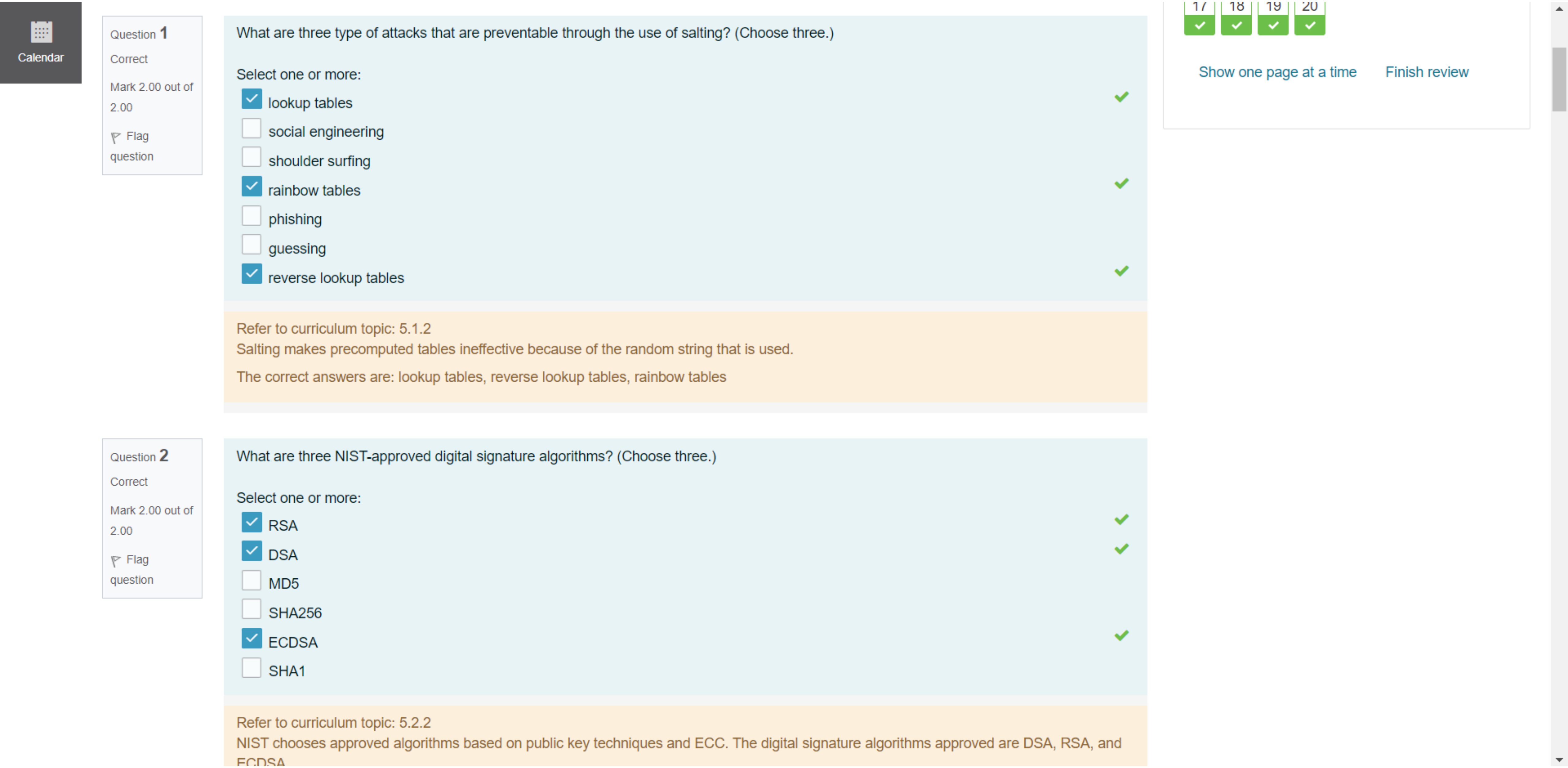


Question **1**

Correct

Mark 2.00 out of 2.00

Flag question

What are three type of attacks that are preventable through the use of salting? (Choose three.)

Select one or more:

☑ lookup tables ✓
□ social engineering
□ shoulder surfing
☑ rainbow tables ✓
□ phishing
□ guessing
☑ reverse lookup tables ✓

Refer to curriculum topic: 5.1.2
Salting makes precomputed tables ineffective because of the random string that is used.

