Maulana Azad National Urdu University

M.C.A V Semester Examination - December - 2018

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) Caesar Cipher .....کی مثال ہے۔

(a) Poly-alphabetic Cipher (b) Mono-alphabetic Cipher

(c) Multi-alphabetic Cipher (d) Pri-alphabetic Cipher

(ii) ان میں سے کون سا Algorithm ہے جو Asymmetric-key Cryptography میں استعمال نہیں ہوتا۔

(a) RSA Algorithm (b) Diffie-Hellman Algorithm

(c) Electronic Code Book Algorithm (d) ان میں سے کوئی نہیں

(iii) Data Encryption Standard (DES) کیا ہے؟

(a) Block Cipher (b) Stream Cipher (c) Bit Cipher (d) ان میں سے کوئی نہیں

(iv) ان میں سے کون سا Cryptographic Protocol ہے جو Secure HTTP Connection فراہم کرتا ہے؟

(a) Stream Control Transmission Protocol (SCTP)

(b) Transport Layer Security (TSL)

(c) Explicit Congestion Notification (ECN)

(d) Resource Reservation Protocol (RRP)

(v) MD5 سب سے (Fast) تیز ہے اور..... Message Digest بناتا ہے۔

(a) 512 bits (b) 1024 bits (c) 128 bits (d) 64 bits

(vi) SET ..... کی مدد سے Anthentication فراہم کرتا ہے۔

Dual Signature (a) Digital Certificate (b)

Payments Public Key (c) Payment's Private Key (d)

(vii) SSH ان Layers کے درمیان رکھا جاتا ہے؟

Transport & Datalink (a) Applications & Presentation (b)

Application and Transport (c) Application and Session (d)

(viii) Merkle اور Hellman نے ..... Concept کو متعارف (Introduction) کروایا۔

Meet in the middle attack (a) Meet is attack (b)

Hijack (c) Virus Attacks (d)

(ix) Blowfish Algorithm کی Maximum Size ..... ہوتی ہے۔

256 bits (a) 512 bits (b) 56 bytes (c) 48 bytes (d)

(x) مندرجہ ذیل Text کو Caesar Cipher کے ذریعے Decipher کیجیے۔

H Q F U B S W H G W H A W

ABANDONED LOCK (a) ENCRYPTED TEXT (b)

ABANDONED TEXT (c) ENCRYPTED LOCK (d)

حصہ دوم

(2) Hill Cipher کو استعمال کرتے ہوئے دیے گئے Message کو Encipher کیجیے۔ "we live in a insecure world"
$key \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$ کو استعمال کیجیے

(3) Transposition اور Substitution Cipher کے مختلف اقسام اور دونوں کے بیچ فرق سمجھائیے۔

(4) Play Fair Cipher کو استعمال کرتے ہوئے دیے گئے Text "SWARAJ IS MY BIRTH RIGHT" کو Keyword MONARCHY کے ذریعہ Encrypt کیجیے۔ Blank Spaces کی جگہ X استعمال کیجیے۔

(5) Elliptic Curve Cryptography کو مثال کے ذریعہ تفصیل سے سمجھائیے۔

(6) Meet in the Middle Attack کسے کہتے ہیں اور یہ کیسے ہوتا ہے؟ Double Data Encryption الگورتھم کو تفصیل سے سمجھائیے۔

(7) E-mail Security کے بارے میں تفصیل سے بیان کیجیے۔

(8) SSL اور Transport Layer Security کے بارے میں وضاحت کیجیے۔

(9) مختلف قسم کے Viruses کیا ہیں؟ Active اور Passive Attack کے بیچ فرق واضح کیجیے۔

حصہ سوم

(10) مندرجہ ذیل کو مثال کے ذریعہ تفصیل سے سمجھائیے۔

Play Fiar Cipher (a) Rail Fence Cipher (b) PGP (c) Digital signature Standard (d)

(11) DES Algorithm کی کارکردگی کو خوبصورت خاکہ کے ذریعہ اس کے اہم مراحل (Steps) کو تفصیل سے سمجھائیے۔

(12) SHA-512 الگورتھم کی کارکردگی کو تفصیل سے بیان کیجیے۔ SHA-1, 256, 384, 512 الگورتھم کے 'Message Digest' Block Size, Message Size اور Word Size کو Tabular Form میں لکھیے۔

(13) Message Authenticatin Code (MAC) کسے کہتے ہیں سمجھائیے۔ HMAC کی کارکردگی کو خاکہ کے ذریعہ اس کے Steps کو تفصیل سے سمجھائیے۔اور HMAC کے نقصانات لکھیے۔

(14) (a) مختلف ملکوں میں Banks کے Network Connection Security اور Online Transaction کے لیے کیا Protocol 'Encryption Algorithm' Message Authentication اور کیا Key Exchange Algorithm استعمال کیا جاتے ہیں؟ Tabular Form میں لکھیے۔

(b) Kerberos اور x.509 پر مختصر نوٹ لکھیے۔

☆☆☆