TASK 4

1. What is hashing?

Hashing is a process of converting data (like a password) into a fixed-length string called a *hash* using a mathematical algorithm. It is a one-way process, meaning the original data cannot be retrieved from the hash. Hashing is mainly used to secure passwords and verify data integrity.

2. Difference between hashing and encryption

Hashing	Encryption
One-way process	Two-way process
Original data cannot be recovered	Original data can be decrypted
Used for password storage and integrity	Used for secure data transmission
No key is used	Uses encryption and decryption keys

3. What is a brute force attack?

A brute force attack is a method where an attacker tries all possible combinations of passwords or keys until the correct one is found. It is effective against weak passwords and systems without protection like account lockout or rate limiting.

4. Why is MFA important?

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring more than one form of verification, such as a password and a one-time code or biometric. Even if a password is stolen, MFA prevents unauthorized access.

5. What makes a strong password?

A strong password is long, unique, and complex. It should include a mix of uppercase letters, lowercase letters, numbers, and special characters. Strong passwords are difficult to guess and resist brute force and dictionary attacks.