Register Number:……..

KUMARAGURU college of technology
character is life

**B.E DEGREE EXAMINATIONS: NOV /DEC 2024**

(Regulation 2018)

Sixth Semester

**INFORMATION SCIENCE AND ENGINEERING**

U18IST6002: Cryptography and Network Security

**COURSE OUTCOMES**

**CO1:** Analyze various security attacks and select appropriate security mechanisms for designing various security services

**CO2:** Understand the mathematical foundations of cryptography

**CO3:** Trace the design of modern block ciphers from basic building blocks

**CO4:** Appreciate how one-way function and other mathematical hard problems are used to construct solutions for message integrity and authentication

**CO5:** Discover how cryptographic algorithms are used to build network security protocols

**CO6:** Identify appropriate mechanisms for providing system security

**Time: Three Hours** **Maximum Marks: 100**

**Answer all the Questions: -**

**PART A (10 x 2 = 20 Marks)**

**(Answer not more than 40 words)**

| | | | |
|---|---|---|---|
| 1. | How many possible keys have to be tried to break a number lock with three rotors and 0 to 9 in each rotor. Analyze its complexity to brute force attack. | CO1 | [$K_4$] |
| 2. | Analyze the connection between hard problems and cryptography. | CO2 | [$K_4$] |
| 3. | What is a product cipher? What are the two techniques which are used in combination to construct a product cipher? | CO3 | [$K_2$] |
| 4. | What is a birthday attack on hash functions? How is it related to Collision. | CO4 | [$K_2$] |
| 5. | By what modification does a http protocol become https protocol? | CO5 | [$K_3$] |
| 6. | What is Cipher Block Chaining mode of block ciphers? | CO3 | [$K_2$] |
| 7. | Analyze the difference between HMAC and SHA. | CO4 | [$K_4$] |
| 8. | Name two security services provided by Digital Signature. | CO4 | [$K_2$] |
| 9. | Differentiate between a virus and worm. | CO6 | [$K_2$] |
| 10. | Can Firewalls defend against attacks from insiders? Which system security mechanism is needed to handle insider attacks. | CO6 | [$K_4$] |

**Answer any FIVE Questions:-**
**PART B (5 x 16 = 80 Marks)**
**(Answer not more than 400 words)**

11. a) The following table has been randomly mapped between Security Attacks, Services and Security Algorithm. Order them properly so that it shows for each of the security attacks, what is the security service to be provided using which security algorithm: 8 CO1 [$K_3$]

| **Security Attacks** | **Security Services** | **Security Algorithms** |
|---|---|---|
| Interception | Confidentiality | SHA |
| Fabrication | Integrity | RAID (for Redundancy) |
| Modification | Availability | AES |
| Interruption | Authentication | HMAC |

b) It is suspected that the following cipher text has been encrypted using the classical Caesar Cipher with some shift from 1 to 25. Find the corresponding Plain Text, given that the Cipher Text is: PRYH QHAW 8 CO1 [$K_4$]

12. a) How will you find the private key (d) from the public key (e), if you know the factors p, q of n, which is used in the RSA Cryptosystem? Assume that e and d are multiplicative inverses modulo φ(n), where φ(n) = (p-1)(q-1) is the Euler's Totient Function for n. Explain the process of calculating d from e, p, and q. 8 CO2 [$K_3$]

b) Given that algorithms like Shor's can factorize large numbers on quantum machines, analyze the impact on public key algorithms such as RSA, when quantum computers capable of these are physically made available. 8 CO2 [$K_4$]

13. a) There are three parameters available to the attacker or cryptanalyst in the context of Cryptanalysis. Plain Text, Cipher Text, and Key. In terms of these three explain what diffusion and confusion is according to Claude Shannon. 8 CO3 [$K_2$]

b) Explain the following with reference to AES: 8 CO3 [$K_2$]

i. Substitute Bytes
ii. Shift Rows
iii. Mix Columns

iv. Add Round Key

| | | | | | |
|---|---|---|---|---|---|
| 14. | a) | Explain the weak and strong collision resistant properties of Hashing Functions | 8 | CO4 | [$K_2$] |
| | b) | Explain HMAC with a block diagram | 8 | CO4 | [$K_2$] |
| 15. | a) | Suppose you are the organizer of Yugam 2025, and all event certificates have to be issued as (cryptographically) digitally signed certificates. You have obtained a private and public key for our institutions from a registered Certificate Authority. Hence the public key of the institution will be available to all adobe readers across the world from the repository. Given a .pdf of the certificate to a participant, explain the key steps of generating the digital signature for the same, so that it is digitally verifiable to anyone who opens the digitally signed certificate. | 12 | CO5 | [$K_6$] |
| | b) | Explain IPSec Encapsulation Security Payload Protocol | 4 | CO5 | [$K_2$] |
| 16. | a) | Explain the statistical anomaly-based approach to Intrusion Detection. | 8 | CO6 | [$K_2$] |
| | b) | Differentiate between packet filtering and application-level gateway (proxy) firewalls. | 8 | CO6 | [$K_2$] |

**********