Maulana Azad National Urdu University

B.Tech VIII Semester Examination, July 2023

Paper - BTCS837PET : Cryptography and Network Security

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 آٹھ سوالات ہیں، اور اس میں 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 پانچ 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 نمبر : 1

(i) DES ایک ..... طریقہ (Method) ہے جسے U.S Government نے Adopt کیا ہے؟

Symmetric Key (a) Asymmetric Key (b)

Either (a) or (b) (c) Neither (a) or (b) (d)

(ii) DES میں Initial اور Permuntation Block Final ہوتا ہے اور اس میں ..... Rounds ہوتے ہیں

14 (a) 15 (b) 16 (c) (d) ان میں سے کوئی نہیں

(iii) ECB اور CBC ..... Cipher ہیں

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

(iv) ..... Method میں دونوں Parties کو Onetime Session Key دی جاتی ہے

Diffie-Hellman (a) RSA (b) DES(c) AES (d)

(v) ..... Malware کا Fullform ..... ہے۔

Malfunctional Software (a) Multipurpose Software (b)

Malicious Software (c) Malfunctiong of Security (d)

(vi) ..... ایک Code Injecting Method ہے جو System کے Database یا Website پر کہا جاتا ہے۔

HTML Injection (a) SQL Injection (b)

Malicious Code Injection (c) XML Injectin (d

(vii) User Session کو Compromise کرنا جو User's Data کو Exploit کرتا ہے اور Malicious Activities اور User's Credential کو Misuse کرتا ہے اسے..... کہتے ہیں۔

(a) Session Hijacking (b) Session Fixation
(c) Cookie Stuffing (d) Session Spying

(viii) ایسا Attack جس میں Valid Request کو Website Answer نہیں کرتی اسے..... کہتے ہیں۔

(a) Smurfing (b) Denial of Service
(c) E-mail Bombing (d) Ping Storm

(ix) WTLS کا Fullform ..... ہے۔

(a) Wireless Transport Security Layer (b) Wireless Transfer System Layer
(c) Wireless Transfer Security Layer (d) Wireless Transport System Layer

(x) Elagamal Encryption System ..... ہے۔

(a) Asymmetric Key Encryption System (b) Asymmetric Key Encryption Algorithm
(c) Notion Encryption Algorithm (d) Block Cipher Method

حصہ دوم

(2) "PLAYFAIR EXAMPLE" کو Key سمجھتے ہوئے (I/J as Interchangeable) لیتے ہوئے دیے گئے Message کو Playfair کے ذریعہ Encrypt کیجیے۔

"Hide the gold in the tree Stump"

(3) DDOS Attack کی تعریف بیان کیجیے۔اس کو کیسے Detect اور Prevent کیا جاسکتا ہے؟

(4) Message Authentication Code کی وضاحت کیجیے۔Hashbased Message Authenticade Code کے نقصانات بیان کیجیے۔

(5) X.509 Digital Certificate Version 3 کے مختلف Fields کے بارے میں سمجھائیے۔

(6) ایک Organisation کے Security Framework قائم (establish) کرنے کے لیے ایک Firewall کیسے مدد کرتا ہے؟ سمجھائیے۔

(7) Man-in-the-middle Attack میں Diffie-Hellman Key Exchange کے ذریعہ Alice اور Bob ایک Secret Key استعمال کرتے ہیں x=13, g=17 اور جس میں Bob x as 3 لیتا ہے اور Bob y as 9 لیتا ہے۔ Tom جو کے ایک Intruder ہے وہ x کو اور y کو 6 لیتا ہے۔ Man-in-the-middle Attack کی کارکردگی بیان کیجیے۔

(8) TCP/IP Protocol Suite میں IP Layer کی Secruity بیان کیجیے۔

(9) مندرجہ ذیل پر مختصر نوٹ لکھیے۔

(a) Fermat's Theorem (b) Packet Sniffing

حصہ سوم

(10) Active اور Passive Attack کی وضاحت کیجیے کسی بھی دس(10) عام Cyber Attacks کے بارے میں لکھیے۔

(11) Public Key Cryptography کی وضاحت کیجیے۔ RSA Algorithm کو استعمال کرتے ہوئے Plain Text M=88 ہے q=11, p=17 اور اس کے Public Components = 7 ہے۔اس کا Encryption معلوم کریں۔

(12) مختلف قسم کے E-mail Protocols بیان کیجیے۔ E-mail Message میں پانچ Secruity Operations بیان کیجیے۔

(13) Message Digest کو مثال کے ذریعہ سمجھائیے اس کی Requirements بیان کیجیے۔ Working of MD5 کو تفصیل سے سمجھائیے۔

(14) مندرجہ ذیل پر تفصیلی نوٹ لکھیے۔

(a) PKIX Services

IDEA Algorithm

☆☆☆