Amrita Vishwa Vidyapeetham

Amrita School of Engineering

TIFAC-Core in Cyber Security

End Semester Examination – Feb 2022

B.Tech in Cyber Security (CSE) – First Semester

Classical Cryptography (20CYS101)

Time: 12:00 PM – 1:30 PM **Total Marks: 20**

1. What is the major limitation of traditional one-time pad? How do the modern stream ciphers address it? [2 Marks]
2. Consider your roll number being a hex string (discard the letters beyond f). Convert it to decimal and use it as the key in Vigeńere cipher to show the encryption and decryption of the word IAMACRYPTOGRAPHER. [2 Marks]
   For eg:
   If roll number = CB.EN.U4CYS21099
   Key = $(C)_{16}(B)_{16}(E)_{16}(4)_{16}(C)_{16}(2)_{16}(1)_{16}(0)_{16}(9)_{16}(9)_{16}$
3. Suppose that you were performing chosen ciphertext attack on the ciphertext sequence 111000101100011010. Your attack successfully gave output for the first nine plaintext bits as 110101100 and the machine stopped working. Suppose that the keystream is generated by LFSR, find the key and recover the whole plaintext. [5 Marks]
4. Eve knows the below keystream and she knows that this is the output of 3-stage LFSR.
   Sequence/Output: 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 . . .
   Find the connection polynomial of the LFSR to help Eve (**without using Berlekamp Massey Algorithm**). [5 marks]
5. Use extended Euclidean theorem to find g, s and t for the equation below. [3 Marks]
   $g = x.s + 101.t$
   where x = last digit of your roll number + 20
6. Find key if below cipher text was generated using hill cipher. [3 Marks]
   Ciphertext = XYJB
   Plaintext = DONT

<u>Bonus Question</u>

1. Find the ciphertext if the key is “EDUCATION” and plaintext is “ACADEMYxy” where x is 2nd last digit of your roll number and y is last digit of your roll number. Use 3X3 matrix of both plaintext and key for finding ciphertext. Also decrypt the ciphertext and verify your answer. Please show step by step solution. [5 Marks]