DEPARTMENT OF INFORMATION TECHNOLOGY

SUB: U20IT703-CRYPTOGRAPHY AND NETWORK SECURITY

YEAR/SEM:IV/VII

PART-B

UNIT 1: (INTRODUCTION)

1. Write about any two classical crypto system (substitution and transposition) with suitable examples (NOV2011,NOV 2010, MAY 2009,APR 2012,NOV 2012,,NOV 2007,NOVN 2008)
2. Write about fermat and euler's theorem in detail. (MAY/JUNE 2013,NOV 2012,DEC2016,APR2017),(APR2011,NOV 2012)
3. Explain any two classical ciphers and also describe the security limitation (APR 2017)
4. Describe linear feedback shift registers sequences and finite fields with their application in cryptography
5. Explain OSI security architecture model with neat diagram (DEC2016)
6. Describe various security mechanisms.(DEC2016)
7. State chinese remainder theorem & find X for given set of congruent equations X=1(mod 5) x=3(mod 9)
    a. x=2(mod 7) x=4(mod 11)
8. Encrypt the following using play fair cipher using the keyword MONOARCHY"SWARAJ IS MY BIRTH RIGHT ". use X for blank space (NOV 2017)
9. Discuss the properties that are to be satisfied by groups, rings & fields.(NOV 2017)
10. Explain classical encryption techniques with symmetric cipher & hill cipher model

Unit 2: (SYMMETRIC KEY CRYPTOGRAPHY)

1. Explain in detail about DES and Triple DES(APR 2012,NOV 2009,NOV 2008,APR 2017)
2. Explain about AES in details (NOV 2009,MAY 2009,NOV 2008,NOV 2009,APR 2017)
3. Explain about RC4 algorithm.(APR 2012)
4. Explain the RSA algorithm & explain the RSA with p=7,q=11,e=17,m=8.also discuss its merits(APR 2011,NOV 2011,NOV 2007,DEC 2016,NOV 2017,APR 2018)
5. Discuss the discrete logarithm and explain diffie helman key exchange algorithm. With its merits and demerits (APR 2011,NOV 2012,NOV 2010,DEC 2016,APR 2017)
6. Explain in details about elliptic curve cryptography(APR 2018)
7. User alice & bob exchange the key using Diffie Helman algorithm. Assume x=5,q=83,Xa=6,Xb=10.find Ya,Yb,K(NOV 2017)
8. Explain the key generation .encryption & decryption of SDES algorithm in detail
9. Explain the block cipher modes of operation
10. Explain the operations of hill cipher with an example

UNIT 3: (PUBLIC KEY CRYPTOGRAPHY)

1. Explain about MD5 in detail(APR 2011,APR 2012,DEC 2016,APR 2018)
2. Illustrate about the SHA algorithm and explain (NOV 2017,NOV 2011,NOV 2010,NOV 2009,MAY 2009,MAY 2007)

3. Write a detailed note on digital signatures (NOV 2011,NOV 2010,DEC 2016,APR 2017)
4. Write notes on birthday attack (APR 2017)
5. Compare the performance of RIPEMD-160 algorithm and SHA-1 algorithm (APR 2017)
6. Describe about hash function. How its algorithm is designed ? Explain in features and properties(NOV 2012,NOV 2008,APR 2018)
7. Write down the steps involved in Elgamal DSS & schnorr DSS (NOV 2017)
8. Explain about diffie hellman key exchange algorithm with one suitable example
9. Explain the SHA in detail(with neat diagram) for SHA-512 processing of a single 1024 bit block
10. Explain the challenges/ response approach in mutual authentication

UNIT 4 : (MESSAGE AUTHENTICATION AND INTEGRITY)

1. Explain kerberos authentication mechanism with suitable diagram(DEC 2016,APR 2018)
2. Explain in detail about firewalls(APR 2011,NOV 2011,APR 2012,NOV 2012 ,NOV 2010,DEC 2016,NOV 2017)
3. Explain about viruses in detail(APR 2011,NOV 2012,APR 2017)
4. Explain the type of intrusion detection system (NOV 2011,NOV 2010,APR 2017)
5. Explain about malicious software (APR 2012)
6. Explain in detail about SET for E-commerce transaction (NOV 2017)
7. Explain briefly about trusted system
8. Explain about the security standard
9. Describe any two advanced anti-virus technique in detail
10. Explain statistical anomaly detection & rule based intrusion detection

UNIT 5 : (SECURITY PRACTICE AND SYSTEM SECURITY)

1. Explain the operation description of PGP (APR 2011,NOV 2012,NOV 2010,NOV 2009,MAY 2009,DEC 2016,APR 2018)
2. Explain in detail about architecture of IP security (APR 2011,APR 2012,NOV 2010,DEC 2017)
3. Discuss authentication ,header , ESP in detail with their packet format(APR 2017,NOV 2017)
4. Describe SSL architecture in details(APR 2011,NOV 2011,MAY 2009,NOV 2007)
5. Discuss the working of SET & PKT with neat diagram (APR 2011,NOV 2011,APR 2012,NOV 2012, NOV 2010,DEC 2016,APR 2018)
6. Explain the step , methodology involved in SSL/TLS protocol(NOV 2017)
7. Explain pretty good privacy in detail
8. Explain about the PKI
9. Explain about S/MME in detail
10. Explain about x.0509 authentication service in detail