Maulana Azad National Urdu University

B.Tech VIII Semester Examination - May - 2017

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) Nigerian Frand سے کیا مراد ہے؟ اور اسے کیسے بچا جا سکتا ہے۔

(ii) 'Websites' کو (Attack) حملہ کرنے کے لئے Attackers کونسے مشہور Tools استعمال کرتے ہیں۔

(iii) Dos Attacks _____ سے ہوتے ہیں۔

(a) Authentication (b) Alteration

(c) Fabrication (d) Replay Attack

(iv) Caesar Cipher _____ کی مثال ہے۔

(a) Substitution Cipher (b) Transposition Cipher

(c) Substitution اور Transposition Cipher (d) ان میں سے کوئی نہیں

(v) Vernam Cipher کو _____ بھی کہا جاتا ہے۔

(a) Rail Fence Technique (b) One Time Paid

(c) Book Cipher (d) Running Key Cipher

(vi) DES _____ Block Bits کو Encrypt کرتا ہے۔

32 (a) 56 (b) 64 (c) 129 (d)

(vii) _____ IDEA Algorithm پہ منحصر (Based) ہے۔

S/MIME (a) PGP (b) SET (c) SSL (d)

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

Blow Fish (a) IDEA (b) Rijndel (c) RC4 (d)

(ix) Blow Fish (Algorithm) الگورتھم Subkey Generation کے لیے _____ الگورتھم کو Execute کرتا ہے۔

IDEA (a) Rijndad (b) RC4 (c) IDEA (d)

(x) Honey Pot کسے کہتے ہیں۔

حصہ دوم

(2) Diffic - Hellman Key Exchange Agreement الگورتھم کو مثال کے ذریعہ سمجھائیے۔

(3) Elliptic Curve Cryptography کے بارے میں آپ کیا جانتے ہیں۔

(4) Initialization Vector (Iv) کیا ہے اور اس کی کیا اہمیت ہے۔

(5) Elgamal Cryptography کے بارے میں بحث کیجئے۔

(6) مندرجہ ذیل پہ مختصر سا نوٹ لکھیئے۔

Pachil Filtering (a) Application Gateways (b)

(7) Radix 64 کے بارے میں سمجھائیے۔

(8) Message Digest کسے کہتے ہیں اور اس کی کیا ضروریات ہیں۔

(9) Digital Signatures کے بارے میں سمجھائیے۔ Digital Signatures پہ ہونے والے حملوں کے بارے میں سمجھائیے۔

حصہ سوم

(10) RC5 میں Encryption کیسے ہوتا ہے۔ RC5 کو (Working) کارکردگی کے بارے میں تفصیل سے لکھیئے۔ RC4 اور RC5 کے بیچ فرق سمجھائیے۔

(11) DES کی کارکردگی کو تفصیل سے سمجھائیے۔ Double DES اور Triple DES کیا ہے۔

(12) Blow Fish الگورتھم کو تفصیل سے سمجھائیے۔

(13) SHA الگورتھم MD5 سے زیادہ Secure کیوں ہے سمجھائیے۔

(14) مندرجہ ذیل پہ مختصر سا نوٹ لکھیئے۔

SSL Hand Shake Protocol (a) Kerberos (b) Key Distribution Centre (c)

☆☆☆