CSC-370
E - Commerce
(BSc CSIT, TU)

Ganesh Khatri
kh6ganesh@gmail.com

9. Data Transaction Security

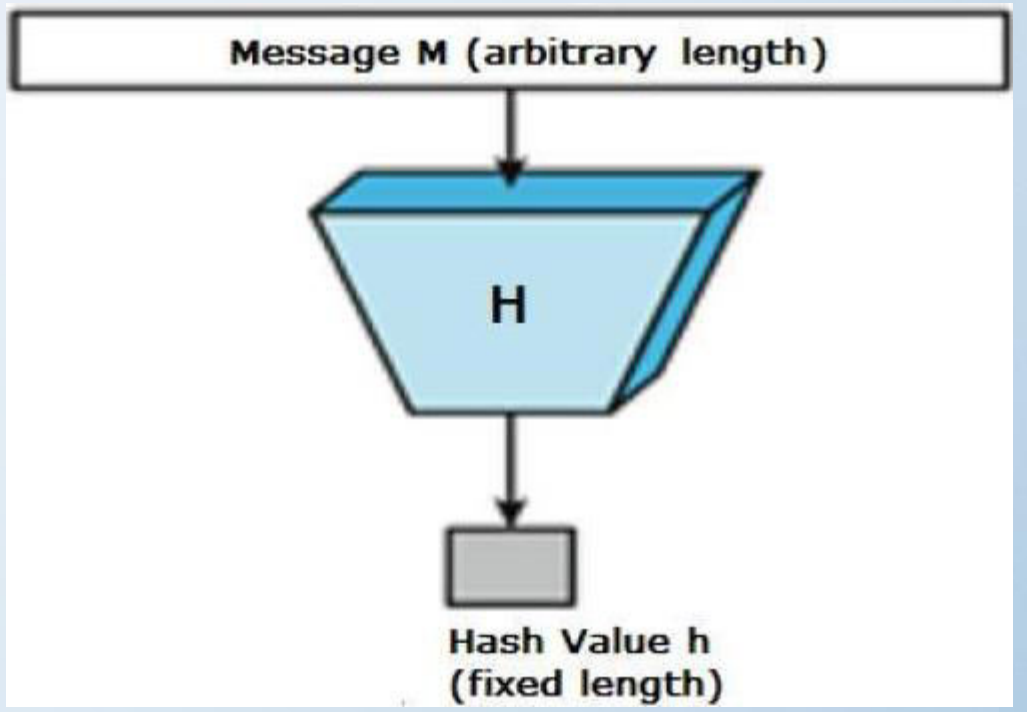
- Many people regularly bank and shop online with ease, confident that the millions of transactions that take place each day are secure.
- Good safeguards are in place, but as the internet is constantly susceptible to new threats, these best practices will help you keep your money and financial information safe
- Online buying presents challenges to keeping your money safe, but if you're smart, they're challenges that aren't too hard to overcome
- Different methods can be used to secure online transactions
  1. Picking a secure password
  2. Two-factor authentication
  3. Use of well known and secured payment gateway apps.
  4. Use of web browser privacy mode
  5. Keeping the browser up to date
  6. Disable Autocomplete/Password storage in-browser
  7. Passwords - make them complex, change them frequently etc.

9. Data Transaction Security

- is an algorithm that takes an arbitrary amount of data input - a credential - and produces a fixed-size output of enciphered text called a hash value, or just "hash." or message digest.
- That enciphered text can then be stored instead of the password itself, and later used to verify the user.
- hash functions are extremely useful and appear in almost all information security applications.
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.
- The input to the hash function is of arbitrary length but output is always of fixed length.

Security Mechanisms : Hash Functions

- **Features**
  - **Fixed Length Output (Hash Value) :** Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data. In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions
  - **Efficiency of Operation :** Generally for any hash function h with input x, computation of h(x) is a fast operation. Computationally hash functions are much faster than a symmetric encryption



Security Mechanisms : Hash Functions

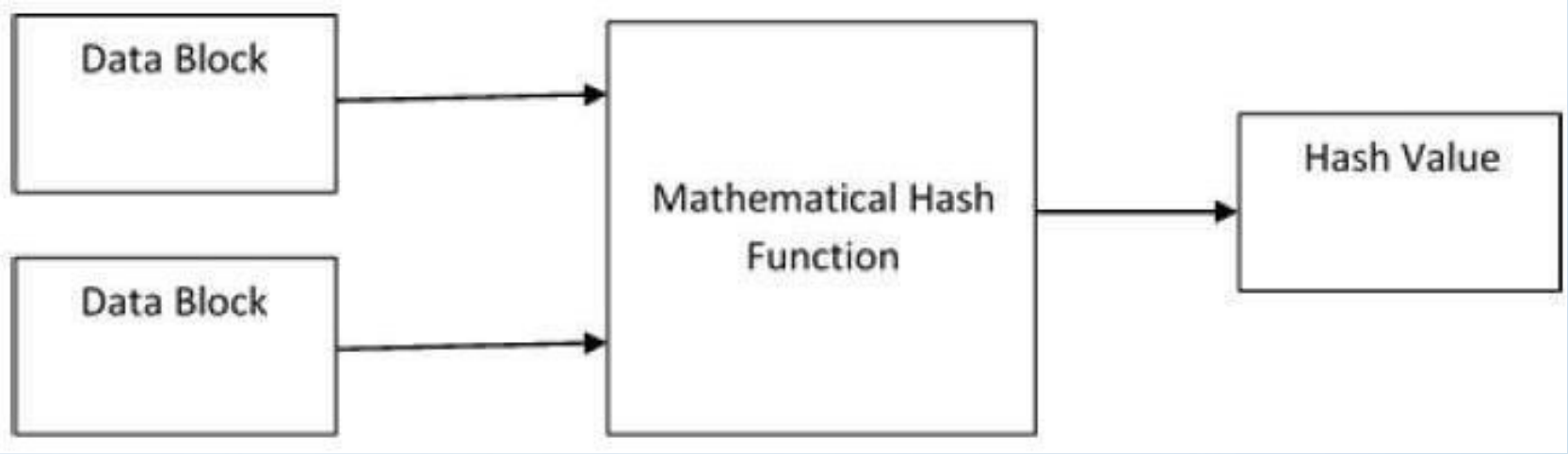
- **Properties :**
- **Pre-Image Resistance :**
  - This property means that it should be computationally hard to reverse a hash function.
  - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  - This property protects against an attacker who only has a hash value and is trying to find the input
- **Second Pre-Image Resistance :**
  - This property means given an input and its hash, it should be hard to find a different input with the same hash.
  - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).

