

International Islamic University Chittagong
Department of Electronic and Telecommunication Engineering
Final Examination, Autumn 2018
 Course Code: ETE-4835
 Course Title: Cryptography and Network Security

Full Marks: 50

Time: 2h 30min

[Answer any two from Group-A and any three from Group-B of the following questions]

Group-A

- | | |
|---|---|
| 1.a) Explain the key distribution scenario. | 5 |
| b) Explain hierarchy key control and decentralized key control. | 5 |
| 2.a) Compare between private key cryptography and public key cryptography | 2 |
| b) Show and explain confidentiality using public key system. | 4 |
| c) Show and explain authentication using public key system. | 4 |
| 3.a) Explain the complete RSA algorithm. | 4 |
| b) Given two prime numbers $p=17$ and $q=11$
Apply complete RSA algorithm to find: | 6 |
| i) Public key | |
| ii) Private key | |
| iii) Encrypted and decrypted results for $M=88$ | |
| Show the complete process in a block diagram. | |

Group-B

- | | |
|---|-----|
| 4.a) Explain the Diffie-Hellman key exchange algorithm. | 5 |
| b) Users A and B use the Diffie-Hellman key exchange technique with a common prime $q=71$ and a primitive root $a=7$
Evaluate: | 5 |
| i) A's public key | |
| ii) B's public key | |
| iii) Shared secret key | |
| 5. Describe the techniques for the distribution of public keys. | 10 |
| 6.a) What is Extensible Authentication Protocol (EAP)? Why we need to maintain Authentication Methods ? | 4 |
| b) Write down the Classification of Hash Functions | 3 |
| c) Write a short note ECC Encryption and Decryption. | 3 |
| 7.a) Define hash function? Explain the basic uses of Hash functions. | 1+3 |
| b) Outline the requirements for Hash function. | 3 |
| c) Write down the importance of Digital Signature. Write down the types of Secure hash Algorithms. | 1+2 |