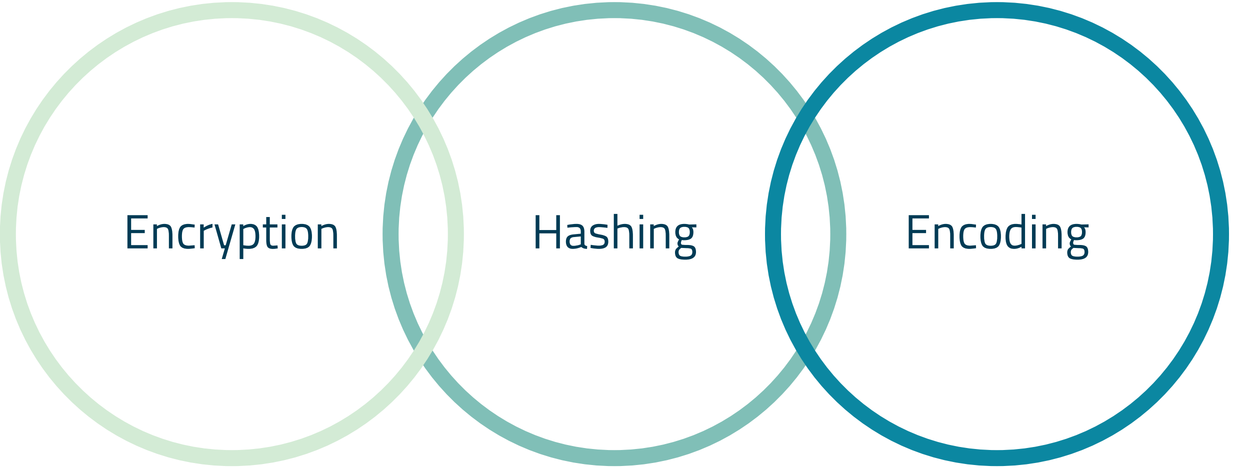
Hashing vs. Encryption vs. Encoding



Encryption

Hashing

Encoding

Understand the difference between Hashing, Encryption, and Encoding

If you think that Hashing, Encryption, and Encoding are the same thing, you are wrong! However, you're not alone.

There is an awful lot of confusion surrounding these three terms. As similar, as they may sound, they are all totally different things.

Before getting down to business though, let's understand a few things first.

Internet Security

From a security point of view what are the most important things when sending data/message on the internet?

1.

You want to let the other person know that the message has been sent from you – not from anyone else.

2.

You want the message to be in the exact same format – without any alteration or modification.

3.

You want your message to be protected from the reach of ill-intended people – hackers, fraudsters & other types of cyber criminals.

These three functions can be designated as:

Identity Verification

Integrity

Confidentiality

“ *So, how exactly is this done? Hashing and Encryption are the answers. Now you must be thinking ‘Doesn’t that make them the same thing?’ The answer is NO.*

Hashing

Hashing –

- Let’s try to imagine life without hashing. Suppose, it’s someone’s birthday and you decide to send a ‘Happy Birthday’ message.

- Your geeky (and funny!) friend decides to have a bit of fun at your expense so he intercepts it and turns your ‘Happy Birthday’ message into a ‘Rest in Peace’ message (imagine the consequences!).

- This could happen and you wouldn’t even know it (until you are at the receiving end of certain reactions!).

- Jokes aside, Hashing protects the integrity of your data. It protects your data against potential alteration so that your data isn't changed one bit.

- Basically, a hash is a number that is generated from the text through a hash algorithm. This number is smaller than the original text.

- The algorithm is designed in such a way that no two hashes are the same for two different texts. And it is impossible (almost!) to go back from the hash value to the original text.

- It’s kind of like a cow moving on stairs – it can move upstairs but not down!! Anyway, looping back to our “happy birthday” message. Had you hashed your message, the intended recipient of your message would unhash the message and see a different value than what should come back.

- At that point, they’ll know the message has been tampered with.

- That’s one of the most indispensable properties of Hashing—its uniqueness. There cannot be the same hash value for different text.

- Even the tiniest bit of change/modification will alter the hash value completely. This is called the Avalanche Effect.

- Let’s understand this with an example. In the below example, we have applied the SHA-1 algorithm. Let’s see how it goes.

