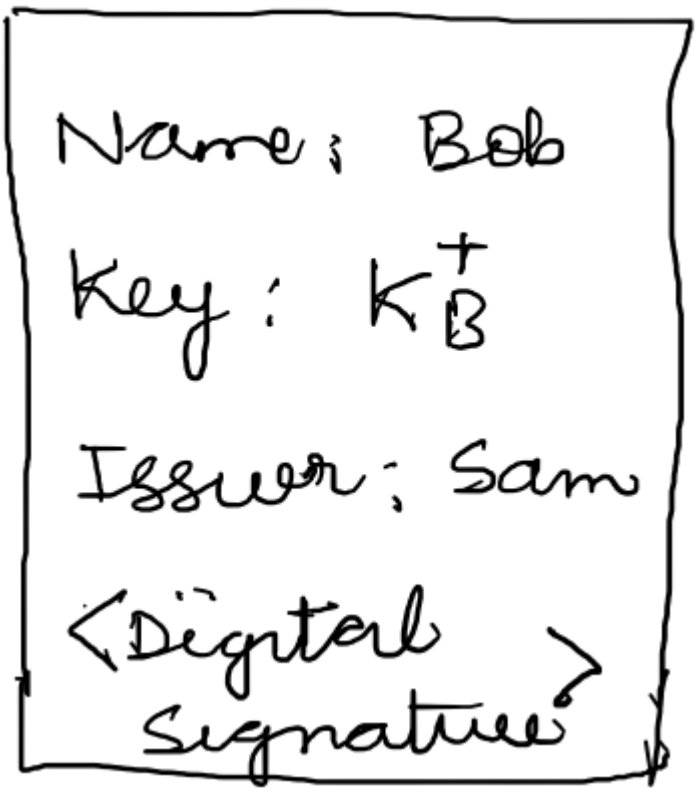
Started on	Wednesday, 6 November 2024, 9:01 AM
State	Finished
Completed on	Wednesday, 6 November 2024, 9:05 AM
Time taken	4 mins 23 secs
Grade	**10.00** out of 10.00 (**100**%)

Question 1

Correct

Mark 2.00 out of 2.00

Consider the following certificate presented by Bob to Alice issued by Sam. Which key will be used by Alice to check the authenticity of the certificate?



Info:
K_B^+ : Bob's public key
K_S^+ : Sam's public key
K_A^+ : Alice's public key

Select one or more:

- a. K^+_A
- b. K^+_B
- c. None of the above
- d. K^+_S ✓

Your answer is correct.

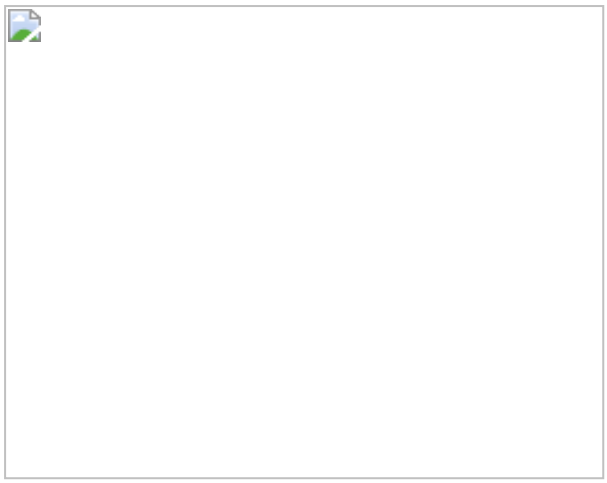
The correct answer is: K^+_S

Question 2

Correct

Mark 2.00 out of 2.00

Consider a 3-bit cipher block chaining scheme with the following cipher:



Consider m(1) = 001 and c(0) = 010. What is the encoding for m(1)?

Answer:

The correct answer is: 100

Comment:

Question 3

Correct

Mark 2.00 out of 2.00

Consider that Bob is using RSA and has advertised his public key to Alice. What is his private key?

$K_B^+ = (55, 3)$

Bob ——— Alice

Select one or more:

- a. (55, 31)
- b. (55, 27) ✓
- c. (55, 12)
- d. (55, 7)

Your answer is correct.

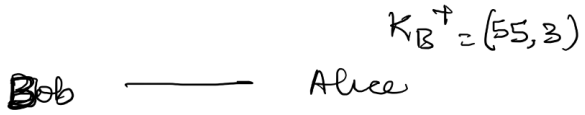
The correct answer is: (55, 27)

Question 4

Correct

Mark 2.00 out of 2.00

Consider the following scenario when Alice and Bob are using RSA. Alice has the public key of Bob as shown in figure. Suppose Alice wants to send 5 to Bob. What is the corresponding Ciphertext?



Answer: 15

The correct answer is: 15

Question 5

Correct

Mark 2.00 out of 2.00

Suppose there are four individuals Pam, Alice, Bob, and Sam and they each want to establish pairwise confidential channels with each other. How many keys/key pairs are required for these individuals to be able to communicate with each other using secret key and public key cryptography systems?

Select one or more:

- [x] a. 6 and 4
- [ ] b. 6 and 6
- [ ] c. 4 and 6
- [ ] d. 4 and 4

Your answer is correct.

The correct answer is: 6 and 4

◀ Quiz10

Jump to...

Quiz12 ▶