Roll No. .....

Question Booklet Number

O. M. R. Serial No.

M. A./M. Sc. (Fourth Semester)
(NEP) EXAMINATION, 2025-26
MATHEMATICS
(Cryptography) (Elective)

Paper Code							
B	0	3	1	0	1	2	T

Questions Booklet Series
B

Time : 1:30 Hours] [*Maximum Marks : 75*

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.

2. The booklet contains 100 questions. Examinee is required to answer 75 questions in the OMR Answer-Sheet provided and not in the question booklet. All questions carry equal marks.

3. Examine the Booklet and the OMR Answer-Sheet very carefully before you proceed. Faulty question booklet due to missing or duplicate pages/questions or having any other discrepancy should be got immediately replaced.

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।

2. प्रश्न-पुस्तिका में 100 प्रश्न हैं। परीक्षार्थी को 75 प्रश्नों को केवल दी गई OMR आन्सर-शीट पर ही हल करना है, प्रश्न-पुस्तिका पर नहीं। सभी प्रश्नों के अंक समान हैं।

3. प्रश्नों के उत्तर अंकित करने से पूर्व प्रश्न-पुस्तिका तथा OMR आन्सर-शीट को सावधानीपूर्वक देख लें। दोषपूर्ण प्रश्न-पुस्तिका जिसमें कुछ भाग छपने से छूट गए हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, तो उसे तुरन्त बदल लें।

(Remaining instructions on the last page) **(शेष निर्देश अन्तिम पृष्ठ पर)**

(Only for Rough Work)

1. What type of structure does AES use for transformations during encryption ?
   (A) Fistal Network
   (B) Digital Signature Algorithm
   (C) Cipher Block Chaining
   (D) Substitution – Permutation Network

2. What is the application of digital signature ?
   (A) To encrypt the message
   (B) To decerypt the message
   (C) To authenticate the user
   (D) Repudiation by user

3. What is Data Encryption Standard ?
   (A) Block cipher
   (B) Stream Cipher
   (C) Bit Cipher
   (D) None of the above

4. Which of the following is used in Data Encryption Standard for operating ?
   (A) Cipher Feedback Mode
   (B) Cipher Block Chaining
   (C) Electronic Code Book
   (D) Output Feedback Mode

5. Which of the following is NOT a stage in every round of Advanced Encryption Standard ?
   (A) Sub Bytes
   (B) Shift Rows
   (C) Mix columns
   (D) Permutation

6. Advanced Encryption Standard replaced which of the following ?
   (A) Data Encryption Standard
   (B) Blowfish
   (C) Diffie-Hellman key exchange
   (D) None of the above

7. Which of the following cannot be chosen as a key in the Caesar cipher ?
   (A) An integer
   (B) A string
   (C) An alphabet
   (D) None of the above

8. Which of the following is a block cipher ?
   (A) Caesar cipher
   (B) Vernam cipher
   (C) Playfair cipher
   (D) None of the above

9. How stream cipher encrypts data ?
   (A) Block by block
   (B) Bit by bit or byte by byte
   (C) Character by character
   (D) Word by word

10. Which operation is commonly used in stream cipher encryption ?
   (A) AND
   (B) OR
   (C) XOR
   (D) None of the above

11. Which of the following is the meaning of "Crypt" ?

(A) Hidden

(B) Writing

(C) Copied

(D) Both (A) and (B)

12. Which of the following is the first step of Advanced Encryption Standard ?

(A) Sub Byte

(B) Shift Rows

(C) Mix columns

(D) Add Round keys

13. Which of the following is false for Electronic Code Book made of operation ?

(i) The plain text is broken into blocks of size 128 bytes

(ii) Books can be swapped, repeated, replaced without recipient noticing.

(iii) Good for short data.

(iv) Encryption of each block is done separately using a randomly generated key for each block.

