مولانا آزاد نیشنل اردو یونیورسٹی

Department of CS&IT,MANUU

End Semester Examination April 2026

Programme:B.Tech

پروگرام B.Tech. :

Semester:8th

سمیسٹر: 8

Title & Paper Code:Crytography&Network Security(BTCS 837PET)

Time:3 Hours Maximum Marks 70 جملہ نشانات:

ہدایات:

یہ پرچہ تین حصوں پر مشتمل ہے: حصہ اول، حصہ دوم، حصہ سوم. ہر جواب کے لئے لفظوں کی تعداد شارۃً ہے. تمام حصوں سے سوالوں کا جواب دینا لازمی ہے.

1. حصہ اول میں 10 لازمی سوالات ہیں جو کہ مختصر جواب والے سوالات ہیں. ہر سوال کا جواب دینا لازمی ہے ہر سوال کے لئے 1 نمبر مختص ہے .

(10Marks =1 x 10)

2. حصہ دوم میں 8 سوالات ہیں، اس میں 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 لئے 6 نمبرات مختص ہیں (30Marks=6 x 5)

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 لئے 10 نمبرات مختص ہیں.

(10 x 3=30Marks)

حصہ اول

سوال (1) Digital Signature کسے کہتے ہیں؟

A) A handwritten signature B) A method to ensure authentication and integrity

C) A password D) A firewall

(ii). Hashing کسے کہتے ہیں؟

A) Reversible encryption B) Converting data into a fixed-length value

C) Data transmission D) Data storage

(III) Malware _____ کو_ے کہتے ہیں کو (B

A)Safe software B) Malicious software designed to harm systems

C) Encryption algorithm D) Network protocol

(IV) Triple DES (3DES) میں _____ key استعمال کیا جاتا ہے

A) 56-bit B) 112-bit C) 168-bit D) 256-bit

(V). کون سا attack حملہ Two Parties کے درمیان Communication کو Intercept کرتا ہے؟

A) Phishing B) Man-in-the-Middle C) DoS D) Brute force

(VI) zero-day attack----------ہے

A) Attack with no impact B) Attack exploiting unknown vulnerabilities

C) Attack on zero data D) Replay attack

(VII) RC4 Algorithm میں _____ key استعمال کیا جاتا ہے

A) Fixed 64-bit B) Variable (40 to 2048-bit)

C) 56-bit D) 128-bit only

(VIII). کونسا حملہ AI attack سے تیار کر Fake videos یا Audios کا استعمال کرتا ہے؟

SQL Injection B) Deepfake attack C) Replay attack D) Buffer overflow (A

(IX). کون سا Modern Attack ان پٹ ڈیٹا (Input Data) کو Manipulate کر کے Machine learning کو نشانہ بناتا ہے؟

A) Phishing B) Adversarial attack C) DoS D) MITM

(X). WLAN Scanner and WLAN Sniffers کسے کہتے ہیں؟

حصہ 2

سوال 2. دیے گئے Playfair Cipher problem کو حل کریں

Encrypt the message ""CYBER ATTACK PREVENTION"" using the keyword "DEFENSE"".

سوال3 Substitution Cipher اور Transposition Cipher کو Define اور Explain کریں؟ Hill cipher کے بارے میں example کے ساتھ تفصیل سے وضاحت کریں

سوال 4. Idea Algorithm کے بارے میں Figure کے ساتھ تفصیل سے وضاحت کریں؟

5سوال SQL Injection کی تفصیل سے وضاحت کریں؟

How can SQL Injection be used to bypass authentication mechanisms?

Illustrate your answer with a suitable example query and suggest effective prevention techniques.?

سوال6. Diffie Hellman Key-Exchange/Agreement Algorithm کو ایک Figure کے ساتھ اور ایک Example کے ساتھ بیان کریں

سوال7. Digital Signature کیا ہے؟ یہ Authentication اور Integrity کو کس طرح یقینی بناتی ہے؟ Digital Certificate کی تعریف کریں اور اس کا اور format بیان کریں۔

سوال8. Session Hijacking کی تفصیل سے وضاحت کریں؟

SSL, SHTTP, Secure Electronic Transaction (SET) پر مختصر نوٹ لکھیں۔

9 سوال درج ذیل پر مختصر نوٹ لکھیں۔

A.Different types of Packet Analysis Tools B. Intrusion Detection System

حصہ سوم

سوال 10. Figure کے ساتھ DES Algorithm کے کام کے بارے میں تفصیل سے وضاحت کریں؟ Double DES Algorithm اور Triple DES Algorithm کی بھی وضاحت کریں؟

سوال11. Message Authentication Code کے بارے میں تفصیل سے وضاحت کریں- MD5 Algorithm کے Steps اور Figure کے ساتھ اس کی Working وضاحت کریں؟

سوال12. IEEE802.11 protocol architechture کے بارے میں تفصیل سے وضاحت کریں اس کے Components اور services کی وضاحت کریں؟ Cookies کسے کہتے ہیں؟ Cookies damage privacy وضاحت کریں؟

سوال13. RSA Algorithm کی وضاحت کی کریں۔ ایک Secure communication system ڈیزائن کریں

Using

RSA for key exchange

AES for data encryption

سوال 14. درج ذیل پر مختصر نوٹ لکھیں

A company's system was compromised because of poor authentication practices.

Propose a multi-layered security framework using

- Cryptographic techniques
- Strong authentication methods
- Network security controls

Explain how each component helps in preventing such attacks.