Protecting customer data is the priority of every organization. A security breach can result in loss of reputation, customer dissatisfaction, and financial losses for the company. For the handling of sensitive data, it is important to use data security methods like hashing and encryption.

You can think of hashing and encryption as two sides of the same coin. Both functions are used for data encoding and prevent malicious activity. Encryption for these two functions is done with the help of algorithms that provide privacy. With so many similarities it is not surprising that the two terms are confused with each other quite often.

Security is an extremely important parameter when we talk about communication systems. If you are in charge of data and communication systems then you must be aware of the computing terms hashing and encryption. These two terms are often confused with each other. Whereas, in reality, they are different in both theory and practice. Our article today highlights the difference between the two. But before we understand the differences between each of them let's understand the individual terms in detail.

## **What is Hashing?**

A hash refers to a random number generated from a specific string. Hashing is a method used to perform one-sided encryption. A one-sided or one-way encryption means that you will not be able to decode the information via a predefined key. A hash that is once produced for a certain string cannot be produced for another which means that a hash is unique. Below are a few attributes of hashing:

1. An input hash will produce a unique output hash only.
2. When an input string has been hashed it is not possible to reverse the output back to the input.
3. Several inputs will result in a different output.
4. If you are modifying any element of the input it would change the structure of the hash.

Hashing is essentially used to compare data that is in large value. It is relatively easier to compare hash values instead of the data itself. Moreover, it is easy to fund data record once it has been hashed. Hashing also prevents the duplication of data and makes [online transactions](http://www.cardzgroup.com) safer.

## **What is Encryption?**

The process of encrypting information is known as encryption. Data that has been encrypted can only be decrypted by using a decryption key. This key is only accessible to those who are in charge of the security system at the receiver end. This way the system remains protected and seamless communication can take place between parties. Encryption is known to be one of the most effective ways of securing data. There are several types of data encryption that serve different purposes.

1. Symmetric encryption: the same key is used to encrypt and decrypt data.
2. Asymmetric encryption: there are two keys involved in this type of encryption; a public key that is known to everyone and a private key that is only known to the receiver.
3. Hybrid encryption: as the name suggests hybrid encryption uses both types of encryption to make a powerful blend that focuses on the advantages provided by both of them.

## **The Key Differences between Hashing and Encryption**

The major difference between encryption and hashing is that encryption is a two-way function that includes both encryption and decryption while hashing is a one-way function that changes data into an irreversible output. Hashing allows the users to validate data by recognizing all the differences to the output. The purpose of encryption is to encrypt data to make it more secure and less vulnerable to external attacks.

In a nutshell, hashing and encryption both provide with means of providing security to data and maintaining privacy. But don't you think business owners would be more interested in hashing as it is almost impossible to break the code? However, at the same time, it is also important to encrypt data so that it can be deciphered at the receiver end. Hashing is more useful in instances where data needs to be stored rather than being transmitted.

The clear differences between the two are the reason why businesses need to understand where they should use hashing and where they should use encryption to maximize the advantages provided by both the functions.