The correct answers are: lookup tables, reverse lookup tables, rainbow tables

Question **2**

Correct

Mark 2.00 out of 2.00

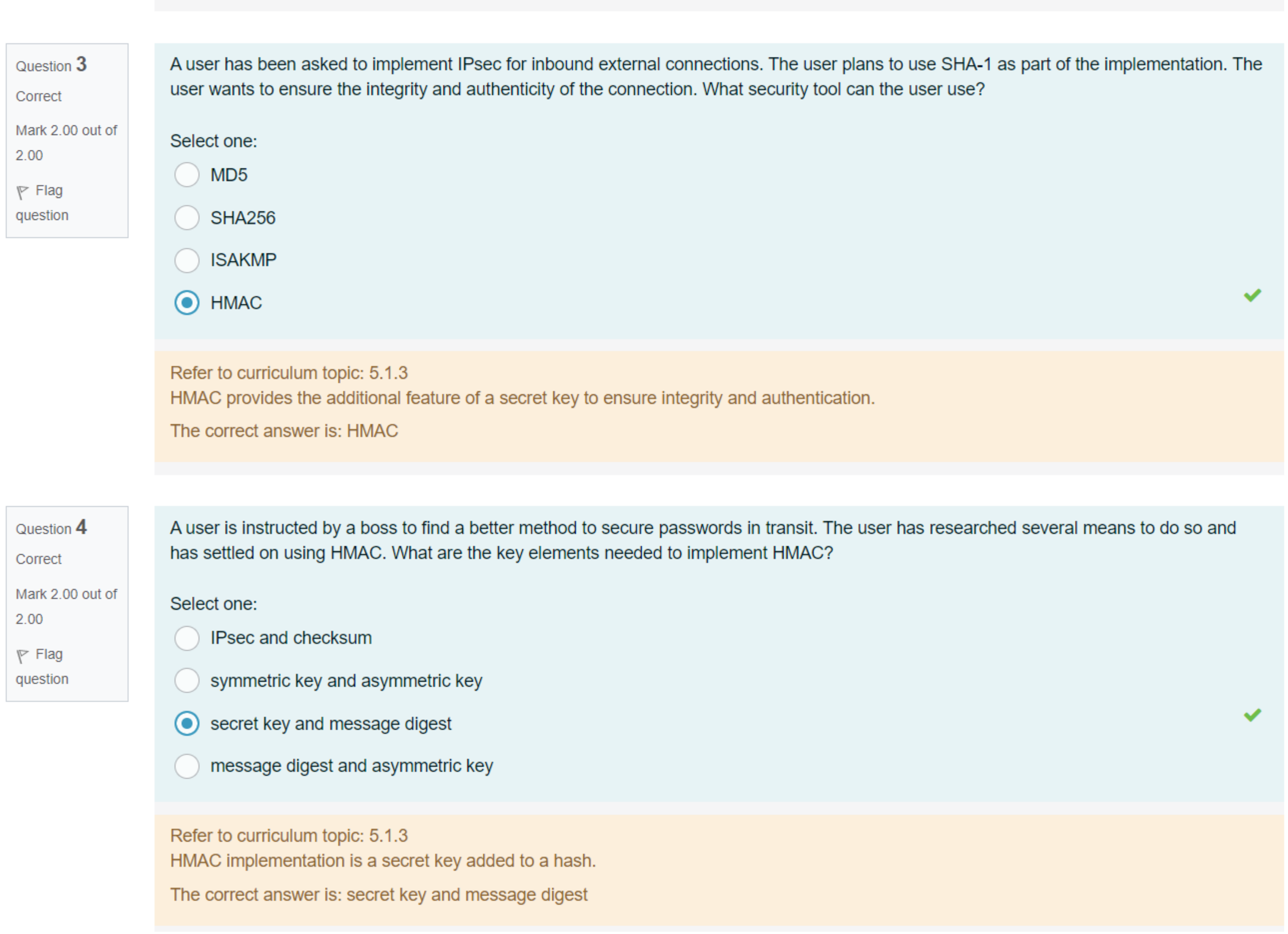
Flag question

What are three NIST-approved digital signature algorithms? (Choose three.)

Select one or more:

☑ RSA ✓
☑ DSA ✓
□ MD5
□ SHA256
☑ ECDSA ✓
□ SHA1

Refer to curriculum topic: 5.2.2
NIST chooses approved algorithms based on public key techniques and ECC. The digital signature algorithms approved are DSA, RSA, and ECDSA



Question **3**

Correct

Mark 2.00 out of 2.00

Flag question

A user has been asked to implement IPsec for inbound external connections. The user plans to use SHA-1 as part of the implementation. The user wants to ensure the integrity and authenticity of the connection. What security tool can the user use?

Select one:

○ MD5

○ SHA256

○ ISAKMP

● HMAC ✓

Refer to curriculum topic: 5.1.3
HMAC provides the additional feature of a secret key to ensure integrity and authentication.

The correct answer is: HMAC

Question **4**

Correct

Mark 2.00 out of 2.00

Flag question

A user is instructed by a boss to find a better method to secure passwords in transit. The user has researched several means to do so and has settled on using HMAC. What are the key elements needed to implement HMAC?

Select one:

