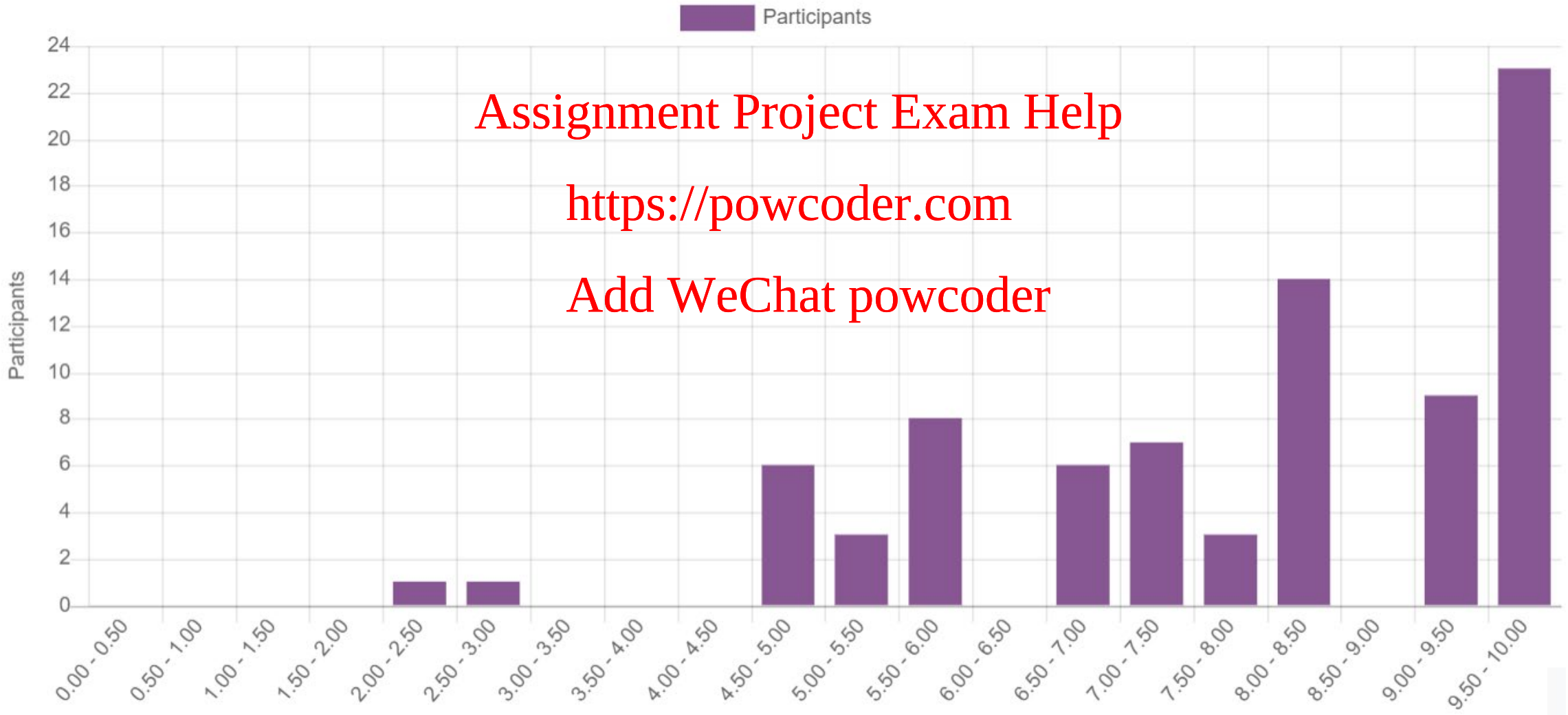
Quiz 8 - statistics

of participants: 81 / 100
average: 7.7 / 10



Alice has received Bob's digital certificate. The certificate is signed by a well-known Certificate Authority (CA). Which of the following statements, pertaining to Bob's certificate, are correct?

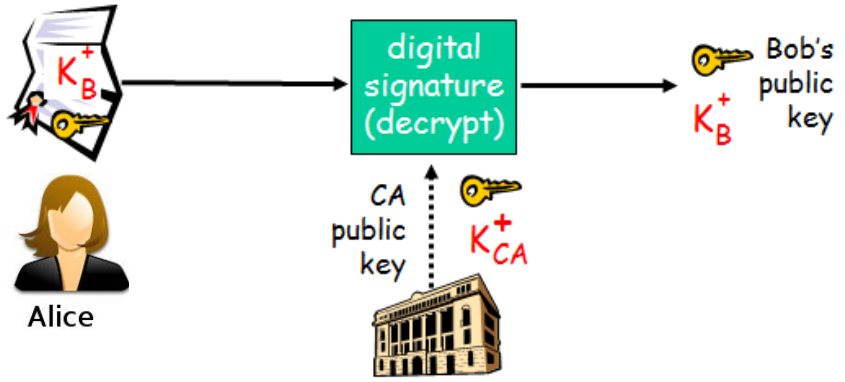
1) The certificate contains the CA's private key. To validate this certificate, Alice needs to use/apply Bob's public key.

