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) "Man in the middle attack" کسے کہتے ہیں؟

(ii) DDOS Attack کسے کہتے ہیں؟

(iii) PEM کا خلاصہ کیجیے۔

(iv) SSO کا خلاصہ.....ہے۔

(v) WTLS کا خلاصہ.....ہے۔

(vi) DOS Attacks اس کی وجہ سے ہوتا ہے۔

(a) Authentication (b) Alteration

(c) Fabrication (d) Replay Attacks

(vii) Network کو (Halt) روکنے کے لیے.....خود کی نقل(Copies) بنا کر Replicate کرتا ہے۔

(a) Virus (b) Worm

(c) Trojan Horse (d) Bomb

(viii) Matrix Thoery ..... Technique میں استعمال ہوتی ہے۔

(a) Hill Cipher (b) Monoalphabetic Cipher

(c) Playfair Cipher (d) Vigenere Cipher

(ix) DES ..... Block of bits کو Encrypt کرتا ہے۔

(a) 32 (b) 56 (c) 64 (d) 128

(x) MD5 Algorithm میں Key کی Size .....ہوتی ہے۔

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

حصہ دوم

(2) مندرجہ ذیل پر مختصر سا نوٹ لکھیے۔

(a) Worm (b) DNS Attack

(c) Packet Siiffing (d) Phishing

(3) دیے گئے 'MY NAME IS ATUL' plant text کو 'PLAYFAIR EXAMPLE' keyword کے ذریعہ Play Fair Cipher کی Technique کو استعمال کرتے ہوئے اس کا Cipher Text معلوم کیجیے۔

(4) Shannon کے Confusion اور Diffusion کے Concept کو سمجھائیے۔

(5) Elliptic Curve Cyrptography کے بارے میں تفصیل سے سمجھائیے۔

(6) Initialization Vector کس لیے استعمال ہوتا ہے؟

(7) IDEA Algorithm کو خاکہ (Figure) کے ذریعہ تفصیل سے سمجھائیے۔

(8) 3-D Secure Protocol کے بارے میں تفصیل سے سمجھائیے۔

(9) مختلف قسم کے Session Hijacking اور اس کے Steps کیا کیا ہیں؟ سمجھائیے۔

حصہ سوم

(10) DES Algorithm کو خاکہ کے ذریعہ اس کی کارکردگی (Working) کو تفصیل سے سمجھائیے۔

(11) Blowfish Algorithm کی کارکردگی (Working) کو خاکہ کے ذریعے تفصیل سے لکھیے۔

(12) Wireless 802.11 Network اور اس کی Security کے بارے میں تفصیل سے بیان کیجیے۔

(13) RC5 Algorithm کی کارکردگی (Working) کو خاکہ کے ذریعہ تفصیل سے لکھیے۔

(14) (a) Diffie Hellman کے Key Exchange کو مثال کے ذریعہ تفصیل سے سمجھائیے۔

(b) مندرجہ ذیل پر مختصر نوٹ لکھیے۔

(i) Digital Certificate

(ii) SSL v. SET

☆☆☆