Maulana Azad National Urdu University

M.C.A V Semester Examination, January 2021

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) مندرجہ ذیل کو Decipher کرنے کے لیے Caeser's Cipher استعمال کیجیے۔

Encrypted Lock (d) Abandoned Text(c) Encrypted Text(b) Abandoned Lock (a)

(ii) Monoalphabetic Ciphers دوسرے Polyalphabetic Ciphers سے زیادہ Strong ہوتے ہیں کیوں کہ اس کی Frequency Analysis پچھلے سے زیادہ Tough مشکل ہوتی ہے۔

(a) صحیح (b) غلط

(iii) DES .....کو استعمال کرتے ہوئے کام کرتا ہے

(a) Permutation & Substituion on 64 bit block of plan text

(b) Only Permutation on blocks of 128 bits

(c) Exclusive Oring keybits with 64 bit blocks

(d) 4 rounds of substitution on 64 bit blocks with 56 bit key

(iv) آج کل استعمال ہونے والے Ciphers کو Round Cipers بھی کہا جاتا ہے کیونکہ اس میں.....ہوتے ہیں۔

Round about (d) Multiple Round(c) Double Round(b) Single Round (a)

(v) Advanced Encryption Standard (AES) کو .....نے Design کیا۔

(a) National Institute of Standards & Technology (b) IBM

(c) HP (d) Intel

(vi) Blow Fish Algorithm's Key Expansion ایک 448 bits key کو کئی Sub Key Arrays میں بڑھاتی ہے اور اس کے..... Bytes ہیں۔

4096 (a) 4608 (b) 4168 (c) 4894 (d)

(vii) Transposition کو.....بھی کہا جاتا ہے۔

Permutation (a) Combination (b) Binomial Variations (c) Variation (d)

(viii) Symmetic System کا Major Drawback ..... ہے۔

Key Distribution (a) Key Diffusion (b)

Key Confusion (c) Key Constructions (d)

(ix) ..... Asymmetric Key Exchange Procedure کی ایک Classical مثال ہے۔

Certificate (a) Cryptographic Hash FUnction (b)

Diffie-Hellman Scheme (c) Digital Signature (d)

(x) Message Integrity فراہم کرنے کے لیے SSL ..... Algorithm استعمال کرتا ہے۔

Hash (a) Null (b) Encyption (c) Decryption (d)

حصہ دوم

(2) (a) Substitution اور Transposition Techniques کے بیچ فرق واضح کیجیے۔

(b) Network Security میں Random Numbers کو کیوں استعمال کیے جاتے ہیں۔تجزیہ (Analyze) کیجیے۔

(3) PGP کی وضاحت کیجیے۔ PGP ایک Open Source کیوں ہے؟ سمجھائیے۔ PGP کے Notations کون سے ہیں؟

(4) IPSEC کی وضاحت کیجیے۔ IPlayer میں Traffic کے لیے IPSEC کون کون سی Services فراہم کرتا ہے۔

(5) Authentication کے لیے Password کی جگہ Biometrics کیسے استعمال ہوتا ہے؟ سمجھائیے۔

(6) مختلف قسم کے Comptuer Virus بیان کیجیے۔ Computer Virus موجود ہونے کے مختلف Signs کیا ہوتے ہیں؟ اور اس کے Counter Measures کیا لینے چاہیے۔

(7) Fiestel Block Cipher کو Fiqure کے ذریعہ تفصیل سے سمجھائیے۔

(8) Hill Cipher کی وضاحت کیجیے اور دیے گئے Plain Text: Act کو Key: GYBNQKURP کے ذریعہ اس کا Cipher Text معلوم کیجیے۔

(9) RC5 Algorithm کی کارکردگی (Working) اور اس کے مختلف مراحل (Steps) کو Figures کے ذریعہ تفصیل سے سمجھائیے۔

حصہ سوم

(10) Digital Signature Standard (DSS) کے بارے میں تفصیل سے سمجھائیے۔ DIgital Signature پر ہونے والے مختلف Atacks کون کون سے ہیں؟ تفصیل سے لکھیے۔

(11) Kerberos کیا ہے؟ Kerberos کیسے کام کرتا ہے اور یہ کس لیے استعمال ہوتا ہے؟ X.509 کے بارے میں آپ کیا جانتے ہیں؟

(12) Collision Theorem کیا ہے؟ Meet-in-the-middle Attacks کسے کہتے ہیں؟

(13) Blowfish Algorithm کی کارکردگی اور اس کے مراحل (Steps) کو تفصیل سے سمجھائیے۔

(14) (a) Elgamal Public Key Crypto System کے بارے میں تفصیل سے سمجھائیے۔

(b) RC5 Algorithm کو تفصیل سے بیان کیجیے۔

☆☆☆