Department of Computer Science and Engineering, S V N I T, Surat
MID-SEMESTER EXAMINATIONS, March 2023
B. Tech. – IV (CSE) – 9ᵗʰ Semester
Course: (CS424) Core Elective V (Network and Systems Security)

&xp.
[20/30]

Date: 6ᵗʰ March, 2023   Time: 14:00 to 15:30   Max Marks: 30

(9.5)

Q.1   Answer the following: **[10]**

(a)   Apply Euclid's algorithm to calculate GCD of 42823 and 6409.   3
(b)   Demonstrate the use of Bloom Filter for proactive password checking.   3
(c)   Describe various access control structures with suitable examples.   2
(d)   Discuss Public Key Requirements with Digital Envelopes.   2

Q.2(a)   Compare and contrast S/MIME with SMTP. (Explain the S/MIME process to send signed and   (9)   **[4]**
              enveloped data to the receiver.)

Q.2(b)   Answer the following (Any Two):   **[6]**

(i)   What is the role of Change Cipher Protocol in TLS/SSL handshaking process? Explain the TLS/SSL
       protocol used to notify the closure of TCP connection.
(ii)   Explain IPsec mode used to create VPN between company network and an employee working
       remotely.
(iii) Explain any one attack used to trick a web server for accepting connections with the older version
       of TLS/SSL protocol.

Q. 3   Answer the following: **[10]** (9.5)

(a)   Which kinds of operations are most likely to lead to buffer overflows in C? Give examples.   2 (1)
(b)   Define input fuzzing. State where this technique should be used.   3 (2)
(c)   State the similarities and differences between command injection and SQL injection attacks.   2 (1)

OR

       Explain the difference between an attack surface and an attack tree. ✗
(d)   Describe how a global data area overflow attack is implemented.   3 (1)