Codes :

(A) Only (i)

(B) (ii) and (iii)

(C) (i) and (iv)

(D) (i), (ii) and (iv)

14. In which networking layer does Diffie-Hellman key provides forward secrecy ?

(A) Application type layer

(B) Transport type layer

(C) Session type layer

(D) Basic type layer

15. What does a transposition cipher rearrange ?

(A) Characters in the plaintext

(B) Bits in a byte

(C) Encryption keys

(D) MAC addresses

16. Upon what the strength of an encryption algorithm depends ?

(A) Key length and complexity

(B) Packet size

(C) MAC address filtering

(D) None of the above

17. Which belongs to key feature of Block-chain ?

(A) MAC address anonymity

(B) High speed encryption

(C) Decentralized, tamper-resistant records

(D) None of the above

18. In public key cryptography, data encrypted with a public key can be decrypted by ……. .
    (A) The corresponding private key
    (B) Another public key
    (C) A symmetric key
    (D) A hash function

19. Which are the examples of asymmetric key algorithm ?
    (A) MD 4, MD 5 and MD 6
    (B) RC 4, RC 5 and RC 6
    (C) AES, DES and Triple DES
    (D) Diffie-Hellman, RSA and El – Gamal

20. What is required by key management practice ?
    (A) Labeling keys so that they are not lost or stolen.
    (B) Choosing a key that is extremely random and the algorithm should use the full range of the key – space
    (C) Returning the key to the certificate Authority after it has completed its lifetime.
    (D) None of the above

21. Which hash value is encrypted by the sender's private key ?
    (A) Digital Signature
    (B) Advanced Encryption Standard
    (C) Data Encryption Standard
    (D) Triple DES

22. Which of the following is a major vulnerability of the basic Diffie-Hellman key exchange ?
    (A) Man-in-the-Middle attack
    (B) Replay attack
    (C) Brute-force of AES key
    (D) Dictionary attack

23. How many bytes of the secret key is generated using Diffie-Hellman encryption/decryption scheme ?
    (A) 256
    (B) 871
    (C) 962
    (D) 1024

24. In which of the following, encryption is slower than decryption ?
    (A) Elliptic curve cryptography
    (B) Parabolic curve cryptography
    (C) Symmetric cryptography
    (D) Asymmetric cryptography

25. How many combinations of keys can be constructed from a 72 cipher text stream cipher ?
    (A) 4271
    (B) 7345
    (C) 3291
    (D) 2556

26. For what RSA encryption is primarily used ?
    (A) Symmetric key encryption
    (B) Asymmetric key encryption
    (C) Data compression
    (D) Network routing

27. In RSA, which key is publicly shared ?

(A) Private key
(B) Secret key
(C) Public key
(D) Master key

28. What type of mathematical problem is RSA based on ?

(A) Matrix inversion
(B) Elliptic curves
(C) Integer factorization
(D) Hash collisions

29. On which fundamental mathematical problem the El-Gamal system is based ?

(A) Integer factorization
(B) Discrete logarithm problem
(C) Knapsack problem
(D) Quadratic residues

30. What operations on encrypted data does El-Gamal support ?

(A) Homomorphic multiplication
(B) Hashing
(C) Symmetric encryption
(D) Asymmetric encryption

31. Elliptic curve cryptography rely on which of the following problems for its security ?

(A) Elliptic curve discrete logarithm problem
(B) Symmetric key distribrition problem
(C) Prime number generation problem
(D) Integer factorization problem

32. How is public key generated in the Elliptic curve cryptography key generation process ?

(A) By hashing the private key
(B) By squaring the private key
(C) By adding the private key to the generator point
(D) By multiplying the private key with a generator point

33. What is the primary goal of information security ?

(A) Protect software updates
(B) Protect information and its critical elements
(C) Limit internet access
(D) Increase data traffic

