COVID – 19 (ONLINE EXAMINATION)

DSVV

ICMR Registration number: COREG001
SRF ID: 050500032797S

देव संस्कृति विश्वविद्यालय

शान्तिकुन्ज, हरिद्वार

आन्तरिक मूल्यांकन परीक्षा – INTERNAL EVALUATION TEST

उत्तर–पुस्तिका

परीक्षार्थी अनुक्रमांक (अंकों में) Student's Roll No. (in numbers) 1824014

पेपर कोड Paper code .....

परीक्षार्थी अनुक्रमांक (शब्दों में) Student's Roll No. (in words) Pranav Mishra

नामांकन संख्या Enrollment Number 18000000137

कक्षा Class BCA 6th 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		

Pranav

परीक्षार्थी के हस्ताक्षर
Signature of student's

परीक्षक के हस्ताक्षर
Signature of Examiner

Short Answer :-

1:- Modern Crypto System :-

It is important to understand the state of modern cryptography and how quantum cryptography may address current digital cryptography limitations. However, because asymmetric encryption is significantly slower than symmetric encryption, a hybrid approach is preferred by many institution to take advantage of the speed of a shared key system and the security of a public key system for the initial exchange of the symmetric key. Thus, this approach exploits the speed and performance of a symetric key system while leveraging the scalability of a public key infrastructure. Uncertainty provides potential risk to areas of national security and intellectual property which require perfect security. Modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one way functions such as that of factoring large integers. If a factoring theorm were publicized or computing became powerful enough to defeat public cryptography, then business, governments, ~~mitli~~ militaries and other affected institutions would have to spend significant resources to reach the risk of damage and potentially depoly a new and costly cryptography system quickly.

Ans:-2:-

→ We will say crypto System have "perfect secure" when the definition of perfect security is ciphertext-only attack.

→ The notion of perfect security is also called as unconditional security, information-theoretic security.

→ 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

Formal definition:-

→ An encryption scheme (GEN, ENC, DEC) over a plaintext space M is perfectly-secure if for every probability distribution over M and K every plaintext $m \in M$ and every ciphertext $c \in C$.

- $Pr[M = m \mid C = c] = Pr[M = m]$

Alternate Definition:-

Original Definition:- Probability of knowing a plain-text remains the same before and after seeing the cipher text

$$Pr[M = m \mid C = c] = Pr[M = m]$$

Alternate Definition:- For every probability definition, over M and K, every plain-text $m_0, m_1 \in M$ and every cipher text $c \in C$

$$Pr[C = c \mid M = m_0] = Pr[C = c \mid M = m_1]$$

Properties:-

- $\Pi = (GEN, ENC, DEC)$, A public known cipher.
- For the attacker, Π induces a probability distribution on M, K and C
  - M : Plaintext space
  - K : Key space
  - C : Ciphertext space

When we will sets all the definition of ciphertext only attack then we will says this system is perfectly secure.

Long Answer :-

3:- OSI Security Architecture :-

→ Security architecture for OSI offers a systematic way of defining security requirements and characterizing the approaches to achieve those requirements.

→ The OSI security architecture was developed in the context of the OSI protocol architecture.

→ The OSI security architecture provides a useful, if abstract, overview of many of the concepts. The OSI security architecture focuses on security attacks, mechanisms, and services.

Needs 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.

The OSI security Architecture :-

→ Such a systematic approach is defined by ITU-T (The international Telecommunication Union - Telecommunication Standardization Sector)

→ It is a United Nation (UN) sponsored agency that develops standards, called recommendations, relating to telecommunication and to open System Interconnection (OSI) recommendations X.800, security Architecture for OSI.

Benefits of OSI Security Architecture:-

→ The OSI security architecture is useful to managers as way of organization the task of providing security.

→ This architecture was developed as international standards, computer and communications vendors have developed security feature for their products and services that relate to this structured definition of services and mechanisms.

OSI Security Architecture Focus:-

- **Security Attack:-** Any action that compromis the security of information owned by an organization.

  Security Attack is a process of gaining an ~~pro~~ access of data by unauthorized user
  - Accessing the Data
  - Modifying the Data
  - Destroying the Data

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

- Security Services:-
- Security Services is the services to implement security policies and implemented by security mechanism.
  - Confidentially
  - Authentication
  - Integrity
  - Non-supudation
  - Access control
- Availability