Question 3

Describe how the Caesar cipher encrypts a message and explain its primary weakness in modern cryptography. [5 marks]

Question 4

Explain the purpose of hashing in data security and identify two specific applications where it is used to protect data. [6 marks]

Marking Guide

#	Sample Response	Response	Mark
3	The Caesar cipher encrypts a message by shifting each letter in the plaintext a fixed number of places down or up the alphabet, known as the "key". For example, with a key of 3, 'A' becomes 'D'. To decrypt, the receiver shifts the letters back by the same number of places. Its primary weakness in modern cryptography is its vulnerability to frequency analysis. Every language has a "fingerprint" where certain letters appear more frequently (e.g., 'E' in English). A codebreaker can count the letter frequencies in the encrypted message and, by matching the most common ciphertext letter to the most common plaintext letter, determine the shift key and easily decode the message.	Describes shift method	1
		Provides shift method example	1
		Identifies weakness	1
		Explains frequency analysis	2
		Explains availability	1
4	The purpose of hashing in data security is to convert data into a fixed-size string of characters, creating a unique "fingerprint" for a set of data. This process is largely irreversible, meaning it's difficult to recreate the original data from its hash. Two specific applications where hashing is used to protect data are: 1. Data Integrity: Hashes are used to ensure data has not been altered during transmission or storage. If a file's hash changes after download, it indicates corruption or tampering. This is also known as a checksum. 2. Password Storage: Instead of storing actual passwords, systems store their hashes. When a user logs in, their entered password is hashed and compared to the stored hash. This prevents actual passwords from being exposed even if a password database is breached.	Explains purpose	1
		Mentions irreversible nature	1
		Names data integrity	1
		Explains data integrity	1
		Names password storage	1
		Explains password storage	1