Maulana Azad National Urdu University

M.Tech II Semester Examination - May - 2018

PAPER - MTCS216PET : Applied Croptography

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۔ 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 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 : 1

(i) Monoalphabetic Cipher اور Polyolphabetic کے درمیان فرق بیان کریں۔

(ii) Stream Chiper اور Block Cipher کے درمیان فرق بیان کریں۔

(iii) One Way Functions کو بیان کریں۔

(iv) Steganography اور Cryptography میں فرق بیان کریں۔

(v) Zero Knowledge Proofs کے Applications بیان کریں۔

(vi) One Time Pad کی وضاحت کریں۔

(vii) Discret Log Problem کی وضاحت کیجیے۔

(viii) $? = 2^{26} \bmod 9$

(ix) Group Properties بیان کریں۔

(x) مختلف Attack Models بیان کریں۔

حصہ دوم

2. $1 \le a \le 10$ کے لیے $a^{-1} \bmod 11$ Trial and Error کے ذریعہ سے حاصل کریں۔

3. Vigenere Cipher کی وضاحت کریں۔ذیل کے Message کا Cipher Text حاصل کریں۔ Vigenere Cipher کے ذریعہ سے

msg:- this crypto system

keyword:- CIPHER

4. Digital Signatures کو بیان کیجیے۔

5. Message Authentication Codes کو سمجھائیے۔

6. Multi Party Cryptographic Protocol کی وضاحت کیجیے۔

7. Side Channel Attacks سے کیا مراد ہے؟

8. DNA Cryptography کی وضاحت کیجیے۔

9 Quantum Cryptography کی وضاحت کیجیے۔

حصہ سوم

10. Public Key Crypto System کی وضاحت کیجیے۔Elgamal Encryption Scheme کو مثال کے ذریعے سمجھائیے۔

11. Diffe-Hellman Key Exchange کی الگورتھم کو مثال کے ذریعہ سمجھائیے۔

12. Advanced Encryption Standard کی وضاحت کیجیے۔

13. Elliptic Curve Cryptography کی وضاحت کریں۔اس میں Point Addition اور Point Doubling کیسے کرتے ہیں؟

14. ذیل پر Short Notes لکھیں۔

(a (4M) Cryptanalysis

(b (3M) Remote User Authentication

(c (3M) Vernam Cipher

☆☆☆