Maulana Azad National Urdu University

B.Tech VIII Semester Examination - May - 2018

Paper - BTCS801PCT : Network Security

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 جواب لازمی 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) Interruption Attacks کو _____ Attack بھی کہا جاتا ہے۔

(a) Masquerade (b) Alteration (c) Denial of Secrice (d) Replay Attacks

(ii) ایک ایسا Mechanism جس میں Text کو Rows میں لکھا جاتا ہے اور Columns میں پڑھا جاتا ہے۔

(a) Vernam Cipher (b) Caesar Cipher

(c) Simple Columnar Transposition Technique (d) Homophonic Substitution Techniques

(iii) Matrix Theory _____ Technique میں استعمال ہوتی ہے۔

(a) Hill cipher (b) Mono Alphabetic Cipher

(c) Playfair Cipher (d) Vigenere Cipher

(iv) ان میں سے _____ Plain Text کی Redundancy کو بڑھاتا ہے۔

(a) Confusion (b) Diffusion

(c) Both confusion & diffusion (d) Neither Confusion nor diffusion

(v) AES Encryption Scheme میں اصل Algorithm _____ ہے۔

(a) Blowfish (b) IDEA (c) Rijndael (d) Rc_4

(vi) IDEA Algorithm میں ' Key Size _____ ہوتی ہے۔

(a) 128 bytes (b) 128 bits (c) 256 bytes (d) 256 bits

(vii) Message کی Integrity کو Verify کرنے کے لیے _____ استعمال ہوتا ہے۔

(a) Message Digest (b) Decryption Algorithm

(c) Digital Envelope (d) ان میں سے کوئی نہیں

(viii) سب سے Strongest Message Digest Algorithm _____ کو سمجھا جاتا ہے۔

(a) SHA - 1 (b) SHA - 256 (c) SHA - 128 (d) SHA - 512

(ix) ایک Digital Certificate ایک صارف (User) کو _____ سے باندھتا ہے۔

(a) Public Key (b) Private Key (c) Organization Name (d) Name

(x) _____ ایک Message Digest Algorithm ہے۔

(a) DES (b) IDEA (c) MD5 (d) RSA

حصہ دوم

(2) Cryptography میں Modular Arithematic کیوں استعمال ہوتا ہے۔

(3) دیے گئے Plain Text M=88 کو RSA Algorithm استعمال کرتے ہوئے Plain Text کا Encryption معلوم کیجیے۔
p=17، q=11 اور Public Component e=7

(4) Active اور Passive Attacks کے بیچ فرق بتائیے۔ دونوں کو مثال کے ذریعہ تفصیل سے سمجھائیے۔

(5) (a) Public Key Infrastructure کے بارے میں تفصیل سے سمجھائیے۔

(b) Brute Force Attack کو استعمال کرتے ہوئے دیے گئے Cipher Text CMTMROOEOORW کا Plain Text معلوم کیجیے۔

(6) Diffie - Hellman Key Exchange الگورتھم کو مثال کے ذریعہ سمجھائیے۔ اسکے فائدہ اور نقصانات بیان کیجیے۔

(7) ARP Spoofing اور Redirection کو خاکہ (Figure) کے ذریعہ سمجھائیے۔

(8) Differential اور Linear Cryptanalysis کے بیچ فرق واضح کیجیے۔

(9) مندرجہ ذیل پر مختصر نوٹ لکھیے۔ (a) Euler's Function (b) Stamping Protocol

حصہ سوم

(10) (a) Rc4 الگورتھم کی کارکردگی کو تفصیل سے سمجھائیے۔

(b) AES Algorithm کو خاکہ کے ذریعہ تفصیل سے سمجھائیے۔

(11) PKCS کے مختلف Standards اور انکے مقصد کو تفصیل سے سمجھائیے۔

(12) TCP/IP Protocol Site میں SSL کے Position کو خاکہ (Figure) کے ذریعہ سمجھائیے۔ - SSL - handshake Protocol کے بارے میں سمجھائیے۔

(13) مندرجہ ذیل پر مختصر سا نوٹ لکھیے۔ (i) PEM (ii) PGP (iii) S/MIME

(14) (a) WLAN Scanners اور WWN Sniffers کے بارے میں سمجھائیے۔

(b) Session Hijacking کے مختلف مراحل (Steps) کے بارے میں سمجھائیے۔

☆☆☆