○ IPsec and checksum

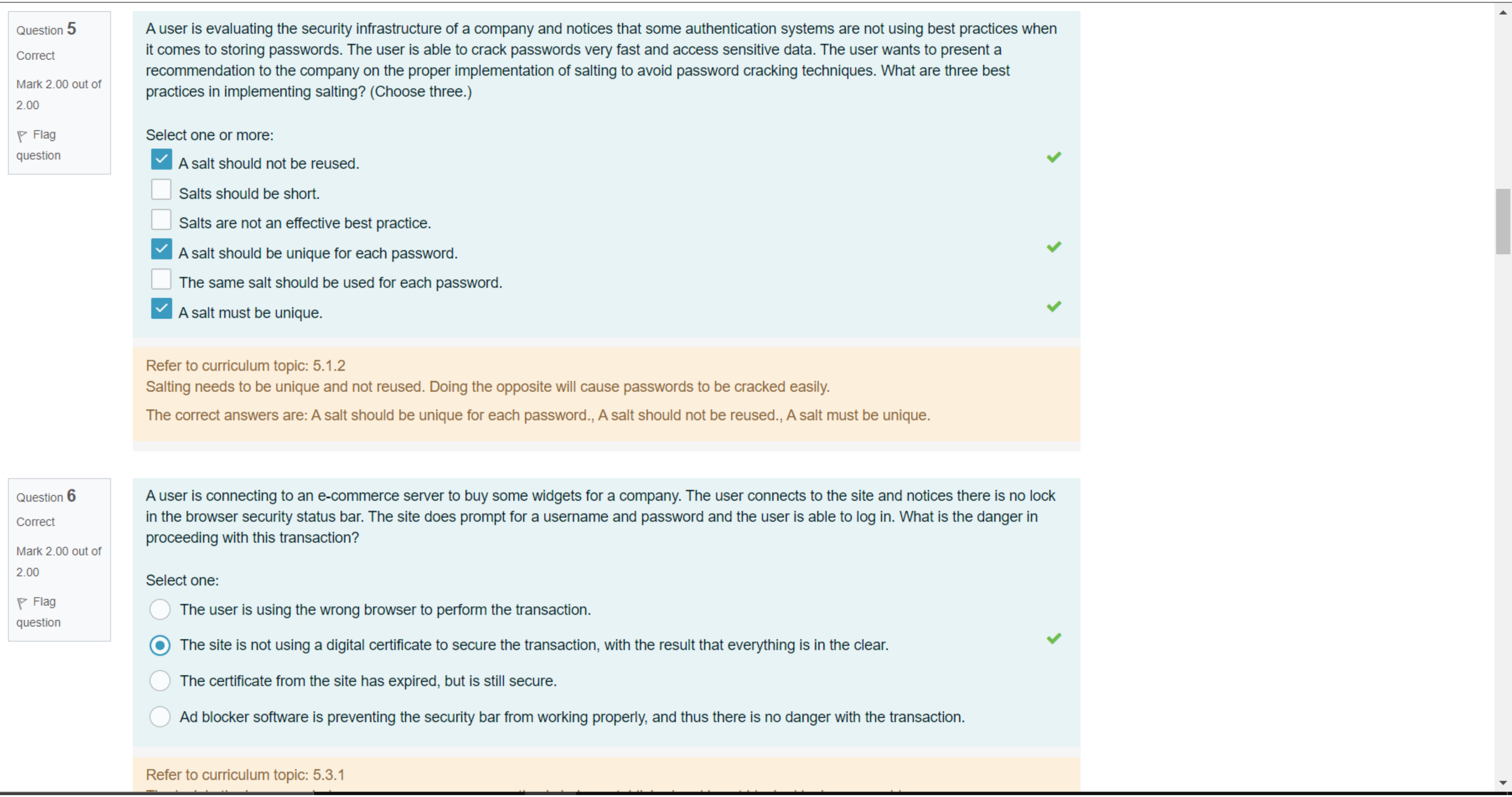
○ symmetric key and asymmetric key

● secret key and message digest ✓

○ message digest and asymmetric key

Refer to curriculum topic: 5.1.3
HMAC implementation is a secret key added to a hash.

The correct answer is: secret key and message digest



Question 5

Correct

Mark 2.00 out of 2.00

Flag question

A user is evaluating the security infrastructure of a company and notices that some authentication systems are not using best practices when it comes to storing passwords. The user is able to crack passwords very fast and access sensitive data. The user wants to present a recommendation to the company on the proper implementation of salting to avoid password cracking techniques. What are three best practices in implementing salting? (Choose three.)

Select one or more:

- ☑ A salt should not be reused. ✓
- □ Salts should be short.
- □ Salts are not an effective best practice.
- ☑ A salt should be unique for each password. ✓
- □ The same salt should be used for each password.
- ☑ A salt must be unique. ✓

Refer to curriculum topic: 5.1.2
Salting needs to be unique and not reused. Doing the opposite will cause passwords to be cracked easily.

The correct answers are: A salt should be unique for each password., A salt should not be reused., A salt must be unique.

Question 6

Correct

Mark 2.00 out of 2.00

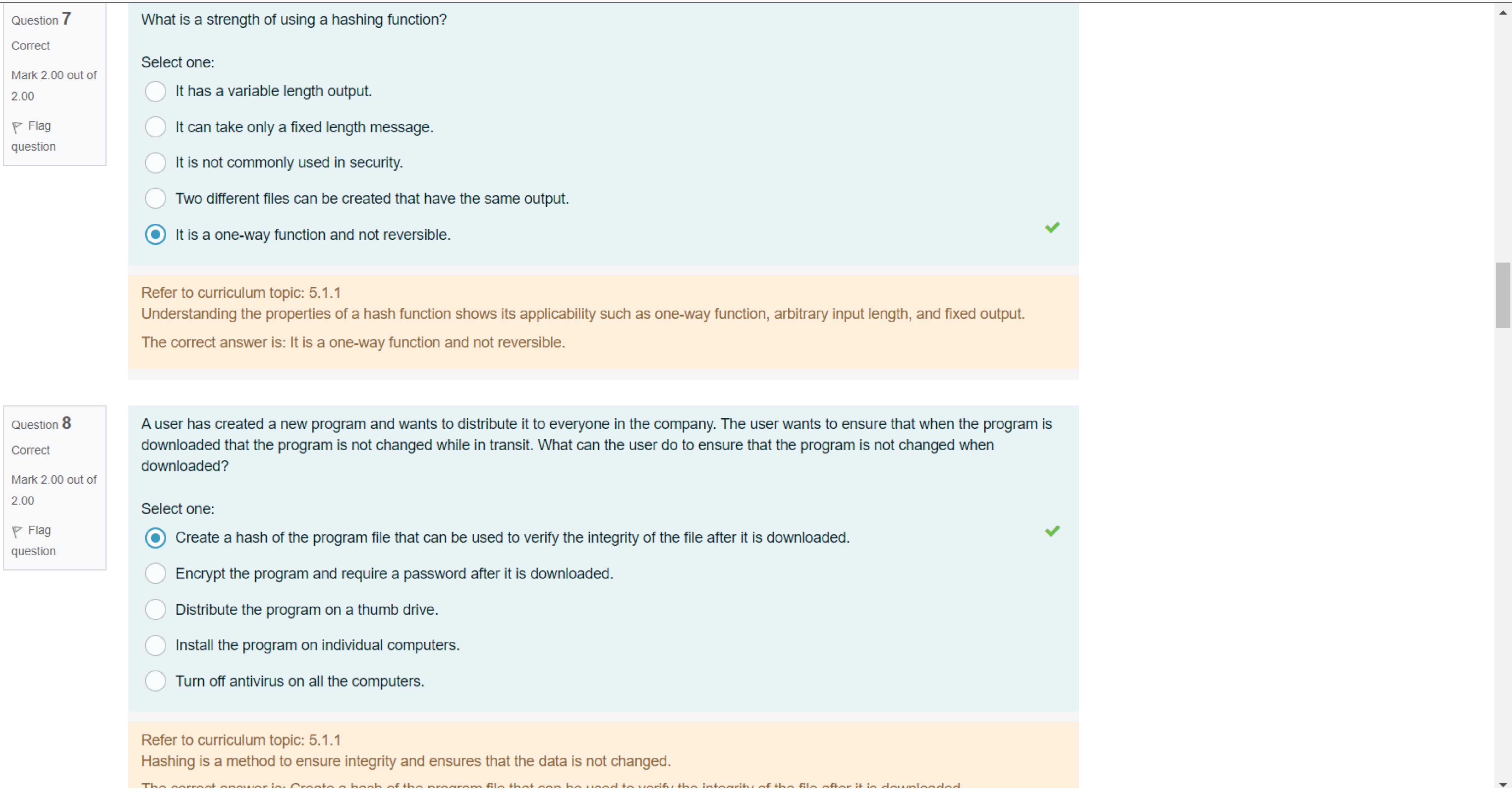
Flag question

A user is connecting to an e-commerce server to buy some widgets for a company. The user connects to the site and notices there is no lock in the browser security status bar. The site does prompt for a username and password and the user is able to log in. What is the danger in proceeding with this transaction?

