Maulana Azad National Urdu University

MCA : V Semester Examination - May - 2018

Paper - MMCA503PCT : Cryptography & Network Security (Backlog)

Time : 3 hrs **Marks : 70**

ہدایات:

یہ پرچہ سوالات تین حصوں پر مشتمل ہے: حصہ اول، حصہ دوم، حصہ سوم۔ ہر جواب کے لئے لفظوں کی تعداد اشارۃً ہے۔ تمام حصوں سے سوالوں کا جواب دینا لازمی ہے۔

1. **حصہ اول** میں **10** لازمی سوالات ہیں جو کہ معروضی سوالات/ خالی جگہ پُر کرنا/مختصر جواب والے سوالات ہیں۔ ہر سوال کا جوابلازمی ہے۔ ہر سوال کے لیے 1 نمبر مختص ہے۔ **(10 x 1 = 10 Marks)**
2. **حصہ دوم** میں آٹھ سوالات ہیں، اور اس میں طالب علم کو کوئی پانچ سوالوں کے جواب دینے ہیں۔ ہر سوال کا جواب تقریباً دوسو **(200)** لفظوں پر مشتمل ہے۔ ہر سوال کے لیے **6** نمبرات مختص ہیں۔ **(5 x 6 = 30 Marks)**
3. **حصہ سوم** میں پانچ سوالات ہیں۔ اس میں سے طالب علم کو کوئی تین سوالوں کے جواب دینے ہیں۔ ہر سوال کا جواب تقریباً پانچ سو **(500)** لفظوں پر مشتمل ہے۔ ہر سوال کے لیے **10** نمبرات مختص ہیں۔ **(3 x 10 = 30 Marks)**

حصہ اول

سوال نمبر : 1

(i) Secruity Attacks کی وضاحت کیجیے۔

(ii) Crypt Analysis کی وضاحت کیجیے۔

(iii) PGP کی تشریح کریں۔

(iv) Intruders کے اقسام بیان کیجیے۔

(v) Honey Pots سے کیا مراد ہے؟

(vi) DOS Attack کی وضاحت کیجیے۔

(vii) SHTTP اور SSL کے درمیان فرق بیان کیجیے۔

(viii) Brute Force Attack کی وضاحت کیجیے۔

(ix) Phishing کی وضاحت کیجیے۔

(x) Steganography کسے کہتے ہیں؟

حصہ دوم

(2) Hill Cipher کومثال کے ذریعہ سمجھایئے۔ Stream Cipherاور Block Cipher کومثال کے ذریعہ سمجھایئے۔

(3) Stream Cipher اور Block Cipher کومثال کے ذریعہ سمجھایئے۔

(4) Electronic Code Book (ECB) اور Cipher Block Chaining Mode (CBC) کوخاکہ (Figure) کے ذریعہ تفصیل سے سمجھایئے۔

(5) S-Box Substitution اور P.Box Permutation کے بارے میں سمجھایئے۔

(6) Double DES اور Triples DES کے بیچ فرق واضح کیجیے۔

(7) Digital Certificate کیاہے؟ اس کی خصوصیات بیان کیجیے۔

(8) Biometrics کو Password Authentication کے بدلے میں کیسے استعمال کیا جاتا ہے؟

(9) Playfair Cipher کیاہے؟ دیے گئے 'HIDE THE GOLD' Plain Text کو Hello World کے ذریعہ Plain Text کو Encrypt کیجیے۔

حصہ سوم

(10) a) کسی بھی چار Substitution Techniques کومثال کے ذریعہ سمجھایے۔

b) Kerberos کی وضاحت کیجیے۔یہ Authentication کیسے فراہم (Provide) کرتا ہے؟

(11) a) SHA Algorithm کوتفصیل سے سمجھایئے۔

b) Blowfish Algorithm کی کارکردگی (Working) کوتفصیل سے سمجھایئے۔

(12) a) Elliptic Curve Cryptography کوتفصیل سے سمجھایئے۔

b) RSA Algorithm کوسمجھایئے۔

(13) Transport Layer Secruity کے بارے میں تفصیل سے سمجھایئے۔SSL اور TLs کے درمیان واضح کیجیے۔

(14) مندرجہ ذیل پر مختصر نوٹ لکھیے۔

i) X.509 Certificate

ii) S/MIME

☆☆☆