Maulana Azad National Urdu University

M.Tech I Semester Examination - December - 2017

Paper - MTCS101PCT : Advance Network Security (New Pattern)

پرچہ : اڈوانس نٹ ورک سیکیوریٹی

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 8 سوالات ہیں، اس میں سے 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 5 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 (1)

(i) Modern Block Cipher کے Components بیان کریں۔

(ii) Diffusion اور Confusion کے فرق بیان کریں۔

(iii) RSA Algorithm کی Keysize کیا ہے؟

(iv) Symmetric Key Cryptographic Algorithm کی وضاحت کریں۔

(v) دو نمبروں کی GCD حاصل کرنے کا Formula بیان کریں۔

(vi) Prime Number p=11 کی سب Relative Prime Numbers لکھیں۔

(vii) Simple DES اور Double DES میں کتنے Rounds ہوتے ہیں۔

(viii) Intruder Types کی تین Broad Categories لکھیں۔

(ix) PGP کی طرف سے فراہم ہونے والے Service بیان کریں۔

(x) Session Hijacking کا کیا مقصد ہے؟

حصہ دوم

(2) Feistel اور Non-Feistel Block Cipher کے فرق بیان کریں۔

(3) Passive Attackes اور Active Attackes کے درمیان فرق بیان کریں' Release of Message Contents' Interruption, Traffice Analysis اور Modification کے لحاظ سے

(4) ہمیں Authentication کی ضرورت کیوں ہے؟ Non-Repudiation Problem مثال کے ذریعہ سمجھائیے۔

(5) Brute Force Attack اور Crypt Analysis کے Hash Fanctions اور Messages Authentication Codes کی Security کا موازنہ کریں۔

(6) Cryptography میں Birthday Attacks کی اہمیت بیان کریں۔

(7) Digital Signature Algorithm کے Steps لکھیں۔

(8) Version 4 اور Version 5 Kerberos کے فرق بیان کریں۔

(9) Wireless Networks کی Jamming اور Anti-Jamming کے کوئی بھی ایک Technique سمجھائیے۔

حصہ سوم

(10) Cryptographic Techniques کی مدد سے ذیل Techniques کے Merits اور Demerits سمجھائیے۔

(a) Polygram Substituion Cipher

(b) Rail Fence Techniques

(11) Public اور Private کو Symmetric Key اور Assymetric Key کے مطابق سمجھائیے۔

(12) مناسب مثال کے ذریعے Diffie-Hellman Key Exchange/agreement Algorithm سمجھائیے۔

(13) مناسب ڈائی گرام کی مدد سے Fiestal Cipher Algorithm for Encryption and Decryption سمجھائیے۔ Algorithm کو Design کرنے کے دوران مسائل پر بھی Discuss کریں۔

(14) تعین کریں کہ ذیل P-Box Permutation Table ایک Straight P-Box ہے۔ایک Compression P-Box ہے یا ایک Expansion P-Box ہے۔

1	1	2	3	4	4

معلوم کریں کہ ذیل P-Box Permutation Table ایک Straight P-Box یا ' ایک Compression P-Box ہے' یا ایک Expansion P-Box ہے۔

1	3	5	6	7

☆☆☆