Select one:

- ○ The user is using the wrong browser to perform the transaction.
- ● The site is not using a digital certificate to secure the transaction, with the result that everything is in the clear. ✓
- ○ The certificate from the site has expired, but is still secure.
- ○ Ad blocker software is preventing the security bar from working properly, and thus there is no danger with the transaction.

Refer to curriculum topic: 5.3.1



Question 7

Correct

Mark 2.00 out of 2.00

Flag question

What is a strength of using a hashing function?

Select one:

○ It has a variable length output.

○ It can take only a fixed length message.

○ It is not commonly used in security.

○ Two different files can be created that have the same output.

● It is a one-way function and not reversible. ✓

Refer to curriculum topic: 5.1.1
Understanding the properties of a hash function shows its applicability such as one-way function, arbitrary input length, and fixed output.

The correct answer is: It is a one-way function and not reversible.

Question 8

Correct

Mark 2.00 out of 2.00

Flag question

A user has created a new program and wants to distribute it to everyone in the company. The user wants to ensure that when the program is downloaded that the program is not changed while in transit. What can the user do to ensure that the program is not changed when downloaded?

Select one:

● Create a hash of the program file that can be used to verify the integrity of the file after it is downloaded. ✓

○ Encrypt the program and require a password after it is downloaded.

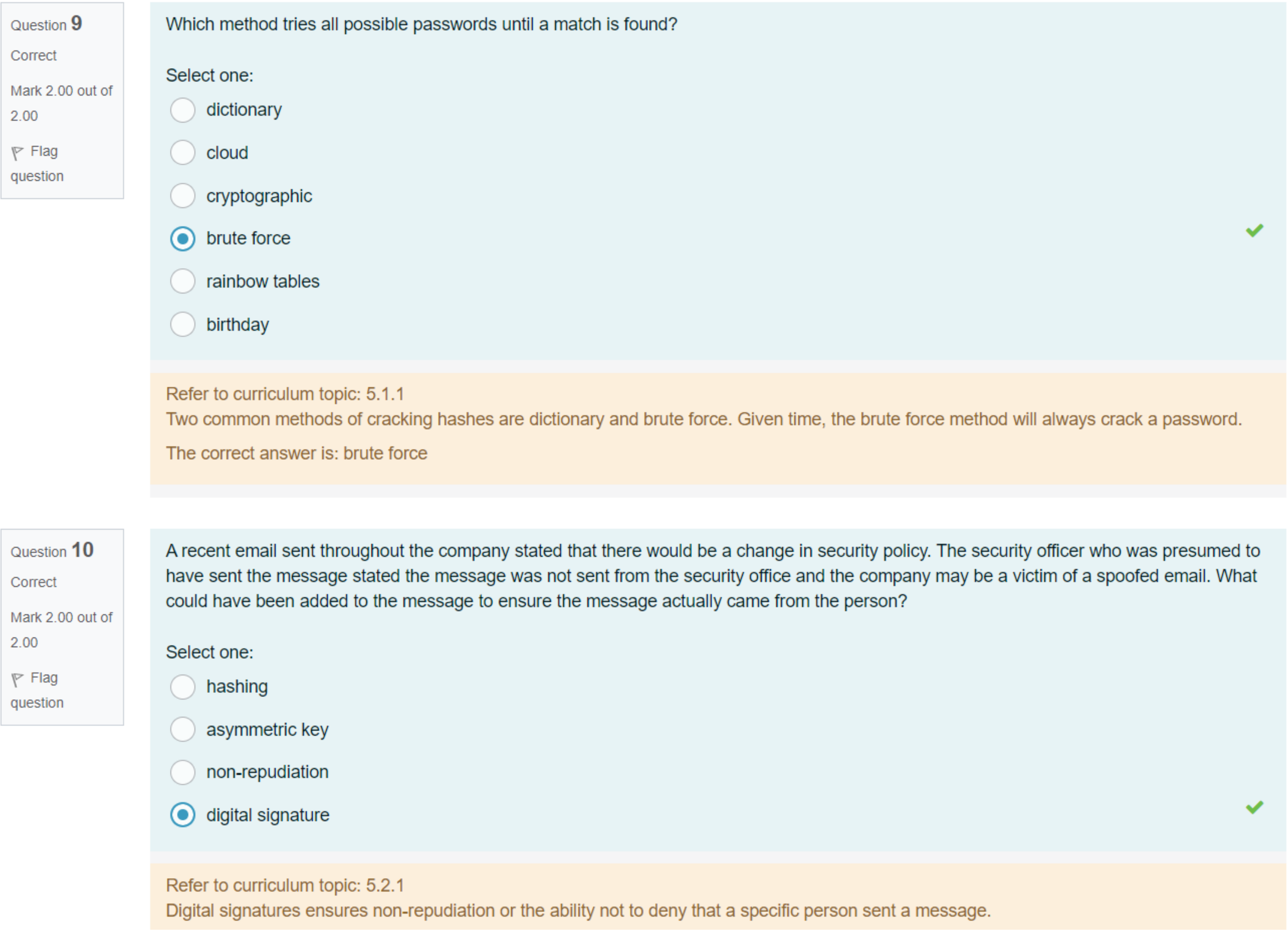
○ Distribute the program on a thumb drive.

○ Install the program on individual computers.

○ Turn off antivirus on all the computers.

Refer to curriculum topic: 5.1.1
Hashing is a method to ensure integrity and ensures that the data is not changed.

The correct answer is: Create a hash of the program file that can be used to verify the integrity of the file after it is downloaded.



Question **9**

Correct

Mark 2.00 out of 2.00

Flag question

Which method tries all possible passwords until a match is found?

Select one:

○ dictionary

○ cloud

○ cryptographic

● brute force ✓

○ rainbow tables

○ birthday

Refer to curriculum topic: 5.1.1
Two common methods of cracking hashes are dictionary and brute force. Given time, the brute force method will always crack a password.

The correct answer is: brute force

Question **10**

Correct

Mark 2.00 out of 2.00

Flag question

A recent email sent throughout the company stated that there would be a change in security policy. The security officer who was presumed to have sent the message stated the message was not sent from the security office and the company may be a victim of a spoofed email. What could have been added to the message to ensure the message actually came from the person?

