COVID – 19 (ONLINE EXAMINATION)

DSVV

देव संस्कृति विश्वविद्यालय

शान्तिकुन्ज, हरिद्वार

आन्तरिक मूल्यांकन परीक्षा – INTERNAL EVALUATION TEST

उत्तर-पुस्तिका

परीक्षार्थी अनुक्रमांक (अंकों में) Student's Roll No. (in numbers) 1824006

पेपर कोड Paper code .....

परीक्षार्थी अनुक्रमांक (शब्दों में) Student's Roll No. (in words) Aniket Kumar

नामांकन संख्या Enrollment Number 18000012G

कक्षा Class BCA (VI Sem.)

विषय Subject Cryptography

दिनाँक Date 26-03-2021

दिन Day Friday

प्रश्न पत्र संख्या Examination Paper Number .....

लघुत्तरीय A) Short Answer Type		योग/Total
1	2	
दीर्घ उत्तरीय B) Long Answer Type		
1		
कुल योग अंकों में / TOTAL IN DIGITS		
कुल योग शब्दों में/TOTAL IN WORDS		

Aniket

परीक्षार्थी के हस्ताक्षर
Signature of student's

परीक्षक के हस्ताक्षर
Signature of Examiner

Short Answer

Ans 1 Limitations of modern Crypto Systems

- Key exchange - This ensures that the encryption key will have to be shared through a protected channel.
- The number of keys needed - A new key is required for each pair of participants wishing to exchange encrypted messages.
- In Assymmetric Cryptography, we can't encrypt large messages as the encryption/decryption throughput is inversely proportional to the duration of the key.
- Public keys are not authenticated - Basically, no one absolutely knows that a public key belongs to the individual it specifies, which means that users will have to verify that their public keys truly belong to them.
- It risks loss of Private key, which may be irreparable - when we lose our Private key, our recieved message will not be decrypted.
- They also have vulnerabilities to attacks such as man in the middle attack.

Ans 2. we can say a crypto system is "Perfectly Secure", when in a communication, the attacker - Should not get any advantage by seeing communication
- Attacker learns underlying key only with Probability 1/2
- It should not be better than guessing the key.

Perfect Secrecy.

- The notion of Perfect Security is also called as unconditional security.
- The attack model considered in the definition of Perfect Security is ciphertext only attack.
- It is assumed that the attacker is computationally unbounded.
- Informal definition -
  - "irrespective of any prior info", The attack has about m, the cipher-text c should not leak 'no additional information' about the Plain text.
- In simple words, Perfect secrecy means that the ciphertext conveys no information about the content of the Plaintext.
- In Practice, it means that no amount of computation applied to the ciphertext will give you any advantage in knowing anything about the Plaintext or Key.

—

Long Answer

Ans 1 OSI Security Architecture.

- It is a systematic approach, defined by ITU-T (The International Telecommunication Union - Telecommunication ~~Union~~ Standardization Sector), which is a United Nations sponsored agency.
- Security architecture for OSI offers a systematic way of defining security requirements and characterizing the approaches to achieve these requirements. It was developed as an International Standard.

Need for OSI Security Architecture

- To assess the security needs of an organization effectively and choose various Security Products and Policies.
- The need for some systematic way of defining the requirements for security and characterizing the approaches to satisfy those requirements.

Benefits.

- The OSI security architecture is useful to managers as way of organization the task of providing security.
- Computer and communications vendors have developed security feature for their products and services that relate to this structured definition of services and mechanisms.

focus of osi security architecture

Security Attack.
- Security attack is a process of gaining an access of data by unauthorized user.
  - Accessing the data
  - Modifying the data
  - Destroying the data
- It can be Passive or Active.

Security Mechanism
- A process that is designed to detect, prevent or recover from a security attack.
- It is a method which is used to protect your message from unauthorized entity.
- mechanisms - Encipherment, Digital Signature, Traffic Padding, Notorization.

Security Services.
- Security services is the services to implement security policies and implemented by security mechanism.
- The security services are - Confidentiality, Authentication, Integrity, Non-refudiation, Access Control and availability.

Services

Confidentiality - Ensures that the information in a Computer System and transmitted information are accessible only for reading by authorized Parties.

Authentication - Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity - ensures that only authorized Parties are able to modify Computer System assets and transmitted information.

Non-reputation - requires that neither the sender nor the reciever of a message be able to deny the transmission.

Access Control - requires that access to information resources may be controlled by or for the target system.

Availability - requires that Computer System assets be available to authorized Parties when needed.