34. Which one of these is NOT a security service category ?

(A) Confidentiality
(B) Authentication
(C) Encryption
(D) Integrity

35. Which attack destroys or disables system assets ?

(A) Interception
(B) Fabrication
(C) Interruption
(D) Modification

36. Which security principle ensures that data is accessible and usable by authorized users when needed ?

(A) Availability

(B) Confidentiality

(C) Integrity

(D) Authenticity

37. A Denial of service attack directly targets which of the following ?

(A) Confidentiality

(B) Integrity

(C) Accountability

(D) Availability

38. Which one is responsible for monitoring and filtering incoming / outgoing network traffic ?

(A) Database

(B) Firewall

(C) Router

(D) Switch

39. Knowing the password of a user for hacking is called …….. .

(A) Spoofing

(B) Sneaking

(C) Cyber stalking

(D) Spamming

40. What is the main purpose of a cryptographic hash function ?

(A) To compress data for storage efficiency

(B) To convert data into a unique string of text

(C) To encrypt data for secure transmission

(D) To create a backup of data

41. How does hashing differ from encryption ?

(A) Hashing cannot be reversed, encryption can be

(B) Both hashing and encryption can be reversed

(C) Hashing requires a key, encryption does not

(D) Hashing is slower than encryption

42. In SHA – 512, the message is divided into blocks of size …….. bits for the hash computation.

(A) 256

(B) 512

(C) 1024

(D) 1248

43. Which of the following is/are offered by the Hash functions ?

(A) Authentication

(B) Non repudiation

(C) Data

(D) All of the above

44. What is the output size of the SHA – 3 hash function family with a security level of 256 bits ?

(A) 128 bits

(B) 256 bits

(C) 512 bits

(D) 1024 bits

45. What is formed by taking the hash of the massage and encrypting the message with the creator's private key ?

(A) Timestamp

(B) Message digest

(C) Hash code

(D) Digital signature

46. Which technology is used in digital signatures ?

(A) Public key Infrastructure

(B) Biometric

(C) Blockchain

(D) OTP Verification

47. In Elgamal signature, which of the following is required during signature generation ?

(A) Prime number

(B) Private key

(C) Random number

(D) All of the above

48. In the Digital Signature Algorithm, what is the purpose of the hash function ?

(A) To encrypt the entire message

(B) To generate a fixed-size message digest for signing

(C) To compress the message for faster transmission

(D) To generate the public key

49. What does "Non-Repudiation" mean in the context of digital signatures ?

(A) The message is kept secret.

(B) The receiver cannot change the message

(C) The sender cannot deny sending the message

(D) The signature is easy to copy.

50. What is the role of a hash function in creating a digital signature ?

(A) To ensure that the message is encrypted

(B) To provide non-repudiation

(C) To produce a unique fingerprint of the message

(D) To manage the keys

51. Which term is also used for a cryptosystem ?

(A) Cipher System
(B) Operating System
(C) Database System
(D) Communication System

52. What is the primary goal of cryptosystem ?

(A) Confidentiality
(B) Integrity
(C) Authentication
(D) All of the above

53. Which type of cryptosystem uses the same key for both encryption and decryption ?

(A) Public key
(B) Asymmetric key
(C) Symmetric key
(D) Hashing

54. Which type of cryptosystem uses both public and private keys ?

(A) Asymmetric key
(B) Symmetric key
(C) Public key
(D) None of the above

55. What is "plaintext" in cryptosystem ?

(A) Encrypted data
(B) Unreadable data
(C) Original, readable message
(D) None of the above

56. What is the preferred way of encryption ?

(A) Secret key
(B) Key distribution center
(C) Symmetric key
(D) Public key encryption

57. What is the other name of symmetric encryption ?

(A) Public key encryption
(B) Asymmetric encryption
(C) Conventional encryption
(D) Hybrid encryption

58. Which of the following is not a type of symmetric key cryptography ?

(A) Diffie-Hellman cipher
(B) Playfair cipher
(C) Caesar cipher
(D) All of the above

59. What is the main requirement for secure communication in a symmetric cipher model ?

(A) The algorithm must be secret
(B) The key must be kept secret and shared by both parties
(C) The cipher text must be public
(D) All of the above

60. In a symmetric cipher system, if N users want to communicate with each other, how many secret keys are required ?

(A) N

(B) 2 N

(C) N (N – 1)

(D) N (N –1)/2

61. In a cipher, what is "avalanche effect" ?

(A) A small change in plaintext or key results in a large change in cipher text.

(B) A large amount of cipher text is produced.

(C) A small change in cipher text changes only one bit of plaintext.

(D) None of the above

62. What is the major problem in the symmetric cipher model ?

(A) Data compression

(B) Key distribution

(C) File storage

(D) Size of the message

63. The receiver converts cipher text back to plaintext using …… .

(A) Encryption

(B) Decryption with the same key

(C) Compression

(D) Encoding

64. What is data encryption standard ?

(A) Block cipher

(B) Stream cipher

(C) Bit cipher

(D) None of the above

65. What is the value of 3^{51} mod 5 ?

(A) 1

(B) 2

(C) 3

(D) 4

66. What is the impact of compromising the key in a cryptographic system ?

(A) Only the specific data encrypted with that key is affected.

