**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**
**End Semester Examination, April/May 2018**

**Course: Cryptography And Cryptanalysis** **Semester: II**
**Program: M.Tech. CSE-Sz-AI-II**
**Time: 03 hrs.** **Max. Marks: 100**

**SECTION A ( Attempt all questions)**

| S. No. | | Marks | CO |
|---|---|---|---|
| Q 1 | Why is SHA more secure than MD5? | **4** | **CO3** |
| Q 2 | Describe the advantage and disadvantage of symmetric and asymmetric key cryptography. | **4** | **CO1** |
| Q 3 | Write a short note on X.509. | **4** | **CO3** |
| Q 4 | Explain Fermat factorization method. Use suitable example | **4** | **CO2** |
| Q 5 | Find out the value of A, B & Key (K1 or K2) if n=11, g=5, x=2 & y=3 using Diffie-Hellman algorithm. | **4** | **CO4** |
| **SECTION B (Attempt Four Questions, Do one from 10th and 11th )** | | | |
| Q 6 | What is algorithm mode? Explain the different algorithm modes along with their advantage and disadvantage. | **10** | **CO1** |
| Q 7 | Using an example, explain the implementation of Friedman Test. | **10** | **CO4** |
| Q 8 | How cryptanalysis is different from cryptography? Explain the different types of cryptanalysis attacks. | **10** | **CO2** |
| Q 9 | A box contains gold coins. If the coins are equally divided among six friends, four coins are left over. If the coins are equally divided among five friends, three coins are left over. If the box holds the smallest number of coins that meets these two conditions, how many coins are left when equally divided among seven friends? | **10** | **CO2** |
| Q 10 | What is digital signature? Which cryptography property can be achieved through digital signature? Explain in detail | **10** | **CO3** |
| **SECTION-C (Attempt Two Questions, Do one from 13th and 14th )** | | | |
| Q 11 | (i) Explain the role of S/MIME protocol in email security.<br>(ii) Explain HMAC design objective and its algorithm? | **10*2= 20** | **CO4, CO3** |
| Q 12 | (i) Factor 31861 using the Pollard Rho method with polynomial $f(x)=x^2+1$ and initial guess $x_0=1$ .<br>(ii) Using Keyword "NETWORK", convert plain text "INJECTION TO JILL" into cipher text by Playfair cipher method. | **10*2= 20** | **CO2** |
| Q 13 | Using example explain the different substitution based cryptography techniques. | **20** | **CO1** |

| Name:<br>Enrolment No: | UPES |
|---|---|

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**
**End Semester Examination, April/May 2018**

**Course: Cryptography And Cryptanalysis** **Semester: II**
**Program: M.Tech. CSE-Sz-AI-II**
**Time: 03 hrs.** **Max. Marks: 100**

**SECTION A ( Attempt all questions)**

| S. No. | | Marks | CO |
|---|---|---|---|
| Q 1 | Explain the difference between MAC and message digest. | 4 | CO3 |
| Q 2 | Explain the role of confusion and diffusion in cryptography. | 4 | CO1 |
| Q 3 | How PGP is providing security to Email. | 4 | CO4 |
| Q 4 | Explain meet in the middle attack. | 4 | CO2 |
| Q 5 | What is the real crux of RSA? | 4 | CO1 |
| **SECTION B (Attempt Four Questions, Do one from 10th and 11th )** | | | |
| Q 6 | Discuss all the key principles of security in detail. | 10 | CO1 |
| Q 7 | Discuss the key features of IDEA algorithm. | 10 | CO3 |
| Q 8 | Using an example, explain The Vigenere cipher. | 10 | CO2 |
| Q 9 | What is key distribution and management? Discuss the associated issues with them | 10 | CO3 |
| Q 10 | Using an example, explain the implementation of Kasiski Test. | 10 | CO2 |
| **SECTION-C (Attempt Two Questions, Do one from 13th and 14th )** | | | |
| Q 11 | (i) Define Kerberos and name its servers. Briefly explain the duties of each server.<br>(ii) Explain the working and purpose of digital signature algorithm. | 10*2= 20 | CO4, CO3 |
| Q 12 | What is differential and linear cryptanalysis. Explain their working in detail. | 20 | CO2 |
| Q 13 | Using example explain the different transposition based cryptography techniques. | 20 | CO1 |