# Maulana Azad National Urdu University

## M.C.A, V Semester Examination, February 2022

## Paper : MMCA503PCT : Cryptography and Network Secruity

## پرچہ : کرپٹوگرافی اینڈ نیٹ ورک سیکیوریٹی

**Time : 3 hrs** **Marks : 70**

**ہدایات:**

یہ پرچہ سوالات دو حصوں پر مشتمل ہے: حصہ اول اور حصہ دوم۔ ہر جواب کے لیے لفظوں کی تعداد اشارۃً ہے۔ تمام حصوں سے سوالوں کا جواب دینا لازمی ہے۔

1. حصہ اول میں 10 سوالات ہیں، اس میں سے طالب علم کو کوئی 08 سوالوں کے جواب دینے ہیں۔ ہر سوال کا جواب تقریباً سو (100) لفظوں پر مشتمل ہے ہر سوال کے لیے 05 نمبرات مختص ہیں۔ **(8 x 5 = 40 Marks)**
2. حصہ دوم میں 05 سوالات ہیں۔ اس میں سے طالب علم کو کوئی 03 سوال کا جواب دینا ہے۔ سوال کا جواب تقریباً ڈھائی سو (250) لفظوں پر مشتمل ہے سوال کے لیے 10 نمبرات مختص ہیں۔ **(10x3 = 30 Marks)**

---

## حصہ اول

1. Security Attack کی تعریف کیجیے۔ مختلف قسم کے Secruity Attacks کے بارے میں لکھیے۔
2. Encryption Algorithm کے دو بنیادی Functions کے بارے میں سمجھائیے۔
3. Fermat Theorem کے بارے میں سمجھائیے۔ دیے گئے Plain Text "ACT" کو key GYBNQKURP کے ذریعہ سے Hill Cipher سے حل کیجیے۔
4. Asymmetric Cryptography زیادہ Data (Huge) کے لیے استعمال نہیں ہوتا۔ اس کی وجہ بتائیے۔
5. Avalanche Effect کسے کہتے ہیں؟ اور Ellipti Curve Cryptography کے بارے میں سمجھائیے۔
6. Digital Signatures اور Authentication Protoccols کے درمیان فرق واضح کیجیے۔
7. Intinder کسے کہتے ہیں؟ Intender کے تین Classes کے بارے میں لکھیے۔
8. دیے گئے Plain Text کو "SWARAJ IS MY BIRTH RIGHT" کو MONARKHY, KEYWORD کے ذریعہ Playfiar Cipher سے Encrypt کیجیے۔
9. درجہ ذیل پر Short نوٹ لکھیے۔

   (a) Honey Pot

   (b) ZOMBIE

   (c) Botnets

10. RSA Algorithm کو استعمال کرتے ہوئے مندرجہ ذیل کا Encryption اور Decryption معلوم کیجیے۔

P = 17; q=11, c=7; M=88

## حصہ دوم

11. DES Algorithm کو تفصیل سے سمجھائیے۔اس کے مختلف مراحل (Steps) کو خاکہ (Figure) کے ذریعہ سمجھائیے۔

12. Diffie, Hellman Key Exchange Algorithm کے Merits اور Demerits کے بارے میں لکھیے۔ Diffie Hellman Key Exchange Protocol کے ذریعہ Alice اور Prob ایک Secret Key (Establish) قائم کرنا چاہتے ہیں۔مان لیجیے کہ:

n=1 1, g=5, x=2, y=3

A,B, $K_1$ & $K_2$

کو Values معلوم کیجیے۔

13. AES Algorithm کی کارکردگی کو تفصیل سے سمجھائیے۔ Kerberos کے بارے میں سمجھائیے۔اگر Client C کو 'Server 'S سے Communicate کرنے کے لیے استعمال ہونے والے Authentication Dialogue لکھیے اور اس کا Kerberos Procedure بیان کیجیے۔

14. Message Digest کے بارے میں سمجھائیے۔ Message Digest کی Requirements بیان کیجیے۔ MD5 Algorithm کی (Working) کارکردگی کو تفصیل سے سمجھائیے۔

15. (a) Message Digest Algorithm SHA - 512 کے بارے میں سمجھائیے۔

(b) Secure Socket Layer (SSL) کے بارے میں سمجھائیے۔

(c) TCP/IP Protocol Suite میں SSL کی Position اور اس کی کارکردگی کے بارے میں سمجھائیے۔

☆☆☆