Text: Everybody loves donuts

SHA-1 Hash value of the text above: daebbfdea9a516477d489f32c982a1ba1855bcd

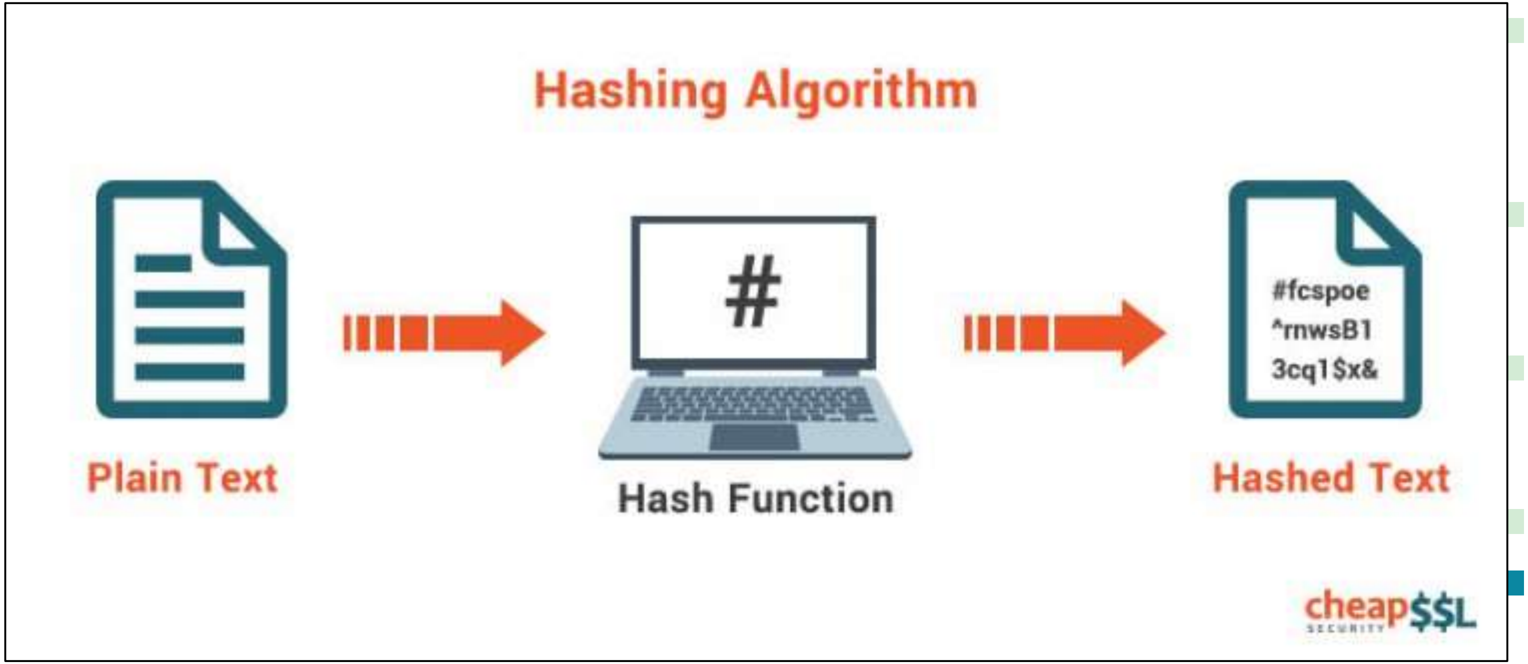
Let’s not get involved in the donut debate (is there a debate?) and focus on hashing for the time being. Now if we make a tiny bit of change in the sentence above, the hash value will change entirely. Let’s see how it goes.

New text: Everybody loves donut.

SHA-1 Hash value of the new text: 8f2bd584a1854d37f9e98f9ec4da6d757940f388

See how the hash value changed entirely when we removed the ‘s’ from Donuts? That’s what hashing does for you.

Hashing Algorithm Example



Use of Hashing

- Hashing is an effective method to compare and avoid duplication in databases.
- Hashing is used in Digital signatures and SSL certificates.
- Hashing can be used to find a specific piece of data in big databases.
- Hashing is widely used in computer graphics.

