Hashing

- Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.

- Hashing is a cryptographic technique that produces hash values using an algorithm or hash function for accessing data for security purposes.

- A hash value (or simply hash), also called a message digest, is a number generated from a string of text.

- The hash is substantially smaller than the text itself.

- In hashing, a fixed-length message digest is created out of a variable-length message.

- The digest is normally much smaller than the message.

- Creates a unique, fixed- length signature for a message or data set.

- Compare sets of data.

- Hash is unique to a specific message, even minor changes to that message result in a dramatically different hash.

- Very resistant to tampering.

- Hashing also refers to a search technique or a method of accessing data records,

- Search time is independent of the number of the elements in the collection.

Importance of Hashing

- Hashing is used to index and retrieve items in a database.

- It is faster to find the item using the shorter hashed key than to find it using the original value.

- In addition to faster data retrieval, hashing is also used to encrypt and decrypt digital signatures (used to authenticate message senders and receivers).

Importance of Hashing

- Hashing plays vital a role in security systems to ensure that transmitted messages have not been tampered with.

- The sender generates a hash of the message, encrypts it, and sends it with the message itself.

- The recipient then decrypts both the message and the hash, produces another hash from the received message

- Compares the two hashes. If same, high probability that the message was transmitted intact.

Importance of Hashing

- A hash function is a formula or an algorithm that-
  - ***takes large data sets of variable length as input, and***
  - ***returns smaller data sets of fixed length as output.***

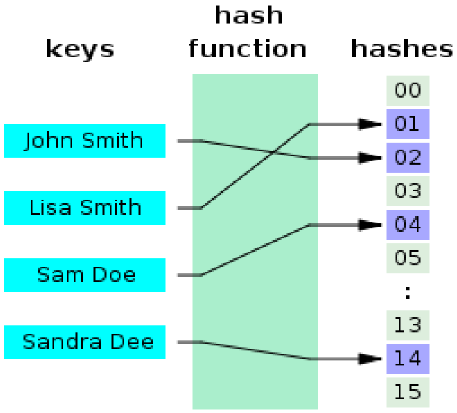
- The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

- Hash function creates hash value in such a way that it is extremely unlikely that some other text will produce the same hash value.

Importance of Hashing

- A hash table (also called hash map) is used to implement an associative array that can map keys to values.

- A hash table uses a hash function to compute an index into an array of buckets or slots, from which the correct value can be found.



Cryptographic Hash Function

- A cryptographic hash function is a hash function

  input - arbitrary block of data
  output - a fixed-size bit string

- The returned value - cryptographic hash value.

- Cryptographic hash function creates hash value - change to the data will change the hash value.

- Therefore, it is extremely unlikely that some other text will produce the same hash value.

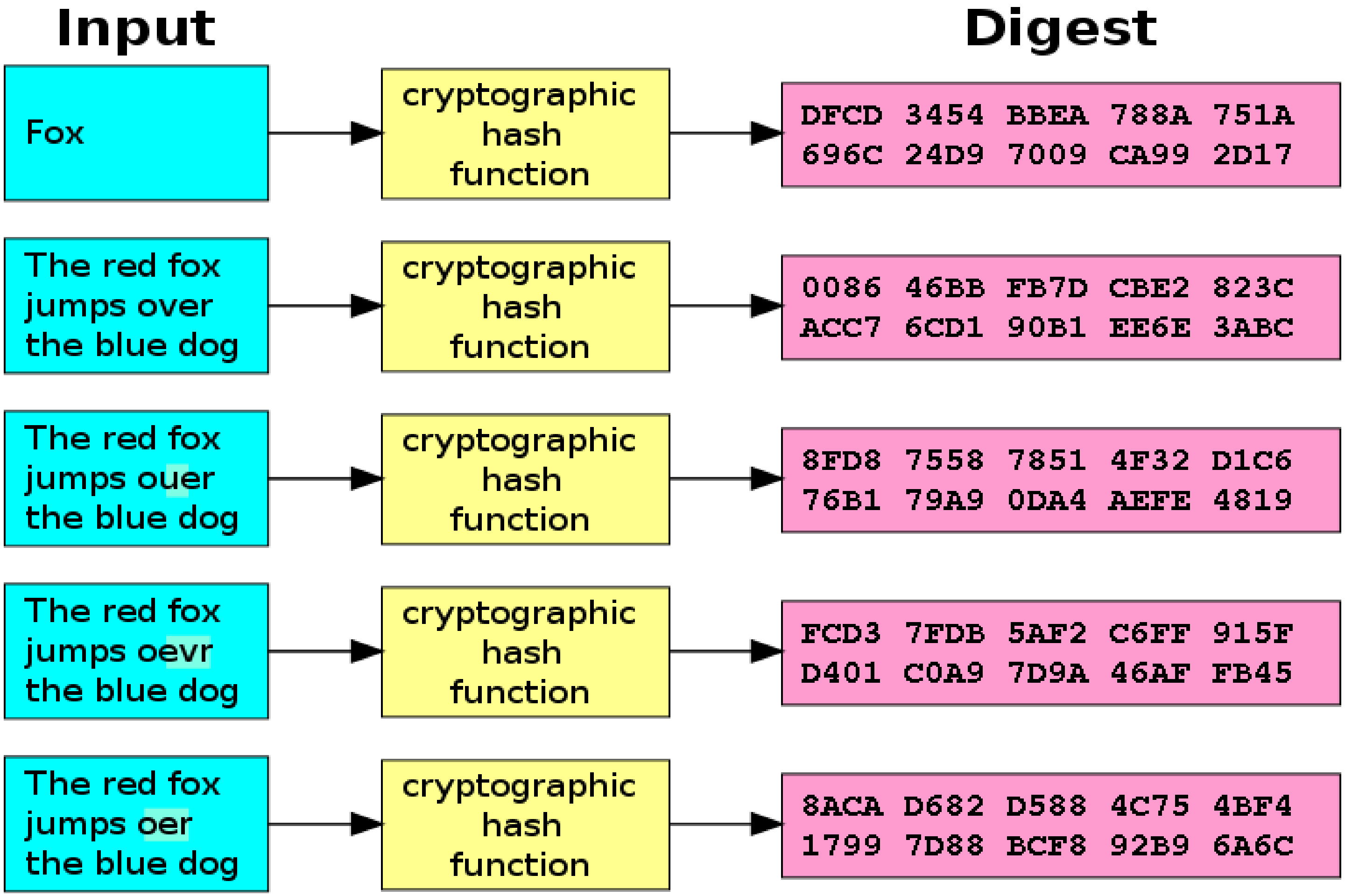
- The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest.

