TYCS NS UT1 2021-2022

Your email will be recorded when you submit this form

Not **jagrut.g@somaiya.edu**? Switch account

* Required

"defend the east wall" convert this into cipher text using rail fence technique(No. of rows 2)

○ DFNTEATALEDEHESWL

○ DFNTTEAALEEDHESWL

○ DFNTEATALEEDHESLW

● DFNTEATALEEDHESWL

Clear selection

Which is not an objective of network security?

○ Identification

○ Authentication

○ Access control

● Lock

Clear selection

__________ is a mathematical process that produces a ciphertext for any given plaintext and encryption key.

● Encryption Algorithm

○ Decryption Algorithm

○ Cryptography

○ Cryptology

Clear selection

The principle of ________ states that resources should be available to authorized parties at all times.

○ Authentication

○ Confidentiality

● Availability

○ Access Control

Clear selection

INCLUDE HELP IS AWESOME convert into cipher text using columnar transposition technique. Sequence is 4, 1, 3, 2

○ LHIEIEUESSCEPWMNDLAO

○ LHIEEIUESSCEPMNWDLAO

○ LHIEEIUESSCEPWMNDLOA

● LHIEEIUESSCEPWMNDLAO

Clear selection

A ________ attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification

○ replay

● masquerade

○ denial of service

○ None of the above

Clear selection

_________ is possible in absence of proper authentication mechanisms

○ Modification.

● Fabrication

○ Non-repudiation

○ None of the above

Clear selection

_____attacks generally make an attempt to either slow down or completely bring to halt, a computer network.

○ Active

○ Passive

● Network level

○ Application level

Clear selection

Security features that control what can access resources in the OS.

○ Authentication

○ Identification

○ Validation

● Access control

Clear selection

In Playfair Cipher, a plaintext message is split into pairs of how many letters?

○ 3

○ 1

○ 5

● 2

Clear selection

Convert plain text message "come home tomorrow" into cipher text using simple columnar transposition technique. Column order is 4,6,1,2,5,3

○ eowoocmoerrhmmto

○ eowocomroerhmmto

○ eowoocmroerhmtmo

● eowoocmroerhmmto

Clear selection

______ attacks do not involve some modification of the data stream or the creation of a false stream .

○ Active

● Passive

○ Network level

○ Application level

Clear selection

Obtaining credit card information on internet or changing the content of message is _______ type of attack

○ Physical level

○ Network level

● Application level

○ None of the above

Clear selection

Student Name *

Jagrut G Gala

In which technique, each letter of the plaintext is substituted by another letter which is ‘shifted’ by some fixed number between 0 and 25 to form the ciphertext?

○ Hill Cipher

○ Rail Fence cipher

○ Playfair

● Shift Cipher

Clear selection

In Playfair Cipher, if both the letters are in the same column, then in the encryption process which letter we used to take?

○ the letter above each one

● the letter below each one

○ right side letter

○ left side letter

Clear selection

The ________ cipher works by writing your message on alternate lines across the page, and then reading off each line in turn.

○ Shift Cipher

○ mono-alphabetic

● Rail Fence

○ Hill

Clear selection

In which cryptography message is encrypted using receipients public key and decrypted using receipients private key?

○ Symmetric cryptoghraphy

● Public key cryptoghraphy

○ Private key cryptoghraphy

Clear selection

The encryption process where different keys are used for encrypting and decrypting the information is known as __________ Key Encryption.

○ Both symmetric and asymmetric

● Asymmetric

○ Symmetric

Clear selection

______ is the field of both cryptography and cryptanalysis.

○ Cryptanalysis

○ Cryptography

● Cryptology

○ Key

Clear selection

In RSA, CT=

○ P+^e mod n

● PT^e mod n

○ PT-e mod n

○ PT^n mod e

Clear selection

Recovering plaintext from ciphertext is called

● Decipher

○ Encipher

○ Plaintext

○ Ciphertext

Clear selection

The principle of __________ specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.

● Confidentiality

○ Authentication

○ Integrity

○ Non-Repudiation

Clear selection

In RSA, n=

● p*q

○ p+q

○ p-q

○ p/q

Clear selection

It is a _______ cipher wherein each letter of the plaintext is substituted by another letter to form the ciphertext.

● mono-alphabetic

○ Shift Cipher

○ Playfair Cipher

○ Hill

Clear selection

Roll No *

2109805

Email id *

jagrut.g@somaiya.edu

In Diffie hellman key exchange algorithm, if n and g are two prime numbers and Alice chooses another large random number x, then calculates A such that

○ A=g-x mod n

○ A=g+x mod n

○ A=g^n mod x

● A=g^x mod n

Clear selection

Submit

Never submit passwords through Google Forms.