Why are there so many hash functions?

Hash functions are frequently employed for data integrity and in conjunction with digital signatures. Even a 1-bit change in a message will result in a different hash with a good hash function (on average, half of the bits change). With digital signatures, a message is hashed and then the hash itself is signed. Furthermore, they are an important and widely used cryptography building block. They are quite simple to comprehend and apply. Most cryptographic hash functions are designed to accept any length string as input and return a fixed-length hash value. As a result, they are utilized to ensure integrity and authenticity.

Similarly, what is a Cryptographic hash function?

Cryptographic hash functions are a special class among hash functions. Every cryptographic hash function is a hash function. But not every hash function is a cryptographic hash. A cryptographic hash function aims to guarantee several security properties. Most importantly that it's hard to find collisions or pre-images and that the output appears random.

If they are "better" why not just use a cryptographic hash function all the time?

It is not always recommended to use the cryptographic hash function because of some reasons:

* A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.
* This ideology has two flaws: Advances in mathematics and computation may render current algorithms obsolete; Key management and authentication in a large and complex environment are so difficult that they undermine the mathematical strength of the best cryptographic algorithms.
* Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures. These need to be fixed through proper design and the setting up of a defensive infrastructure.
* The security of cryptographic techniques is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.
* Another fundamental need of information security of selective access control also cannot be realized using cryptography. Administrative controls and procedures are required to be exercised for the same.

References:

Cryptography Benefits & Drawbacks. (2022). Retrieved 5 January 2022, from https://www.tutorialspoint.com/cryptography/benefits\_and\_drawbacks.htm

Function?, W. (2012). What is the difference between a Hash Function and a Cryptographic Hash Function?. Retrieved 5 January 2022, from https://security.stackexchange.com/questions/11839/what-is-the-difference-between-a-hash-function-and-a-cryptographic-hash-function