Cryptographic Hash Function

- In cryptographic hash function, even a small changes in the input would cause a large change in the output.

- Figure below shows how the slight changes input (here in the word "over") drastically change the resulting output.

Cryptographic Hash Function



Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Use of Hash Function

- Cryptographic hash functions have many information security applications

  - *digital signatures*
  - *message authentication codes (MACs)*
  - *other forms of authentication*

- Hash functions are primarily used to generate fixed-length output data that acts as a shortened reference to the original data. This is useful when the output data is too cumbersome to use in its entirety.

Use of Hash Function

- ***For example, consider a list of person’s names. Here, name of each person is of variable length. Searching for a person's name in the list is slow; time required to retrieve each name may also vary. But if each name could be hashed to a fixed length integer, then searching and retrieving each name will be performed in faster with constant time.***

- To accelerate table lookup or data comparison tasks such as
  - finding items in a database,
  - detecting duplicated or similar records in a large file,
  - finding similar stretches in DNA sequences, and so on.

Hash Functions Used in Cryptography

Commonly used hash functions are MD5 and SHA-1.

MD5:

- MD - Message Digest.
- Several MD hash algorithms designed by Ron Rivest are MD2, MD4 and MD5.
- The last version MD5 is more secured than the previous versions.
- It divides the message into blocks of 512 bits and creates a 128-bit digest.

Hash Functions Used in Cryptography

SHA-1:

- SHA stands for Secure Hash Algorithm.
- This standard was developed by NIST (National Institute of Standards and Technology).
- This standard is mostly based on MD5.
- Several versions of SHA standard were realsed: SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.
- SHA-1 returns a string of 160 bits.
- Both MD5 and SHA-1 hash functions are built with the Merkle- Damgard construction.

Hash Functions Used in Cryptography

Merkle-Damgard Scheme:

- The Merkle-Damgard construction method takes an arbitrary sized input and breaks the input into fixed size blocks of the same size as the output.
- It applies a one way compression function to each of the blocks in turn, combining a block of input with the output of the previous block.
- The last block has bits representing the length of the entire message.

Hash Functions Used in Cryptography

- A one way compression function
  - two fixed size inputs - the key and the plain text
  - one single output - the cipher text

which is the same size as the plain text.

- Example - Davis-Meyer compression function.

Hash Functions Used in Cryptography

- It feeds the previous hash value (Hi-1) as the plaintext to be encrypted.

- Uses the each block of the message (mi) as the key.

- The output ciphertext is then XORed with the previous hash value (Hi-1) to produce the next hash value (Hi). In the first round when there is no previous hash value it uses a predefined inital value (H0).

Application of Hash Function in Cryptography

Hash functions are used for:

- Verifying the integrity of message and file
- Verifying password for secure login
- fingerprints of keys
- authentication
- digital signatures

Application of Hash Function in Cryptography

Verifying the integrity of files or messages:

- Determining whether any changes have been made to a message, is accomplished by comparing message digests calculated before and after transmission

- Most digital signature algorithms only confirm the authenticity of a hashed digest of the message to be "signed".

- Verifying the authenticity of a hashed digest of the message is considered proof that the message itself is authentic.

Application of Hash Function in Cryptography

Verifying password for secure login:

- Storing all user passwords as plaintext character can result in a massive security breach if the password file is compromised.

- Only store the hash digest of each password

- Any user can read the contents of the file, but, because the hash function is a one-way function, it is almost impossible to guess the value of the password.

Application of Hash Function in Cryptography

Verifying password for secure login:

- When the password is created , the system hashes it and stores the hash in the password file.

- When the user sends her user ID and password, the system creates a hash of the password and then compare the hash value with the one stored in the file.

- If there is a match, the user is granted access; otherwise, access is denied.

Application of Hash Function in Cryptography

Authentication:

- Authentication is the assurance that the communicating entity is the one that it claims to be.

- Cryptographic hash function can be used for provide authentication.

Application of Hash Function in Cryptography

Digital Signature:

- When making a digital signature, cryptographic hash functions are generally used to construct the message digest.

- A digital signature servers three important purposes:
  - Verifies data integrity.
  - Provides authentication of the sender.
  - Provides non-repudiation

Simple Hash Function

Some Popular Hash Function:

- Division-remainder method
- Mid-square method
- Folding method

THANK YOU!!!