مولانا آزاد نیشنل اردو یونیورسٹی

Department of CS&IT,MANUU

End Semester Examination April 2026

Programme:MCA

پروگرام MCA:

Semester:2nd

2 سیمسٹر: _____

_____

Title & Paper Code:Crytography&Cyber Security(MMCA213PET)

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. (10x 1= 10Marks)

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 (5x 6=30Marks)

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)

حصّہ اول

سوال(1) کس Key Size کو ہم Symmetric Encryption کے لیے آج غیر محفوظ سمجھا جاتا ہے؟

A) 128-bit B) 192-bit C) 256-bit D) 56-bit

(ii). Elliptic Curve Cryptography (ECC) RSA سے ملتی جلتی Security حاصل کرتی ہے لیکن اس کے ساتھ:

A) Larger key sizes B) Smaller key sizes C) Same key sizes D) No keys

(iii). جدید RSA Encryption کے لیے عام طور پر کون سا Key Size تجویز (Recommend) کیا جاتا ہے؟

A) 512 bits B) 1024 bits C) 2048 bits D) 256 bits

(iv). کون سی Vulnerability حملہ آوروں (Attackers) کو Victim کے Browser میں Scripts کو Execute کرنے کی اجازت دیتی ہے؟

A) SQL Injection B) Cross-Site Scripting (XSS) C) CSRF D) DoS

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

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

(VI) Given:p=3,q=11,e=3,M=4

What is the ciphertext?

A) 9 B) 16 C) 4 D) 64

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

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

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

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

(IX). Secure Key Exchange کے لیے کون سا Algorithm استعمال کیا جاتا ہے؟

A) AES B) MD5 C) Diffie-Hellman D) DES

(X). Steganography کسے کہتے ہیں؟

حصہ 2

سوال 2 گئے دیئے Playfair Cipher problem کریں حلکو

Encrypt the message **"SECURE DATA TRANSFER SYSTEM"** using the keyword **"CYBER".**

سوال3. مثالوں کے ساتھ Substitution Cipher اور Transposition Cipher کو Define اور Explain کریں؟

سوال 4. Elliptic Curve Cryptographic کے بارے میں Figure کے ساتھ تفصیل سے وضاحت کریں؟

سوال5. درج ذیل پر مختصر نوٹ لکھیں۔

RC4 Algorihm

MD5 Algorithm

سوال 6.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 مقصد بیان کریں۔

سوال8. public key infrastructure کی تفصیل سے وضاحت کریں؟

Components

Working of PKI with a suitable example

Applications and advantages of PKI in secure communication

سوال 9 درج ذیل پر مختصر نوٹ لکھیں۔

A company experiences a data breach due to weak authentication.

Suggest a complete security solution using:

Cryptography

Authentication

Network security

حصّہ سوم

سوال10. 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.Elgamal Encryption Algorithm ، اس کے Components اور Figure کے ساتھ اس کی Working وضاحت کریں؟

سوال12.IP SecurtyArchitecture کے بارے میں تفصیل سے وضاحت کریں_اس کی Features، Protocol اور Packet Format کی وضاحت کریں؟

1. Public Key Infrastructure Model کے تصور کو واضح کریں-Working of PKI (Step-by-Step) with figure

سوال3

سوال14. RSA Algorithm اینکی وضاحت کی کریں۔ Secure communication system ۔ڈیزائن Using

RSA for key exchange

AES for data encryption

****