36 Lecture - CS403

Important Subjective

1. **What is the purpose of hashing?**
   Answer: The purpose of hashing is to convert data into a fixed-length value or key that represents the original data. It is used for various applications, such as data encryption, password storage, and digital signatures.

   How does a hash function work?
   Answer: A hash function takes an input (such as a password or data file) and produces a fixed-length output (the hash value) based on the input data. The hash function is designed to be one-way, meaning that it is computationally infeasible to reverse the process and obtain the original data from the hash value.

   What is a hash collision?
   Answer: A hash collision occurs when two different inputs produce the same hash output. This can be a security risk in certain applications, such as password storage, as it can allow an attacker to access sensitive data.

   What is a salt in the context of password hashing?
   Answer: A salt is a random value that is added to a password before it is hashed. This helps to prevent hash collisions and makes it more difficult for an attacker to crack the password through brute force attacks.

   What are some common hash algorithms?
   Answer: Some common hash algorithms include MD5, SHA-1, SHA-256, and SHA-3.

   What is a rainbow table?
   Answer: A rainbow table is a precomputed table of hash values and corresponding input data. It can be used to crack passwords by comparing the hash value of a password to the values in the table to determine the original password.

   What is a hash function collision attack?
   Answer: A hash function collision attack is a type of attack in which an attacker tries to create two different inputs that produce the same hash output. This can be used to circumvent security measures such as digital signatures.

   What is the difference between a cryptographic hash function and a non-cryptographic hash function?
   Answer: A cryptographic hash function is designed specifically for security applications and is much more difficult to reverse than a non-cryptographic hash function. Non-cryptographic hash functions are used for other applications such as data indexing and searching.

   What is the birthday attack in the context of hash functions?
   Answer: The birthday attack is a type of attack in which an attacker tries to find two different inputs that produce the same hash output. The name comes from the statistical probability of

two people in a room having the same birthday.

What is a hash tree?
Answer: A hash tree is a data structure that uses hash functions to create a hierarchical representation of data. This can be used for efficient storage and verification of large datasets.