2) The certificate contains Bob's private key. To validate this certificate, Alice needs to use/apply her own public key.

3) The certificate contains Bob's public key. To validate this certificate, Alice needs to use/apply CA's private key.

4) The certificate contains Bob's public key. To validate this certificate, Alice needs to use/apply CA's public key.

5) None of the above.



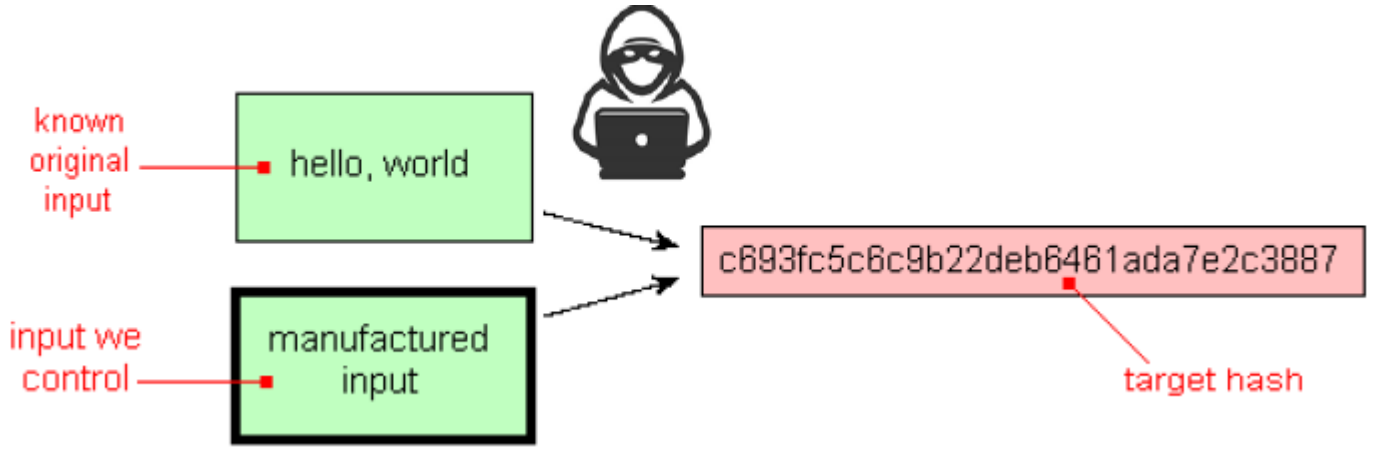
Bob and Alice have sent each other their respective Digital Certificates over an unprotected (i.e., public) network. Now, they would like to start exchanging confidential/encrypted messages using the AES algorithm. They have agreed that it will be Bob's responsibility to generate the AES key and send it to Alice.

Which of the following will ensure a safe transmission of the AES key from Bob to Alice?

1) Bob encrypts the AES key with his private key, and sends it to Alice. Anybody can decrypt it.
2) Bob encrypts the AES key with Alice's public key, and sends it to Alice.
3) Bob encrypts the AES key with his public key, and sends it to Alice. Alice cannot decrypt it.
4) Bob encrypts the AES key with Alice's private key, and sends it to Alice. Impossible - Bob does not have Alice's private key!!!

Which particular property of hash functions states that " it must be extremely difficult to find an alternative message with the same hash value as a given message".

1) strong collision resistance
2) preimage resistance
3) second preimage resistance
4) one-wayness



Multi-factor authentication is a form of access control in which the user/supplicant is required to provide two or more pieces of evidence (or factors) in order to be granted access to the system. Recall, four main authentication factors are: 'something the user knows', 'something the user has', 'something the user is' and 'something the user produces'.

Which of the following are not examples of multi-factor authentication access control?

1) access control based on type-in user-id and memorized password — something you know x 2
2) access control based on RFID-tag and finger-scan — s. you have & s. you are
3) access control based on magnetic swipe-card and memorized pin — s. you have & s. you know
4) access control based on finger-scan and memorized pin — s. you are & s. you know
5) all of the above are examples of multi-factor authentication