Cryptography

shikhar18099@iiitd.ac.in Switch account

Draft saved

Your email will be recorded when you submit this form

A traditional computational bit can take either a 0 or a 1 value. How many values can one quantum bit (qubit) take? 1 point

- (●) 2^64
- ( ) 512
- ( ) 2
- ( ) 8

Clear selection

If we call Euclid's GCD, EuclidGCD(a, b), algorithm, what will be the value of a and b in 4th recursive call when EuclidGCD(824, 520) is called? Here 4th recursive call refers to the 4th function call after the function is called with initial inputs (No further hints or clarifications will be given on this). 2 points

- ○ 216,88
- ○ 88,40
- ○ 40,8
- ○ 95,36

When a user needs to provide message integrity, what options may be best? 1 point

- ○ Send a digital signature of the message to the recipient.
- ○ Encrypt the message with a symmetric algorithm and send it.
- ○ Encrypt the message with a private key so the recipient can decrypt with the corresponding public key.
- ◉ Create a checksum, append it to the message, encrypt the message, then send to recipient.

Clear selection

What is a trial-and-error method used to decode encrypted data through exhaustive effort rather than employing intellectual strategies? 1 point

- ◉ Brute-force cracking
- ○ Cryptanalysis

Clear selection

Rivest-Shamir-Adleman, or RSA, is an algorithm used for symmetric key cryptography. 1 point

- ○ True
- ◉ False

Clear selection

What is a disadvantage of using a public key algorithm compared to a symmetric algorithm? 1 point

- ○ A symmetric algorithm provides better access control.
- ○ A symmetric algorithm provides nonrepudiation of delivery.
- ○ A symmetric algorithm is more difficult to implement.
- ◉ A symmetric algorithm is a faster process.

Clear selection

How long would a 10-bit message be after being encrypted by a stream cipher? 1 point

- ○ 2 bits
- ○ 5 bits
- ○ 20 bits
- ◉ 10 bits

Clear selection

What is the name of the encryption/decryption key known only to the party or parties that exchange secret messages? 1 point

- ○ E-signature
- ○ Digital certificate
- ◉ Private key
- ○ Security token

Clear selection

What is the Diffie-Hellman key exchange vulnerable to? 1 point

- ○ Snooping
- ◉ Man-in-the-middle attacks
- ○ Phishing attacks
- ○ Denial-of-service attacks

Clear selection

A copy of your responses will be emailed to shikhar18099@iiitd.ac.in.

Submit Page 1 of 1 Clear form