| | |
|---|---|
| **Started on** | Saturday, 21 October 2023, 8:41 PM |
| **State** | Finished |
| **Completed on** | Saturday, 21 October 2023, 8:42 PM |
| **Time taken** | 1 min 4 secs |
| **Marks** | 4.00/5.00 |
| **Grade** | **80.00** out of 100.00 |

## Question 1

Correct

Mark 1.00 out of 1.00

Kerckhoffs' Principle states that a cryptosystem should remain secure even if everything about it other than the key is public knowledge. The security of a system's design is in no way dependent upon the secrecy of the design, in and of itself.

Select one:

- True ✔
- False

The correct answer is 'True'.

## Question 2

Incorrect

Mark 0.00 out of 1.00

In the RSA system, the receiver does as follows:

1. Randomly select two large prime numbers p and q, which always must be kept secret.
2. Select an integer number E, known as the public exponent, such that (p 1) and E have no common divisors, and (q 1) and E have no common divisors.
3. Determine the private exponent, D, such that (ED 1) is exactly divisible by both (p 1) and (q 1). In other words, given E, we choose D such that the integer remainder when ED is divided by (p 1)(q 1) is 1.
4. Determine the product n = pq, known as public modulus.
5. Release publicly the public key, which is the pair of numbers n and E, K = (n, E). Keep secret the private key, K = (n, D).

The above events are mentioned in the correct order as they are performed while writing the algorithm.

Select one:

- True ✖
- False

The correct answer is 'False'.

## Question 3

Correct

Mark 1.00 out of 1.00

The term _____is often used to describe modifying the design and/or implementation of a software module without changing its external behavior, and is sometimes informally referred to as “cleaning it up.”

Select one:

- a. Designing
- b. Factoring
- c. Refactoring ✔
- d. Polymorphism

The correct answer is: Refactoring

## Question 4

Correct

Mark 1.00 out of 1.00

If you are able to anticipate that the components are likely to be reused in future projects then it is not advisable to use the Pub-Sub design pattern.

Select one:

- True
- False ✔

The correct answer is 'False'.

## Question 5

Correct

Mark 1.00 out of 1.00

Indirect communication is usually used when an object cannot or does not want to know the identity of the object whose method it calls.

Select one:

- True ✔
- False

The correct answer is 'True'.