MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

I SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) END SEMESTER MAKE UP EXAMINATIONS, JAN. 2024

SUBJECT: ADVANCED CRYPTOGRAPHY AND CRYPTANALYSIS

[CSE 5120]

(12/01/2024)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1.A In a certain RSA cryptosystem implementation, the receiver selects two prime numbers p and q as 7 and 17 respectively and the public key e=5. In addition, receiver selects the private key d and maintains it as secret. Compute the secret key d. Determine the cipher text for the message comprising of characters '**MIT**'. Also verify that upon decryption it gives back the message. Show all the steps clearly. Hint: Encrypt each character separately. **5M**

1.B Cryptanalyze the Affine Cipher to find the keys used for encryption, if through frequency analysis, it is known that the ciphertext character R maps to character E in plaintext and ciphertext character K maps to plaintext character T. Hence decode the ciphertext **HFQR**. Show clearly all the steps. **3M**

1.C Determine the index of coincidence for the following ciphertext produced by Vigenere cipher. **2M**

SMWP PYAJS TLVA SMWJP

2.A Illustrate the method in which symmetric key can be distributed using symmetric encryption with the help of a Key Distribution Centre. Mention one disadvantage of this method. **5M**

2.B Illustrate the Diffie Hellman key agreement protocol with the help of an example. **3M**

2.C Outline any two methods that could be used to find the collision between two lists. **2M**

3.A Justify the need for the various criterions to be satisfied by the hash function with the help of an example each. **5M**

3.B Suppose Bob uses RSA algorithm to encrypt a message using the public modulus 899 and public key 7. Demonstrate how Pollard's (p-1) algorithm can be used to attack the RSA cryptosystem. Clearly indicate all the steps. **3M**

3.C Outline the steps in Lenstra's elliptic curve factorization method. **2M**

4.A Differentiate between modification detection code and message authentication code. Explain the various uses of message authentication codes. **5M**

4.B	Illustrate the various trust models that are used to verify the public keys of the users in a large setting with many certificate authorities.	**3M**
4.C	Develop a method to attack the RSA algorithm using the birthday paradox.	**2M**
5.A	Using Baby step Giant step algorithm, compute x in $3^x = 19 (\text{mod } 59)$.	**5M**
5.B	The ElGamal digital signature scheme is vulnerable to existential forgery, but it is very hard to do a selective forgery on this scheme. Justify this statement with examples.	**3M**
5.C	Compare digital signature with conventional signature.	**2M**