Function 2 outputs

```
file1.txt - 804537a7adfa4e1bce4d72d0b212a80af2dae3a5e
file2.txt - ba429665c8b95d05a963ee89fded2c7f18892d13e
file3.txt - 804537a7adfa4e1bce4d72d0b212a80af2dae3a5e
file4.txt - 7fa2901ebbb731eb283487afc033e45dae210a89e
```

Which of the following statements is supported by the file hashes?

(A) The files **`file1.txt`** and **`file3.txt`** are exact copies of each other.

(B) Function 1 is more secure than Function 2.

(C) Function 1 and Function 2 are the same hashing function.

(D) The files **`file1.txt`** and **`file3.txt`** have a collision in one hashing function.

6. The security manager at a hospital is planning to upgrade the hospital's physical security system to ensure that only authorized personnel can access areas containing sensitive medical equipment and patient records. Because these areas require a high level of security, the manager wants an authentication method that is unique to each individual and extremely difficult for an adversary to duplicate or spoof. Which of the following authentication methods is best suited for these areas?

(A) Authentication token

(B) Password

(C) Retina scan

(D) Access card

12. The system administrator at a high school receives an alert that there may have been multiple unauthorized login attempts to the school's online grading system. To investigate, the administrator decides to review the authentication logs. Which of the following best describes how authentication logs can be used to determine whether unauthorized login attempts have occurred?
    (A) The logs record which password was used in each login attempt, which allows the administrator to verify account ownership.
    (B) The logs record all login activity, which allows the administrator to reconstruct when and how login attempts occurred.
    (C) The logs record the location of each user attempting to log in, which allows the administrator to identify login attempts from other geographic regions.
    (D) The logs record the type of device attempting to log in, which allows the administrator to block unauthorized devices.

13. The network administrator for a manufacturing facility has implemented a signature-based network detection system. Which of the following is a potential impact of using this network detection method instead of anomaly-based detection?
    (A) More false negative alerts
    (B) Higher operating costs
    (C) Slower detection time
    (D) More alert fatigue

14. Consider the following lines from a log file.

```
2025-09-25 08:01:14 ARP Reply: 192.168.1.13 is-at 00:01:5e:00:fc:16
2025-09-25 09:14:15 ARP Reply: 192.168.1.13 is-at 00:3b:cc:5e:ee:01
```

    Which of the following attack types is indicated in the log file?
    (A) ARP poisoning attack
    (B) DNS poisoning attack
    (C) Evil-twin attack
    (D) MAC flooding attack

15. Which of the following best describes the length of a cryptographic hash function output?
    (A) The length of the output is longer than the input due to the hashing process.
    (B) The length of the output is fixed regardless of the length of the input.
    (C) The length of the output varies based on the length of the input.
    (D) The length of the output is shorter than the length of the input.