Maulana Azad National Urdu University

M.C.A V Semester Examination - December - 2017

Paper - MMCA503PCT : Crptography & Network Security

پرچہ : کرپٹوگرافی اینڈ نیٹ 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) ..... Attacks میں Message کے Content ' Modify ہوتے ہیں۔

(a) Passive Attacks (b) Active Attack (c) Replay Attacks (d) ان میں کوئی نہیں

(ii) Network کو Halt کرنے کے لیے.....خود کی Copies بنا کے Replicate کرتا ہے۔

(a) Virus (b) Worm (c) Trojan Horse (d) Bomb

(iii) Vernam Cipher .....کی ایک مثال ہے۔

(a) Substitution Cipher (b) Transposition Cipher (c) دونوں بھی (d) ان میں کوئی نہیں

(iv) Matrix Theory ..... Technique میں استعمال ہوتی ہے۔

(a) Hill Cipher (b) Monoalphabetic Cipher

(c) Playfair Cipher (d) Vigenere Cipher

(v) ..... ہر بار Plain Text کا ایک ہی Bit کو Encrypt کیا جاتا ہے۔

(a) Stream Cipher (b) Block Cipher (c) دونوں بھی (d) ان میں کوئی نہیں

(vi) ..... Plain Text کی Redundancy کو بڑھاتا ہے۔

(a) Confusion (b) Difussion (c) دونوں بھی (d) ان میں کوئی نہیں

(vii) DES ..... bits کو Encrypt کرتا ہے۔

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

(viii) ..... IDEA الگورتھم پر منحصر (Based) ہے۔

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

(ix) AES میں 16 - byte key کو .....میں Expand کیا جاتا ہے۔

184 Bytes (d) 176 Bytes (c) 78 bytes (b) 200 bytes (a)

(x) RC5میں کم سے کم ..... Roundsہونے چاہیے۔

20 (d) 16 (c) 12 (b) 8 (a)

حصہ دوم

(2) کسی بھی دس (10) مختلف قسم کے ہونے والے Security Attacks کے بارے میں لکھیے۔

(3) CBC, ECB اور CFB کو خاکہ کے ذریعہ سمجھائیے۔

(4) Blow Fish الگورتھم میں Subkey Generation کے بارے میں سمجھائیے۔

(5) (HMAC) Hash-based Message Authentication Code کے بارے میں لکھیے۔

(6) Knapsack الگورتھم کو مثال کے ذریعہ سمجھائیے۔

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

(8) Digital Signatures کسے کہتے ہیں؟ Digital Signaturesپر ہونے والے حملوں کے بارے میں سمجھائیے۔

(9) مندرجہ ذیل پر نوٹ لکھیے۔

(a) Transport Layer Security

(b) RC4 Algorithm

حصہ سوم

(10) IDEA الگورتھم کی کارکردگی کو خاکے کے ذریعہ تفصیل سے سمجھائیے۔

(11) Secure Hash Algorithm کو تفصیل سے مثال کے ذریعے سمجھائیے۔

(12) MD5 Message Digest الگورتھم کی کارکردگی کو تفصیل سے سمجھائیے۔

(13) RSA Algorithm کے بارے میں سمجھائیے۔ p = 7; q =11; e = 17; m = 8 کو استعمال کرتے ہوئے Encryption اور Decryption معلوم کیجیے۔

(14) مندرجہ ذیل پر تفصلی نوٹ لکھیے۔

(a) SSL in TCP/IP Protocol Suite

(b) Wired Equivalent Privacy (WEP)

☆☆☆