What is cryptography hashing?

Let's assume that you are sending a movie to your friend. Before sending the movie, you let your friend know the title of the movie and the summary of the movie. After making sure all things go smoothly and correctly, you proceed to send the movie to your friend.

You may upload the movie to Google Drive or similar free storage. Once it's done, you will then ask your friend to download the movie through there. Let's say the movie is 2 hours long, your friend downloaded the movie and proceed to watch it.

Your friend encounter a problem, he/she is able to watch the movie until the duration reach 1 hour long but when he/she wants to proceed with watching the movie. No matter how he/she forward the duration or move through the duration. The movie sounds a little off and does not show anything to his/her screen.

He/she proceeds to ask you about the reason that this happens. You just couldn't answer it and to make things worse, you have already checked that the whole movie was uploaded.

You just couldn't figure out the problem. This problem does not only limit to movie, the same problem can also exist when sending files/documents/software. Cryptography hashing was design to solve such issue.

The idea of cryptography hashing was to generate a unique ID that sources from data and can't be reversed. If this sounds too technical, here's another description. The idea of cryptography hashing was that if you feed in any data, it will automatically turn it into a data that's similar to a human's fingerprint.

Any changes made to the data will produce different human's fingerprint.

You can feed the whole movie into cryptography hashing function. It will generate a human's fingerprint. You send that fingerprint to your friend. Your friend waits for the download to finish. Once it's finished, your friend do the same thing as you to make sure the same fingerprint was generated. If it's not the same fingerprint, your friend knows that this movie happens to have some problem and he/she will report that to you.

This is the first problem that cryptography hashing solves.

Any variation to the data that you feed into the cryptography hashing will surely result in producing different human fingerprint. This kind of characteristic was used in passwords/passphrases as the server only needs to know the fingerprint but not the original passwords/passphrases.

Other usage of cryptography hashing includes generating encryption/decryption key from passwords and generating MAC (Message Authentication Code) which was used in symmetric encryption's stream cipher.

https://www.tools4noobs.com/online_tools/hash/ (This link here is a website that allows you to play with numerous cryptography hashing function's algorithms)

This may or may not spark your interests and that's fine. If this sparks your interest, what I hope is you as a user will give more chances to application which deliberately have low user experience and ease of use as they guarantee your security/privacy.