Maulana Azad National Urdu University

M.Tech II Semester Examination - May - 2019

PAPER - MTCS206PET : 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) Cryptography اور Cyptoanalysis کے درمیان فرق بیان کریں۔

(ii) Monoalphabetic Ciphers کے Names بیان کریں۔

(iii) Polyalphabetic Ciphers کے Names بیان کریں۔

(iv) Oneway Functions کی وضاحت کریں۔

(v) Common Attack Models کے Names بیان کریں۔

(vi) Ring Properties بیان کریں۔

(vii) Diffie Hellman Key Exchange کا کیا مقصد ہے؟

(viii) Symmetric Key Crptography اور Asymmetric Key Cryptography کے درمیان فرق بیان کریں۔

(ix) Quanum Cryptography کے فوائد بیان کریں۔

(x) Zero Knowledge Proof کے Properties بیان کریں۔

حصہ دوم

2. Stream Ciphers کی وضاحت کریں اور اسے تفصیل سے سمجھائیے۔

3. Steganography تفصیل سے بیان کیجیے۔
4. Multiparty Cyrptography مثال کے ذریعہ سمجھائیے۔
5. Differential Cryptoanalysis کو تفصیل سے لکھیے۔
6. Digital Signatures سمجھائیے۔
7. RSA Algorithm مثال کے ذریعہ بیان کیجیے۔
8. Affine Cipher مثال کے ذریعہ سمجھائیے۔
9 Privacy Mechanism تفصیل سے بیان کیجیے۔

حصہ سوم

10. A&S Algorithm تفصیل سے بیان کرے۔
11. Kerberoes کیا ہے؟ تفصیل سے وضاحت کرے۔
12. Message Authentication Codes کو سمجھائیے۔
13. مختلف Cryptoanalysis تفصیل سے لکھیے۔
14. مندرجہ ذیل پر مختصر نوٹ لکھیں۔

(a) Pseudo random Numbers

(b) Vigenere Cipher

(c) Secure Hash Algorithm

(d) DNA Cryptography

☆☆☆