Hashing

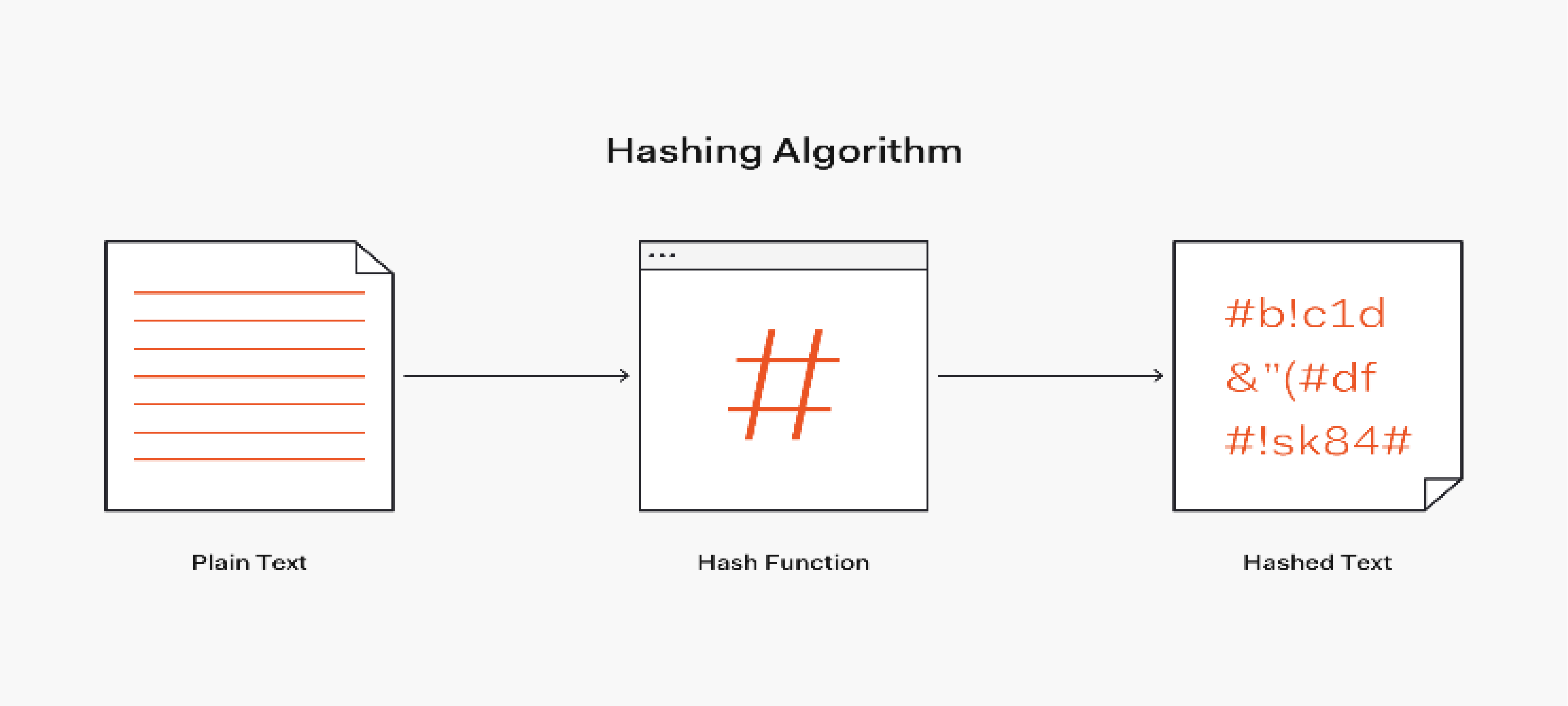
Cyber Security Foundation Course

AGENDA

- Definition
- You should know
- Hash Algorithms
- Hash Usage

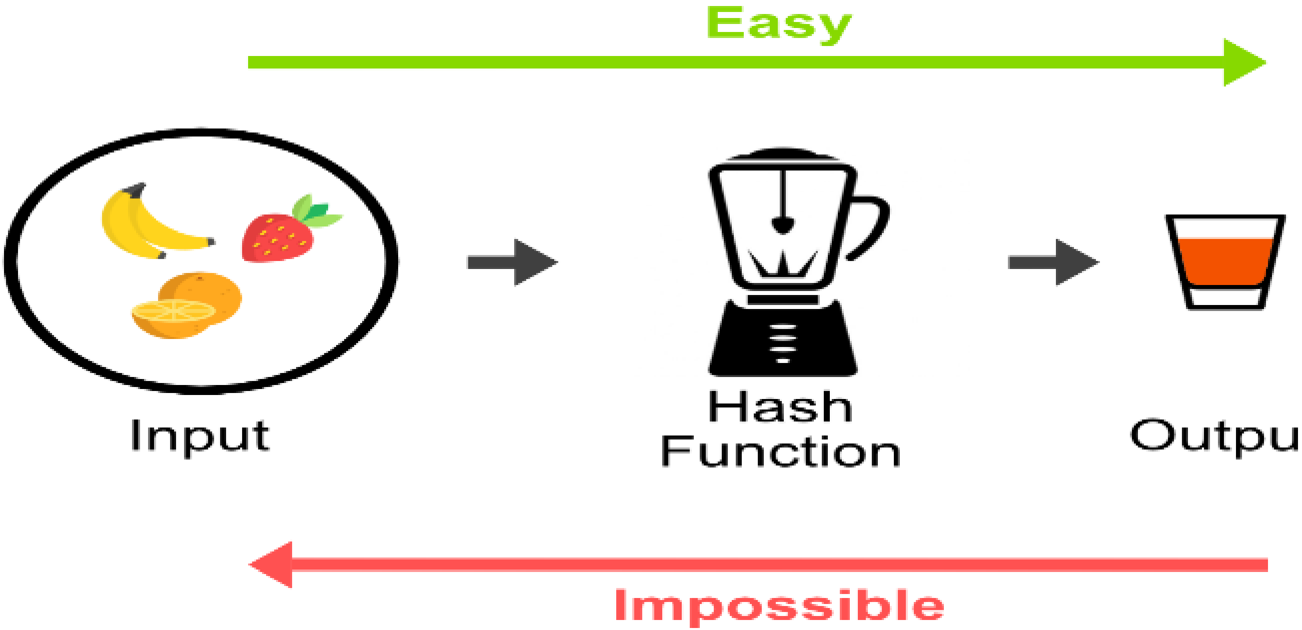
Definition

Hashing is an algorithm performed on data such as word, File or message to Generate a new Characters called a hash, That hash Value is used to verify that data is not modified or corrupted (Date Integrity Check)



You should know

- you can Generate a hash of a file or a message, but you can’t use the hash to Reproduce the original file or message.
- The hashing algorithms always generate the same length regardless the length of plain text or the file Size.
- If one character changed the generated Hash has will also changed.



Hash Algorithms

There are several Hashing algorithms, we will discuss the most common of them

Message Digest 5 (MD5): Produce a unique 32 characters for a file or a Word.
Secure Hash Algorithm (SHA-1): Produce a unique 40 characters for a file or a Word.
Secure Hash Algorithm (SHA-256): Produce a unique 64 hexadecimal characters for a file or a Word.

Hash Usage

- File or Message Integrity Check.
- File Identification for malwares.
- Password Storing

Thanks!

Any questions?