|  |  |  |  |
| --- | --- | --- | --- |
| **Continuous Comprehensive Evaluation TEST – III** | | | |
| **Course :** | **Cryptography and Network Security** | **Academic Year :** | **2024 –2025** |
| **Course Code :** | **BCICR515** | **Date :** | **12/12/2024** |
| **Sem / Branch :** | **V (A and B section)** | **Max. Marks :** | **15** |
| **Department :** | **AIML** | **Duration :** | **1 Hour** |
| **Faculty** | **Prof. Revathy BD** | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| USN: |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***INSTRUCTION TO STUDENTS:* Answer ONE FULL question** | | | | | | |
| **MODULE – V** | | | | | | |
| **Q. No.** | |  | **Marks** | **BL** | **CO** | **PO** |
| **1.** | **a)** | Describe the application and benefits of IPsec. | **7** | **L2** | **CO1** | **PO1** |
|  | **b)** | Consider the given data    Apply the concept of PGP transmission and reception messages for achieving authentication. | **8** | **L3** | **CO2** | **PO1** |

|  |  |
| --- | --- |
| **Course Outcomes (CO)** | |
| CO1 | Understand the need of security and various encryption techniques |
| CO2 | Apply the use of public key crypto system to authenticate the messages. |
| CO3 | Analyse the digital signature standards and IP security policies. |
| CO4 | Demonstrate the various Security Algorithms for a given problem in a team. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Course Instructor** | **Course Coordinator** | **PAC Committee** | **Head of the Department** |
| **Name:** | Prof. Revathy BD | Dr. Chethan B K | Prof. Latha D U | Dr. Aditya C R |
| **Signature:** |  |  |  |  |

**Verified By: -**

**Scheme of valuation**

**1 a). Describe the application and benefits of IPsec. 7M**

**Ans:**

Applications of IPsec

IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

•                 Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

•                 Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider(ISP) and gain secure access to a company network. This reduces the cost of tollcharges for traveling employees and telecommuters.

•                 Establishing extranet and intranet connectivity with partners: IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange   mechanism.

•                 Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

**Benefits of IPsec :**

•                 When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

•                 IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

•                 IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

•                 IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

•                 IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

**(b). Apply the concept of PGP transmission and reception messages for achieving authentication -8M**

**Ans:**

* + When PGP is used, at least part of the block to be transmitted is encrypted.
  + If only the signature service is used, then the message digest is encrypted (with the senders private key) .
  + If the confidentiality service is used, the message plus signatyre(if present) are encrypted.
  + Thus, part or all of the resulting block consists of a stream of arbitrary 8-bit octets.
  + However, many electronic mail systems only permit the use of blocks consisting of ASCII text.
  + To accommodate this restriction, PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters.
  + The scheme used for this purpose is radix-64 conversion.
  + Each group of three octets of binary data is mapped into four ASCII characters.
  + This format also appends a CRC to detect transmission errors.
  + The use of radix 64 expands a message by 33%.
  + One noteworthy aspect of the radix-64 algorithm is that it blindly converts the input stream to radix-64 format regardless of content, even if the input happens to be ASCII text.
* On transmission (if it is required), a signature is generated using a hash code of the uncompressed plaintext. Then the plaintext (plus signature if present) is com- pressed.
* Next, if confidentiality is required, the block (compressed plaintext or com- pressed signature plus plaintext) is [encrypted](https://www.brainkart.com/article/Pretty-Good-Privacy_8491/) and prepended with the public-key- encrypted symmetric encryption key.
* Finally, the entire block is converted to radix-64 format.
* On reception, the incoming block is first converted back from radix-64 format to binary.
* Then, if the message is encrypted, the recipient recovers the session key and decrypts the message.
* The resulting block is then decompressed.
* If the message is signed, the recipient recovers the transmitted hash code and compares it to its own calculation of the hash code.

A diagram of a flowchart

Description automatically generated