Security Mechanisms : Hash Functions

- **Properties :**
- **Collision Resistance :**
  - This property means it should be hard to find two different inputs of any length that result in the same hash.
  - This property is also referred to as collision free hash function.
  - In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
  - Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions.
  - This property of collision free only confirms that these collisions should be hard to find.
  - This property makes it very difficult for an attacker to find two input values with the same hash

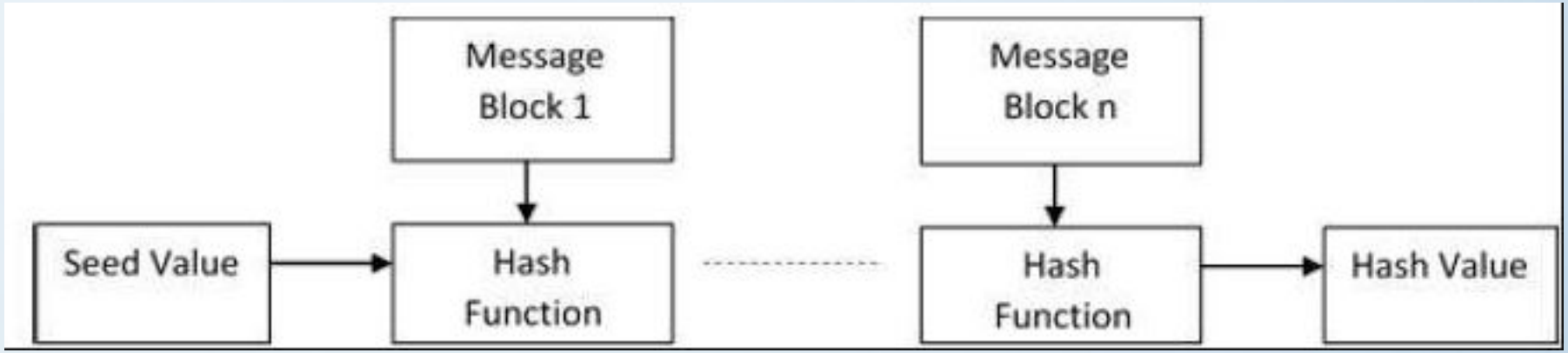
Security Mechanisms : Hash Functions

- **Design of Hashing Algorithms**
  - At the heart of a hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code.
  - This hash function forms the part of the hashing algorithm.
  - The size of each data block varies depending on the algorithm.
  - Typically the block sizes are from 128 bits to 512 bits.
  - The following illustration demonstrates hash function :



Security Mechanisms : Hash Functions

- **Design of Hashing Algorithms**
  - Hashing algorithm involves rounds of above hash function like a block cipher.
  - Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round.
  - this process is repeated for as many rounds as are required to hash the entire message.
  - Schematic of hashing algorithm is depicted in the following illustration



Security Mechanisms : Hash Functions

- **Design of Hashing Algorithms**
  - Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on.
  - This effect, known as an avalanche effect of hashing
  - **Hash function** generates a hash code by operating on two blocks of fixed-length binary data
  - **Hashing algorithm** is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together

Security Mechanisms : Hash Functions

- Examples of popular hash functions are :
- **Message Digest(MD) :**
  - It is a 128-bit hash function.
  - Different versions are MD2, MD4, MD5 and MD6
  - Most popular version is MD5.
  - In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster.
  - This collision attack resulted in compromised MD5 and hence it is no longer recommended for use

Security Mechanisms : Hash Functions

- Examples of popular hash functions are :
- **Secure Hash Function (SHA) :**
  - Different versions are : SHA-0, SHA-1, SHA-2, and SHA-3
  - The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993.
  - SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.
  - SHA-3 is the latest version developed in 2012.

Security Mechanisms : Hash Functions

- Examples of popular hash functions are :
- **RIPEMD :**
  - The RIPEMD is an acronym for RACE Integrity Primitives Evaluation Message Digest.
  - This set of hash functions was designed by open research community and generally known as a family of European hash functions.
  - Versions : RIPEMD, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.

Security Mechanisms : Hash Functions

- Examples of popular hash functions are :
- **Whirlpool :**
  - This is a 512-bit hash function.
  - It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.
  - Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.