Select one:

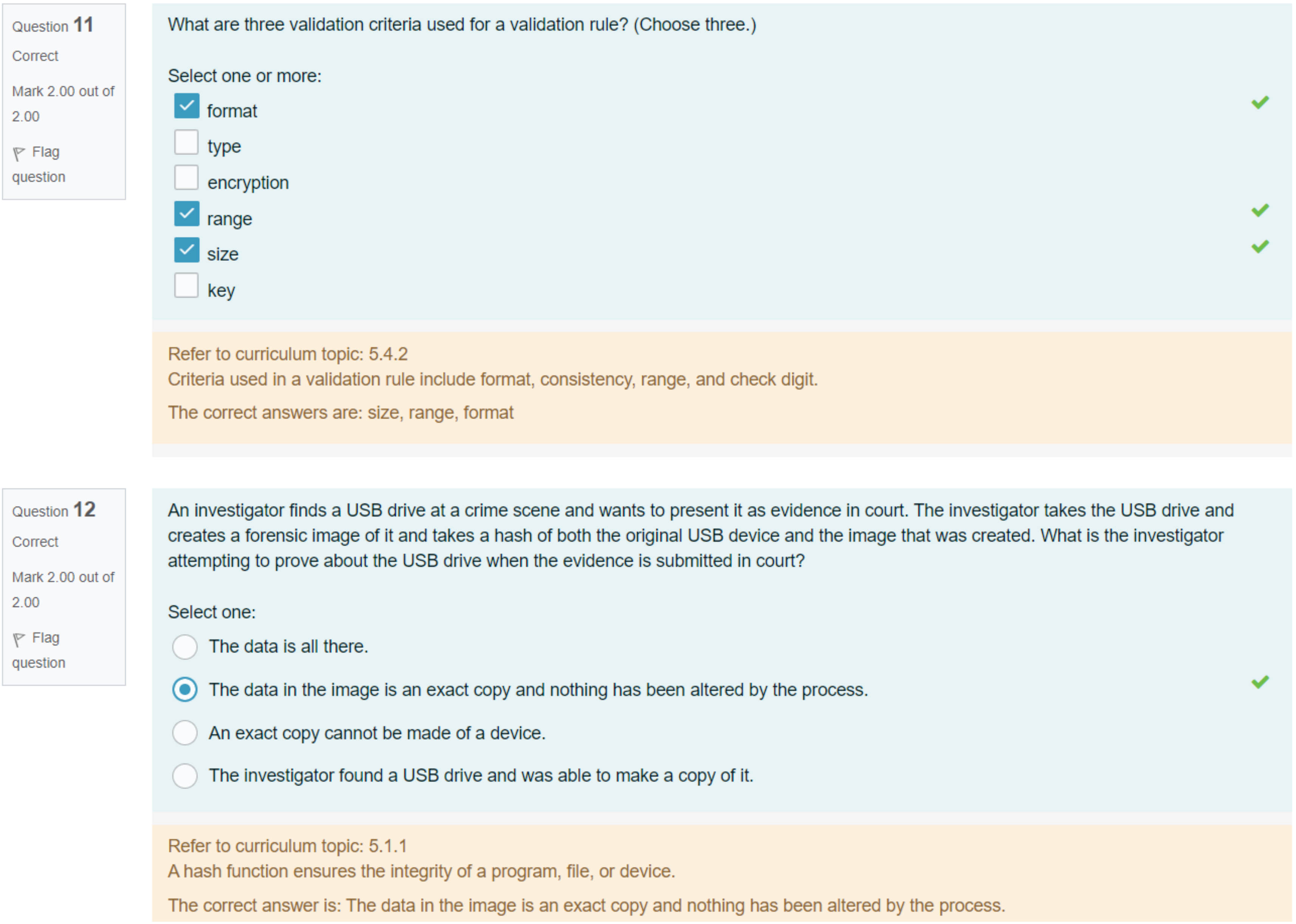
○ hashing

○ asymmetric key

○ non-repudiation

● digital signature ✓

Refer to curriculum topic: 5.2.1
Digital signatures ensures non-repudiation or the ability not to deny that a specific person sent a message.



Question **11**

Correct

Mark 2.00 out of 2.00

Flag question

What are three validation criteria used for a validation rule? (Choose three.)

Select one or more:

- ☑ format ✓
- □ type
- □ encryption
- ☑ range ✓
- ☑ size ✓
- □ key

Refer to curriculum topic: 5.4.2
Criteria used in a validation rule include format, consistency, range, and check digit.