Encryption

Encryption

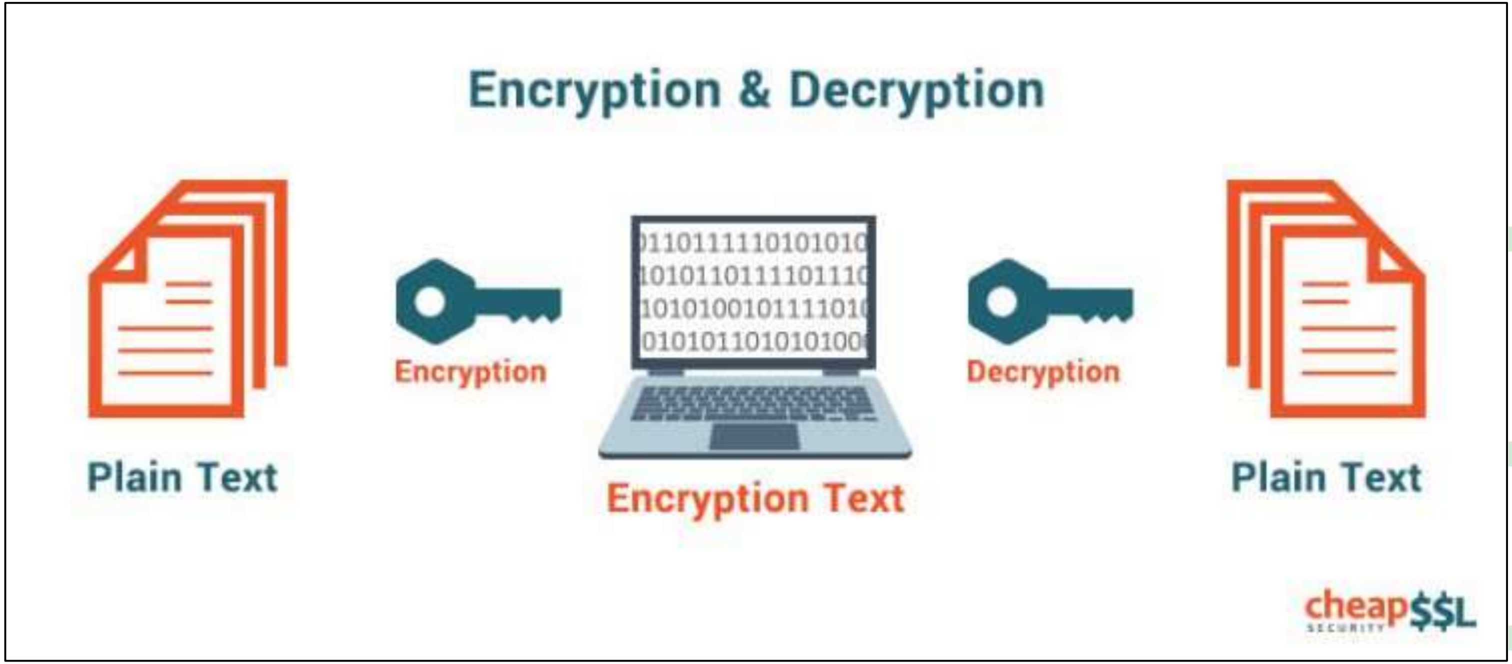
- It’s almost impossible to imagine the internet without Encryption.

- Encryption is what keeps the artificial world of the internet secured. Encryption keeps data secured and confidential.

- Fundamentally, it is the process of transforming your confidential data into an unreadable format so that no hacker or attacker can manipulate or steal it.

- Thereby, serving the purpose of confidentiality.

Encryption & Decryption



- The encryption of data is executed through cryptographic keys. The information is encrypted before it’s sent and decrypted by the receiver. Therefore, the data is safe when it is “in the air.”

- Based on the nature of the keys, encryption can be classified into two main categories – symmetric encryption, asymmetric encryption.

Encryption Types

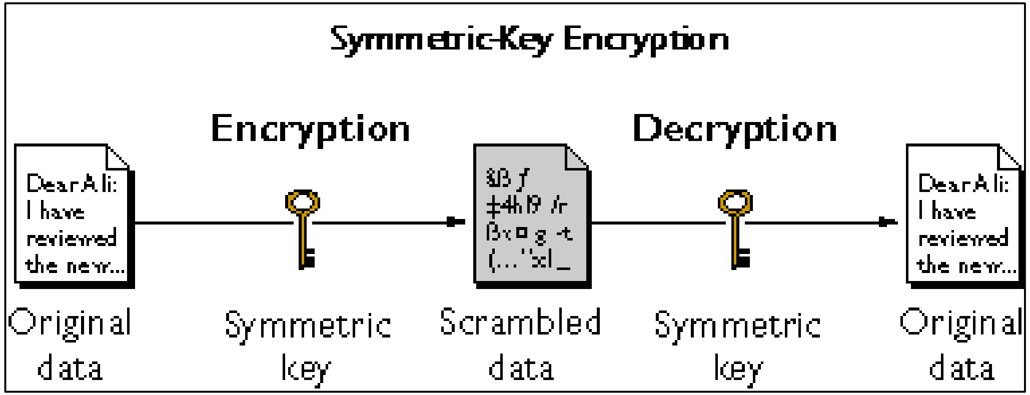
Symmetric Encryption

In symmetric encryption, the data is encrypted and decrypted using a single cryptographic key. It means that the key used for encryption is used for decryption as well.

