DEPARTMENT OF COMPUTER SCIENCE AND ENGG.
NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI.

END SEMESTER EXAMINATION
CSPC35 Principles of Cryptography

10/05/21 Time: 2 hours

ANSWER ALL THE QUESTIONS

MAX: 30 Marks

1. (a) Use Fermat's Theorem to find a number *a* between 0 and 72 with *a* congruent to 9794 modulo 73. (2)
   (b) Find out the gcd (400,60) and the values of s and t using the Extended Euclidean algorithm. (2)
   (c) State and explain the CRT and its applications. (2)

2. (a) Given a one-time pad version of the Vigenère cipher scheme, where the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 ..., then the first letter of plaintext is encrypted with a shift of 3letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.
   (i). Encrypt the plaintext **sendmoremoney** with the key stream 9 0 1 7 23 15 21 14 11 11 2 8 9. (2)
   (ii). Using the ciphertext produced in part a, find a key so that the cipher Text decrypts to the plaintext **cashnotneeded.** **(**2)
   (b) With appropriate diagrams, explain the working of any two types of PRNG highlighting their merits and demerits. (2)

3.(a) Why does the round key generator need a parity drop permutation? (2)
(b)Find out whether GF (17) is a valid Galois field. (1.5)
(c) Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101},
Find out the,
(i) original contents of **State**, displayed as a 4 x 4 matrix.

(ii) value of **State** after initial AddRoundKey.
(iii)value of **State** after SubBytes.
(iv) value of **State** after ShiftRows.
(v) value of **State** after MixColumns (2.5)

4.(a) What is a trap door one way function? What are its properties? (2)

(b) In an RSA system, the public key of a given user is *e* = 31, *n* = 3599. What is the private key of this user?
(2)

(c) Suppose q=2579 and α=2. α Is a primitive element modulo q. Let X_B=7. Suppose Alice wishes to send the message M=1299 to Bob. Let k=853 is the random integer she chooses. Show the steps in El Gamal algorithm. (2)

5.(a) Distinguish between HMAC and CMAC. (2)

(b) It is possible to use a hash function to construct a block cipher with a structure similar to DES? Justify your answer. (2)

(c) DSA specifies that if the signature generation process results in a value of *s* = 0, a new value of *k* should be generated and the signature should be recalculated. Why? (2)

****