The correct answers are: size, range, format

Question **12**

Correct

Mark 2.00 out of 2.00

Flag question

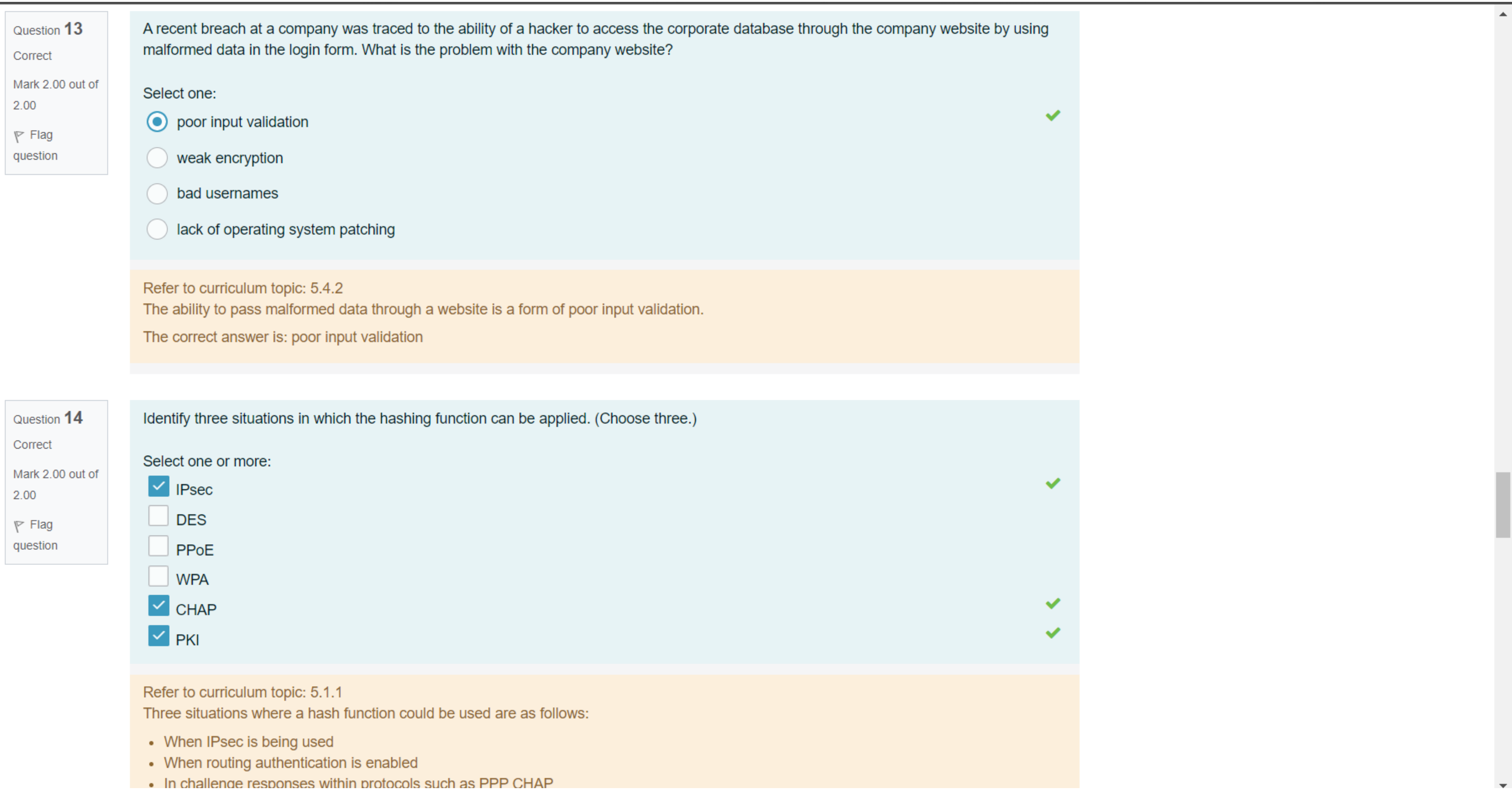
An investigator finds a USB drive at a crime scene and wants to present it as evidence in court. The investigator takes the USB drive and creates a forensic image of it and takes a hash of both the original USB device and the image that was created. What is the investigator attempting to prove about the USB drive when the evidence is submitted in court?

Select one:

- ○ The data is all there.
- ● The data in the image is an exact copy and nothing has been altered by the process. ✓
- ○ An exact copy cannot be made of a device.
- ○ The investigator found a USB drive and was able to make a copy of it.

Refer to curriculum topic: 5.1.1
A hash function ensures the integrity of a program, file, or device.

The correct answer is: The data in the image is an exact copy and nothing has been altered by the process.



Question **13**

Correct

Mark 2.00 out of 2.00

Flag question

A recent breach at a company was traced to the ability of a hacker to access the corporate database through the company website by using malformed data in the login form. What is the problem with the company website?

Select one:

● poor input validation ✓

○ weak encryption

○ bad usernames

○ lack of operating system patching

Refer to curriculum topic: 5.4.2
The ability to pass malformed data through a website is a form of poor input validation.

The correct answer is: poor input validation

Question **14**

Correct

Mark 2.00 out of 2.00

Flag question

Identify three situations in which the hashing function can be applied. (Choose three.)

Select one or more:

