Maulana Azad National Urdu University

M.Tech I Semester Examination - December - 2018

Paper - MTCS101PCT : Advanced Network Security

پرچہ : اڈوانس نٹ 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۔

689

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) ..... Attack جو Confidentality سے تعلق رکھتا ہے۔

(a) Interception (b) Fabrication (c) Modification (d) Intteruption

(ii) Secret Key Croptography ..... سے مترادف (Synonyms) ہے۔

(a) Symmetric Key Cryptography (b) Asymmetric Key Cryptography

(c) Private Key Cryptography (d) Quantum Cryptography

(iii) 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 (d) ان میں سے کوئی نہیں

(iv) 28 کا 53 Base 2 Modulo کا Discrete Logarithm ..... ہے۔

(a) 29 (b) 16 (c) 47 (d) 42

(v) ECC کا RSA کے مقابلہ اہم فوائد اس کا ..... میں Performance ہے۔

(a) Decryption for Large Key Sizes (b) Encryption & Decryption for Large Key Size

(c) Decryption Over All Key Sizes (d) ان میں سے کوئی نہیں

(vi) IBE کو ..... نے Propose کیا۔

Diffie-Hellman (a) Taher Elgamal (b) Adi Shamir (c) ان میں سے کوئی نہیں (d)

(vii) مندرجہ ذیل میں سے IBE کے لیے کون سا صحیح ہے۔

(a) A user has to communicate with the PKG each time he/she wishes to encrypt his/her message

(b) A user's public key is a function of his/her identity.

(c) A user's private key is a function of his/her identity

(d) a اور c دونوں

(viii) Digital Certificate ..... کو باندھتا ہے۔

A person's public key to his private key (a) A person's public key to his identity (b)

A person's private key to his identity (c) ان میں سے کوئی نہیں (d)

(ix) SSL کون سے Layer پہ Security فراہم کرتا ہے۔

Application (a) Transport (b) Network (c) Data Link (d)

(x) Payment Gateway کا کردار (Role) ..... ہے۔

Proxy to the merchant (a) A Government Regulator (b)

Proxy tot he bank card network (c) ان میں سے کوئی نہیں (d)

حصہ دوم

(2) Algorithm Modes کے بارے میں تفصیل سے سمجھایئے۔ Initialization Vector (IV) کسے کہتے ہیں؟

(3) AES Algorithm کے First Round کے لیے Subkey معلوم کیجیے۔ Key m کا Hexadecimal ..... ہے

41, 50, 47, 41, 41, 4b 4b 53 46 50 53 53 50, 41, 42, 58

(4) Elgamal Crypto System کے مندرجہ Components کے بارے میں سمجھایئے۔

Key Generation (a) Encryption (b) Decryption (c)

(5) اگر Merkle-Hellman Knapsack Cryptosystem استعمال کرتے ہوئے Bob کو اگر ایک Message {m=1100101} بھیجنا ہے اور مندرجہ Information دیا گیا ہو۔

Superincreasing tuple (b) : [7, 11, 19, 39, 79, 157, 313]

Modulus (N) = 800, Random integer (r) = 37

Encryption اور Decryption کو Step by Step سمجھایئے۔

6) Boneh-boyen IBE کے مختلف Components کو سمجھائیے۔

Key Generation (a) Encryption (b) Decryption (c)

(7) Digital Certificate کے مختلف Contents کیا ہے؟ CA اور RA کا کردار (Role) سمجھائیے۔

(8) Secure Socket Layer اور Secure Electronic Transaction کی وضاحت کیجیے۔

(9) TCP Sequence Number کیا ہے؟ XSS Attack کی وضاحت کیجیے۔

حصہ سوم

(10) 3-D Secure Protocol کو Diagram کے ذریعہ سمجھائیے یہ SSL سے کیسے مختلف ہے؟

(11) IDEA Algorithm کا Encryption اور Decryption معلوم کیجیے۔ Binary میں Key مندرجہ ذیل ہے۔

1100 0110 0011 0101 111 0111 0101 1010

(12) اگر Alice Base Point $G_A = (2,7)$ in E_{11} (1,6) اور Private Key $d_A=5$ کو Choose کرتا ہے۔
اگر Alice کو اپنے Plain Text کو Elliptic Curve پر Encrypt اور Decrypt کرنا ہے اور
Plain Text Point m = (3.5) دیا گیا ہے۔ اس Process کو Step by Step سمجھائیے۔

(13) Post Quantum Cryptography کے بارے میں بحث کیجیے۔ Mc Elice Cryptosystem کو مثال کے ذریعہ سمجھائیے۔

(14) مندرجہ ذیل پر مختصر نوٹ لکھیے۔

Session Hijacking (a) RDDOS (b)

Jamming (c) Sniffing (d)

☆☆☆