*ssl connection vs ssl session
*types of malicious software
*attacks that is prevented by message authentication
*phases of virus
*draw Des round in detail

أعجبني · رد · عرض الترجمة · 1 أ

Nourhan Gamal
-Hash function requirements.
-Block vs stream
-Stenography vs encryption
-authentication requirements

أعجبني · رد · عرض الترجمة · 1 أ · تم التعديل

Nourhan Gamal
-ssl stack
-ssl handshake, alert, cipher change usage

أعجبني · رد · عرض الترجمة · 1 أ

- Draw ssl protocol stack
- ssl Security record and its security services
- provide function for each of:
1- ssl alert
2- ssl handshake
3- ssl cipher change

Nour Nasser
Compare:
Stream, block cipher
Diffusion, confusion
Steganography, encryption
Active, passive attacks
Monoalphabetic, polyalphabetic
ناقص واحدة بس هنا
Ssl connection and smth else

Sarah Mohamed
SSL and TLS

Ahmed Essam Eldeen
ssl connection and ssl session

Nour Nasser
In certificate authority:
A. List 4 assumptions
B. Draw

Mohamed Mokhtar
Draw des

Abdelrahman Mohamed
Mohamed Mokhtar single phase

Mohamed Mokhtar
Ssl services

Mohamed Mokhtar
Description one sentence

Sarah Mohamed
Write types of malicious software and their description
Draw SSL architecture
Draw one round of DES
Write operations of SSL record protocol
Write hash function requirements and their description

Sarah Mohamed
Draw certificate authority
Describe at least 3 attacks

Sarah Mohamed
Use Vigenere to encrypt word "exploration" by key Concept

Mohamed Mokhtar
Compare between ssl session and ssl connection in two questions

Abdelrahman Mohamed
Mention virus states and describe each one (4 states)

Nour Nasser
True and false
1. Alice is sending a message to bob using asymmetric encryption. She will encrypt using Alice's public key.
2. In asymmetric encryption both encryption and decryption use the same key
3.ceaser cipher is considered polyalphabetic cipher

Mohamed Mokhtar
Definition in one term
One way function
Authorization

Which of following are Reducible in gf(2)?
X3+x2+1
X3+x+1
None
All of the above

If a plain text is successfully hashed, then its confidentiality is ensured?
True false

Certificate authority verify/authenticate
Hash function
Public key
Shared key in session key
Digital signature

Abdulrahman El Shafei
MCQ: p and q for RSA are ...
a. coprime
b. primes
c. all of the above
d. none of the above
True or false: Block ciphers encryption modes used in stream ciphers

Mostafa Elshaer
Mention 5 malicious softwares (name / description)

مسؤول Yosry Muhammad ElGamal
Certificate authority diagram

مسؤول Yosry Muhammad ElGamal
Encrypt "exploration" using Vigenère Cipher with key "concept"

Ahmed Essam Eldeen
T/F
in symmetric key encryption we use public channel for key exchange

mcq
1) which is false about ECB
- used in short data
- encryption can be executed in parallel
- blocks can be repeated or swapped without being noticed by the receiver
- non of the above

Which mode permits the block cipher encryption function to be called before the data is available