20194171

Department of Computer Science and Engineering
Motilal Nehru National Institute of Technology Allahabad
B.Tech VI semester (Computer Science and Engineering) May 2022
Cryptography and Network Security CS16104

Avoid story telling. Write the answers to the point.
All the questions are compulsory. Please assume any missing data and write it at the top of the answer.

Time 1.5 hrs **M.M 30**

Q1 a) Analyze DES with respect to brute force attack, differential cryptanalysis and linear cryptanalysis. 3*2=6 marks

b) Consider a variation of DES (Data Encryption Standard). Let's call this new variation D^{2}ES. In this approach, we use two instances of DES ciphers for encryption and two instances of reverse ciphers for decryption. Each instance uses a different key, which means that the size of the key is now doubled (112 bits). Analyze whether D^{2}ES is vulnerable to known-plain text attack.

Q2 a) Give a general formula to calculate the number of each kind of transformation (SubBytes, ShiftRows, MixColumns, and AddRoundKey) and the number of total transformations for each version of AES. The formula should be parameterized on the number of rounds. 3*2=6 marks

b) What is a weak key? What is the disadvantage of using a weak key?

Q3 a) Alice uses Bob's RSA public key (e = 3, n = 35) and sends the ciphertext 22 to Bob. Is it possible for Eve to find the plaintext using the cycling attack? Justify. 3*2=6 marks

b) Suppose that we have a block cipher where n=64.If there are 10 1's in the ciphertext, how many trail-and-error tests does Eve need to do to recover the plaintext from the intercepted ciphertext in each of the following cases:

i) The cipher is designed as a substitution cipher
ii) The cipher is designed as a transposition cipher

Q4 Discuss the susceptibility of RSA digital signature scheme to key-only attack, known message attack and chosen-message attack. 6 marks

Q5 a) Use a Hill cipher to encipher the message "We live in an insecure world". Use the following key: 3*2=6 marks

03	02
05	07

b) Atbash was a popular cipher among Biblical writers. In Atbash, "A" is encrypted as "Z", "B" is encrypted as "Y", and so on. Similarly, "Z" is encrypted as "A", "Y" is encrypted as "B", and so on. Suppose that the alphabet is divided into two halves and the letters in the first half are encrypted as the letters in the second and vice versa. Find the type of cipher and key. Encipher the message "an exercise" using the Atbash cipher.