BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

NETWORK SECURITY (CS G513)
SECOND SEMESTER 2022-23 MID-SEMESTER EXAMINATION
(CLOSED BOOK)

Maximum Marks: 25
Time: 90 minutes

Instructions:

1. Answer all parts of a question together in the answer sheet. Answers at separate places will not be accepted.
2. Do not write any information irrelevant to the question.

Q.1. Answer the following: [3 × 2 = 6 M]

a. What is avalanche effect in DES? Briefly describe its types with suitable examples.

b. Given the keyword as "MONDAY", what should be the third letter of the second row in the 5×5 Playfair matrix (consider that the row and column numbering start from 1)? Also, what should be the key domain if a successful Brute-force attack is to be performed on the encrypted text generated using the devised matrix?

Q.2. Consider a new prime polynomial for AES algorithm as $x^7 + x^5 + x^2 + x + 1$. What should be the effect of this modification on the Round Constant (RC) computation? Provide the RC word for the ninth round by considering new polynomial. [4 M]

Q.3. Answer the following: [3 × 2 = 6 M]

a. Given that the set G forms a group under the binary operation *, defined as a * b = a + b + 5; a, b ε G. Find the inverse of -12 in G.

b. Considering extended Euclidean algorithm, find the greatest common divisor, *gcd(a,b)*, and values of s and t for the below cases.

Case I: When $a = 17$ and $b = 0$
Case II: When $a = 0$ and $b = 45$

Q.4. What is broadcast attack in RSA? Given a secret value S as 150 and four different modulus $m_1 = 5,\ m_2 = 17, m_3 = 19$, and $m_4 = 29$, show (in clear and detailed step-wise manner) how this attack can be performed. [5 M]

Q.5. Given an efficient function ensemble (a function that is computable in polynomial time) $g: \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$, with $l(n)$ being a polynomial with $l(n) > n$. If for all adversaries A running in polynomial time, the success probability (prediction probability) of A for g is represented as:

$$P\left[A\left(I, g(X)_{\{1,\ldots,l-1\}}\right) = g(X)_I\right] < \frac{1}{p(n)} \quad \forall p$$

where, p is a polynomial, X and I are random variables distributed respectively on $\{0,1\}^n$ and on $\{1, \ldots, l(n)\}$. Describe in detail which pseudo random property the given function ensemble represents by considering the success probability of adversaries, A. Provide sufficient justification to support your answer. [4 M]

[---------- END OF QUESTION PAPER ----------]