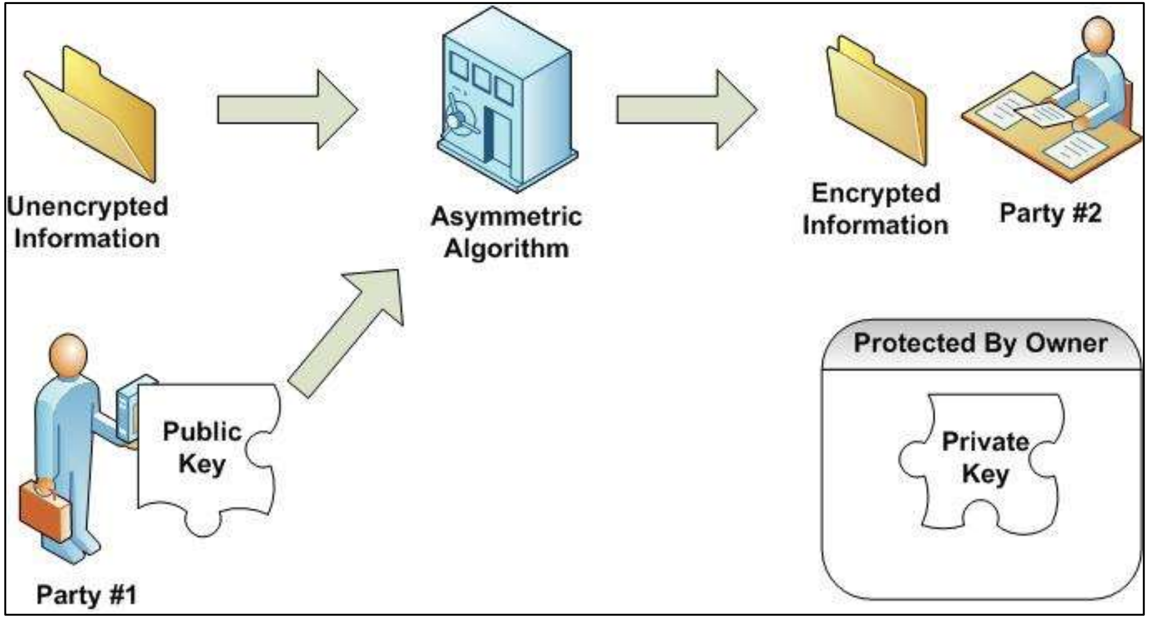
Asymmetric Encryption

Asymmetric encryption is a relatively new technique compared to its counterpart. It involves the use of two different keys, one for encryption and one for decryption purposes. One key is known as a ‘Public Key’ and the other is regarded as a ‘Private Key.’

Symmetric Encryption



Asymmetric Encryption



- The Public Key is virtually everywhere. Even you possess it without even knowing it. One is stored in your web browser every time you visit an HTTPS-enabled website.

- When you send any data to an encrypted site, it is encrypted using the Public Key. The Private Key, on the other hand, is only with the receiver and must be kept discreet. Private Key is used to decrypt the encrypted data. The use of two distinct keys makes the encryption process more secure and a tad slower.

- Both these techniques are used in the SSL/TLS certificates. The Asymmetric Encryption is first applied for the SSL handshake process — server validation if you call it. Once the connection is in place between the server and the client, Symmetric Encryption takes care of the data encryption.

Encoding

Encoding

- Unlike Encryption and Hashing, Encoding is not used for security purpose.

- Fundamentally, it is just a technique to transform data into other formats so that it can be consumed by numerous systems.

- There is no use of keys in encoding. The algorithm that is used to encode the data is used to decode it as well.

- ASCII and UNICODE are examples of such algorithms.

Let's flashback a bit

Hashing
A string of numbers generated to confirm the integrity of data through hashing algorithms.

Encryption
A technique used to maintain the confidentiality of data by converting the data into an undecipherable format.

Encoding
A conversion of data from one format to another format.

Thanks

- If you have any questions about this document please don’t hesitate to contact us at:

- https://cheapsslsecurity.com/blog/
- https://twitter.com/sslsecurity
- https://www.facebook.com/CheapSSLSecurities
- https://plus.google.com/+Cheapsslsecurity