☑ IPsec ✓

☐ DES

☐ PPoE

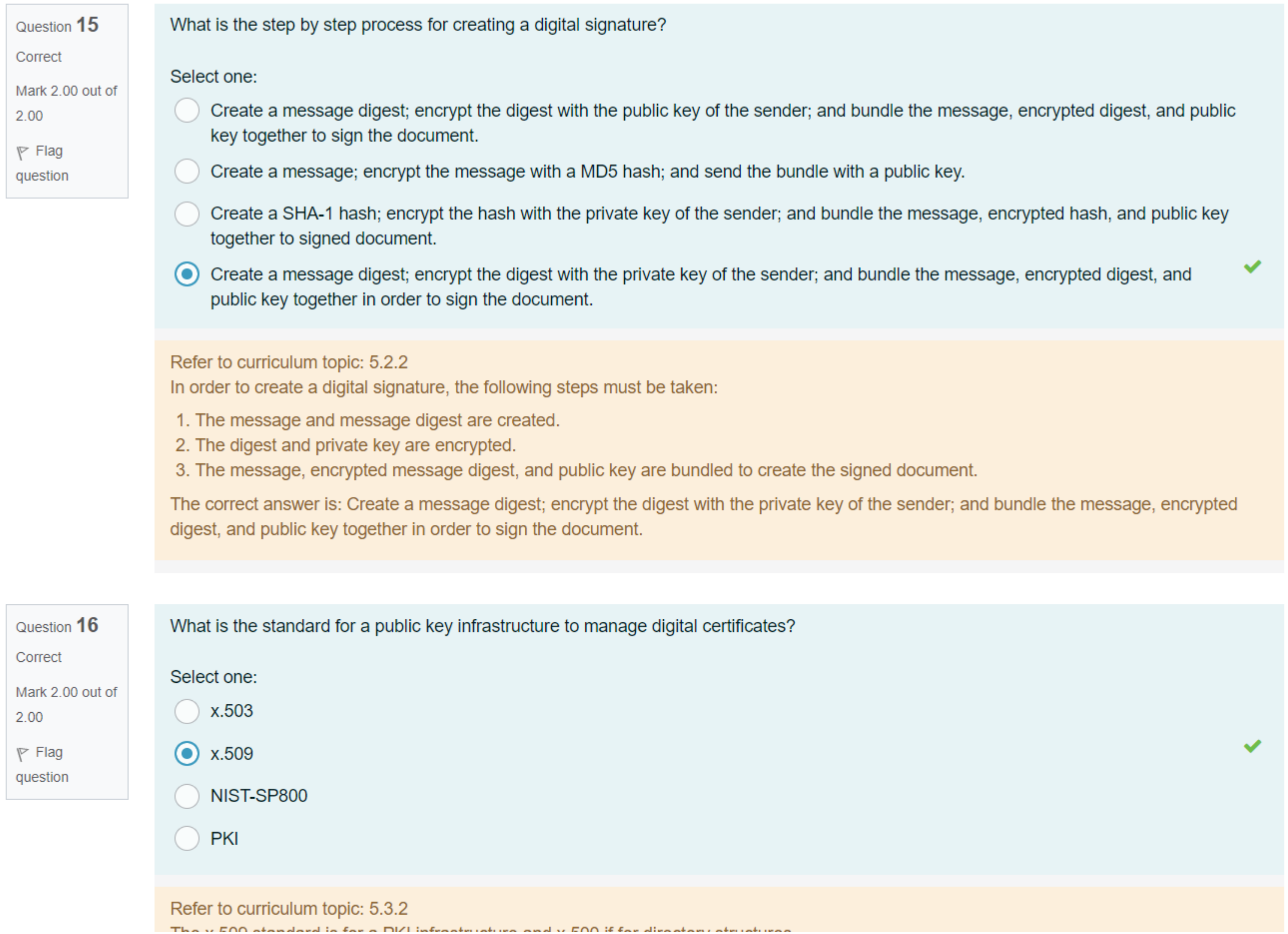
☐ WPA

☑ CHAP ✓

☑ PKI ✓

Refer to curriculum topic: 5.1.1
Three situations where a hash function could be used are as follows:

- When IPsec is being used
- When routing authentication is enabled
- In challenge responses within protocols such as PPP CHAP



Question **15**

Correct

Mark 2.00 out of 2.00

Flag question

What is the step by step process for creating a digital signature?

Select one:

○ Create a message digest; encrypt the digest with the public key of the sender; and bundle the message, encrypted digest, and public key together to sign the document.

○ Create a message; encrypt the message with a MD5 hash; and send the bundle with a public key.

○ Create a SHA-1 hash; encrypt the hash with the private key of the sender; and bundle the message, encrypted hash, and public key together to signed document.

● Create a message digest; encrypt the digest with the private key of the sender; and bundle the message, encrypted digest, and public key together in order to sign the document. ✓

Refer to curriculum topic: 5.2.2
In order to create a digital signature, the following steps must be taken:

1. The message and message digest are created.
2. The digest and private key are encrypted.
3. The message, encrypted message digest, and public key are bundled to create the signed document.

The correct answer is: Create a message digest; encrypt the digest with the private key of the sender; and bundle the message, encrypted digest, and public key together in order to sign the document.

Question **16**

Correct

Mark 2.00 out of 2.00

Flag question

What is the standard for a public key infrastructure to manage digital certificates?

Select one:

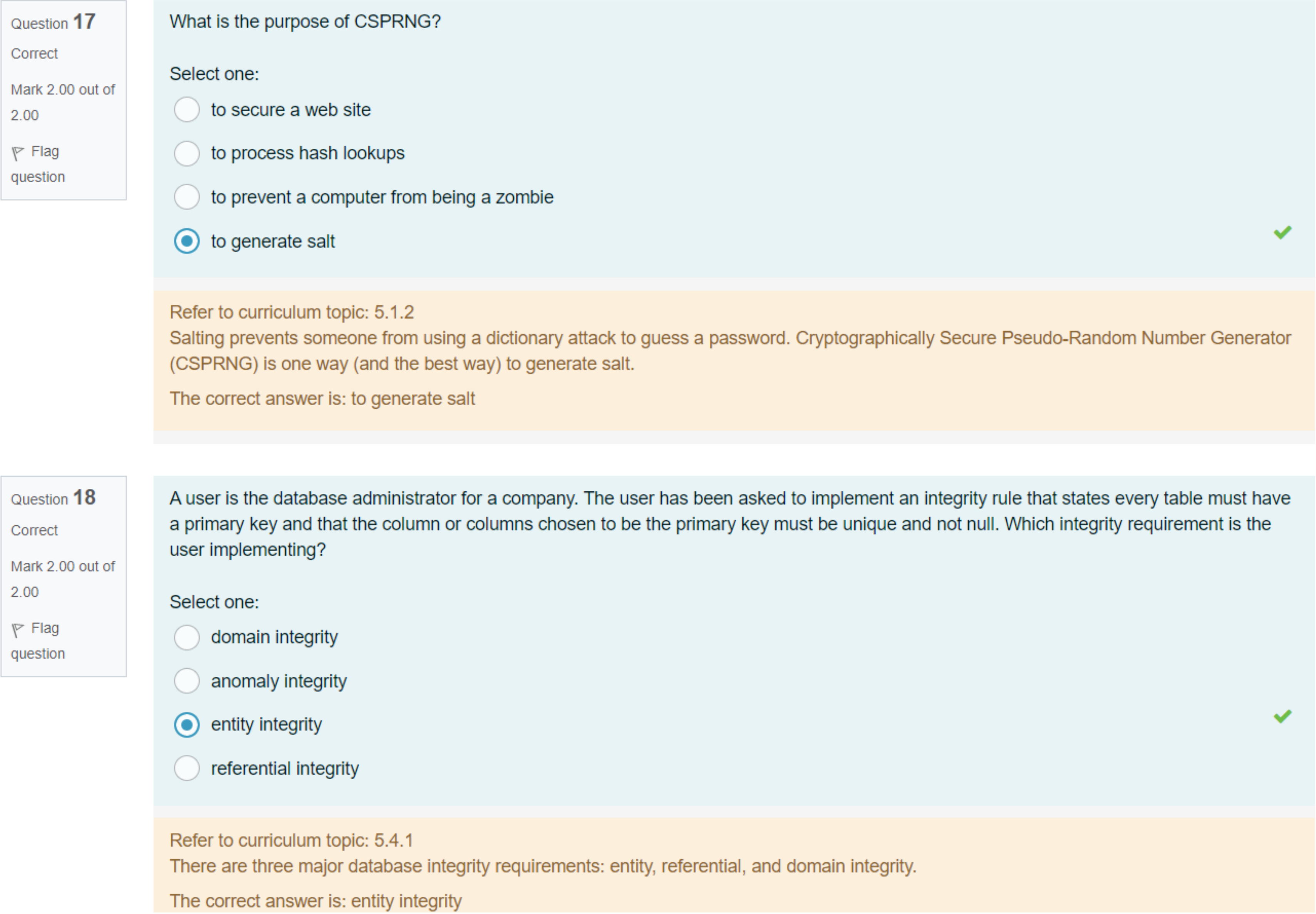
○ x.503

● x.509 ✓

○ NIST-SP800

○ PKI

Refer to curriculum topic: 5.3.2
The x.509 standard is for a PKI infrastructure and x.500 if for directory structures.



