

Maulana Azad National Urdu University
M.C.A V Semester Examination - December - 2018
Paper - MMCA503PCT : Crptography & Network Security

پرچہ : کرپٹوگرافی اینڈ نیٹ ورک سیکورٹی

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 اشارہ 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 دو سو (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

(1) سوال

- (i) Caesar Cipher کی مثال ہے۔

Mono-alphabetic Cipher (b)	Poly-alphabetic Cipher (a)
Pri-alphabetic Cipher (d)	Multi-alphabetic Cipher (c)
- (ii) ان میں سے کون سا Algorithm ہے جو Asymmetric-key Cryptography میں استعمال نہیں ہوتا۔

Diffie-Hellman Algorithm (b)	RSA Algorithm (a)
Electronic Code Book Algorithm (c)	ان میں سے کوئی نہیں (d)
- (iii) Data Encryption Standard (DES) کیا ہے؟

Block Cipher (a)	Stream Cipher (b)	Bit Cipher (c)	ان میں سے کوئی نہیں (d)
------------------	-------------------	----------------	-------------------------
- (iv) ان میں سے کون سا Cryptographic Protocol ہے جو Secure HTTP Connection فراہم کرتا ہے؟

Stream Control Transmission Protocol (SCTP) (a)	Transport Layer Security (TSL) (b)	Explicit Congestion Notification (ECN) (c)	Resource Reservation Protocol (RRP) (d)
---	------------------------------------	--	---
- (v) MD5 سب سے (Fast) تیز ہے اور Message Digest بناتا ہے۔

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

- (vi) SET Authentication فراہم کرتا ہے۔
 Digital Certificate (b) Dual Signature (a)
 Payment's Private Key (d) Payments Public Key (c)
- (vii) Layers ان SSH کے درمیان رکھا جاتا ہے؟
 Applications & Presentation (b) Transport & Datalink (a)
 Application and Session (d) Application and Transport (c)
- (viii) Hellman اور Merkle نے Concept کو متعارف (Introduction) کروایا۔
 Meet is attack (b) Meet in the middle attack (a)
 Virus Attacks (d) Hijack (c)
- (ix) Blowfish Algorithm کی Maximum Size ہوتی ہے۔
 48 bytes (d) 56 bytes (c) 512 bits (b) 256 bits (a)
- (x) مندرجہ ذیل Text کو Caesar Cipher کے ذریعے Decipher کیجیے۔
 H Q F U B S W H G W H A W
 ENCRYPTED TEXT (b) ABANDONED LOCK (a)
 ENCRYPTED LOCK (d) ABANDONED TEXT (c)

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) Substitution Cipher اور Transposition 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 ذریعے Encrypt کیجیے۔ Blank Spaces کی جگہ X استعمال کیجیے۔
- (5) Elliptic Curve Cryptography کو مثال کے ذریعے تفصیل سے سمجھائیے۔
- (6) Meet in the Middle Attack کے 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) Transport Layer Security اور SSL 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۔
Digital signature Standard (d) PGP (c) Rail Fence Cipher (b) Play Fiar Cipher (a)
- (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) کے کہتے ہیں سمجھائیے۔ HMAC کی کارکردگی کو خاکہ کے ذریعہ اس کے Steps کو تفصیل سے سمجھائیے۔ اور HMAC کے نقصانات لکھیے۔
- (14) مختلف ملکوں میں Banks کے Network Connection Security اور Online Transaction کے لیے کیا Key Exchange Algorithm اور کیا Message Authentication 'Encryption Algorithm' Protocol استعمال کیا جاتے ہیں؟ Tabular Form میں لکھیے۔
(b) Kerberos اور x.509 پر مختصر نوٹ لکھیے۔

☆☆☆