Question **17**

Correct

Mark 2.00 out of 2.00

Flag question

What is the purpose of CSPRNG?

Select one:

○ to secure a web site

○ to process hash lookups

○ to prevent a computer from being a zombie

● to generate salt ✓

Refer to curriculum topic: 5.1.2
Salting prevents someone from using a dictionary attack to guess a password. Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) is one way (and the best way) to generate salt.

The correct answer is: to generate salt

Question **18**

Correct

Mark 2.00 out of 2.00

Flag question

A user is the database administrator for a company. The user has been asked to implement an integrity rule that states every table must have a primary key and that the column or columns chosen to be the primary key must be unique and not null. Which integrity requirement is the user implementing?

Select one:

○ domain integrity

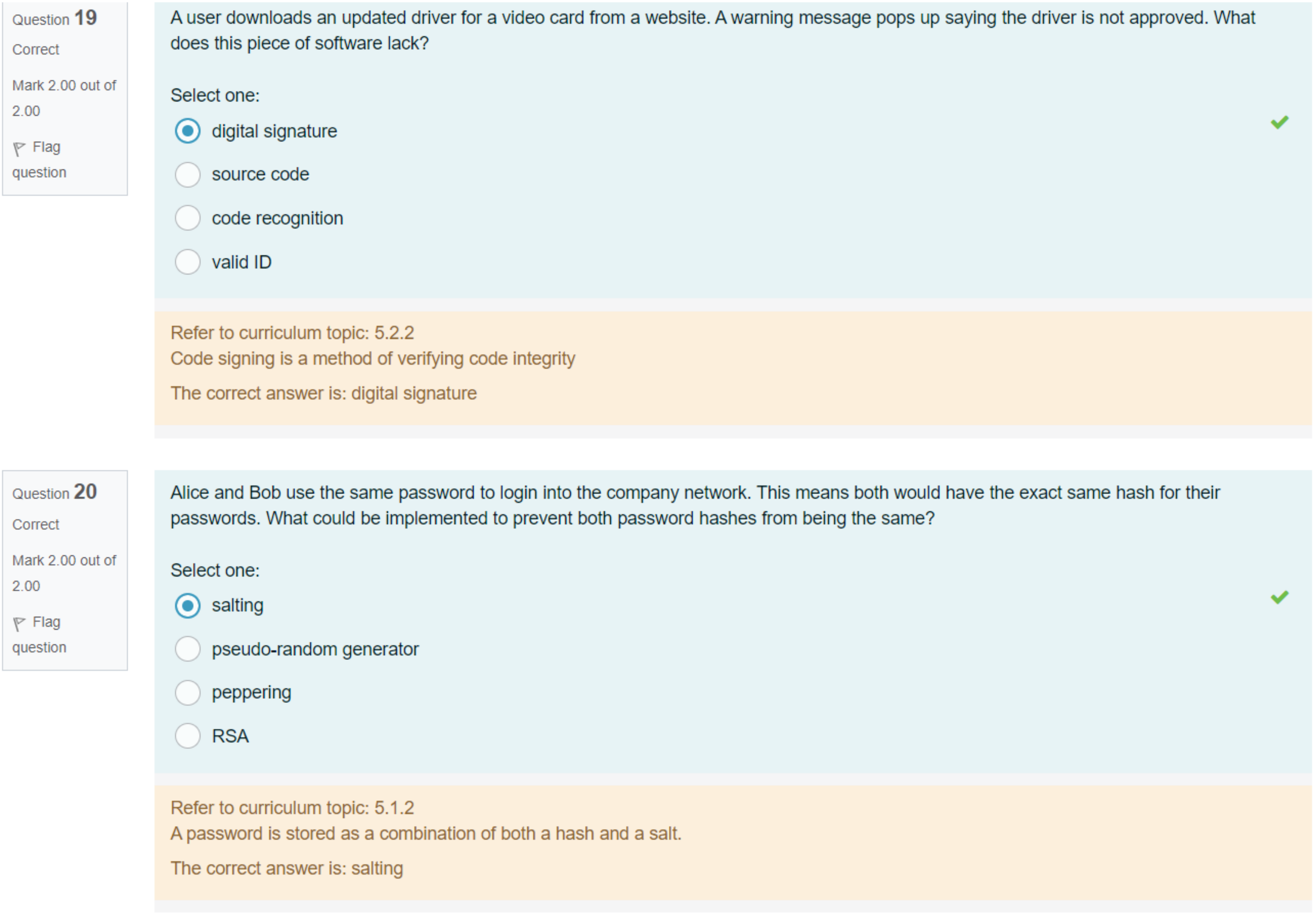
○ anomaly integrity

● entity integrity ✓

○ referential integrity

Refer to curriculum topic: 5.4.1
There are three major database integrity requirements: entity, referential, and domain integrity.

The correct answer is: entity integrity



Question **19**

Correct

Mark 2.00 out of 2.00

A user downloads an updated driver for a video card from a website. A warning message pops up saying the driver is not approved. What does this piece of software lack?

Select one:

- ● digital signature ✓
- ○ source code
- ○ code recognition
- ○ valid ID

Refer to curriculum topic: 5.2.2
Code signing is a method of verifying code integrity

The correct answer is: digital signature

Question **20**

Correct

Mark 2.00 out of 2.00

Alice and Bob use the same password to login into the company network. This means both would have the exact same hash for their passwords. What could be implemented to prevent both password hashes from being the same?

Select one:

- ● salting ✓
- ○ pseudo-random generator
- ○ peppering
- ○ RSA

Refer to curriculum topic: 5.1.2
A password is stored as a combination of both a hash and a salt.

The correct answer is: salting