(B) The cipher becomes stronger against attacks.

(C) Access to the data is permanently revoked.

(D) The entire system becomes vulnerable.

67. Which type of attack is NOT associated with symmetric ciphers ?

(A) Phishing attack

(B) Known – plaintext attack

(C) Brute – force attack

(D) None of the above

68. What are the two basic building blocks of all encryption techniques ?

(A) Addition and multiplication

(B) Alphabetic and numeric

(C) Substitution and transposition

(D) Encoding and decoding

69. Which technique map plaintext elements into cipher text elements ?

(A) Transposition

(B) Substitution

(C) Symmetric

(D) Traditional

70. What is the simplest transposition cipher mentioned in the text ?

(A) Rail fence

(B) Playfair cipher

(C) Columnar transposition

(D) Row transposition

71. What is the general Caesar algorithm for encryption in the Caesar cipher ?

(A) $C = E(p) \bmod 26$

(B) $C = E(p) \times 26$

(C) $C = E(p) + 3$

(D) $C = E(p) - 3$

72. What is the encryption rule for Playfair cipher when plaintext letters fall in the same row of the matrix ?

(A) Replaced by the letter to the above

(B) Replaced by the letter to the below

(C) Replaced by the letter to the left

(D) Replaced by the letter to the right

73. How is encrypted message read in the rail fence cipher ?

(A) Column by column

(B) Row by row

(C) Diagonal by diagonal

(D) All of the above

74. Which technique is used for deciphering a message without any knowledge of the enciphering details ?

(A) Blind deciphering

(B) Steganography

(C) Cryptanalysis

(D) Transposition

75. Who introduced the concepts of diffusion and confusion in cryptography ?

(A) Alan Turing

(B) Claude Shannon

(C) Whitfield Diffie

(D) Martin Hellman

76. What is the main goal of diffusion ?

(A) Make encryption faster

(B) Hide the relationship between plaintext and ciphertext

(C) Spread the influence of a single plaintext symbol over many ciphertext symbols

(D) Reduce key length

77. Which cryptographic technique mainly provides confusion ?

(A) Substitution

(B) Transposition

(C) Permutation

(D) Encoding

78. What is the block size of the Data Encryption Standard ?

(A) 64 bits

(B) 32 bits

(C) 56 bits

(D) 48 bits

79. How many tables of Substitution Boxes does DES use ?

(A) 32 tables

(B) 16 tables

(C) 8 tables

(D) 4 tables

80. What type of attack have been successful against DE ?

(A) Differential Cryptoanalysis

(B) Linear Cryptanalysis

(C) Brute-force attacks

(D) Exhaustive key search

81. What properties does DES satisfy as a block cipher ?

(A) Symmetry and Asymmetry

(B) Linearity and Non–linearity

(C) Confusion and Diffusion

(D) Avalanche effect and completeness

82. Find the remainder when $f(x) = x^4 - 2x^3 + x^2 - 3x + 4$ is divided by $(x - 3)$?

(A) 31

(B) 8

(C) – 14

(D) – 5

83. Which is the factor of $f(x) = x^3 - 6x^2 + 11x - 6$?

(A) $x = -2$

(B) $x = 3$

(C) $x = 4$

(D) $x = 5$

84. In cryptography, why is modular addition important ?

(A) It ensures result within a fixed range, preventing overflow.

(B) It makes computations slower for security.

(C) It only works for prim numbers.

(D) None of the above

85. Which cryptographic protocol uses modular exponentiation for secure key exchange ?

(A) AES

(B) Diffie-Hellman

(C) SHA – 256

(D) Quick Sort

86. Find the value of $(2^{10} + 3^5)$ mod 7 ?

(A) 6

(B) 5

(C) 1

(D) 0

87. What is the correct definition of the finite field GF(p) ?

(A) Real numbers between 0 and p

(B) Polynomials of degree less than p

(C) Integers [0, 1, …., p – 1] under modulo p arithmetic

(D) Integers [1, 2 ….., p] under multiplication

88. Choose the correct answer, if A(x) and B(x) are added in GF(2^n).

(A) A(x) – B(x)

(B) (mod A(x)) B(x)

(C) A(x) (mod B(x))

(D) A(x) + B(x) (mod n)

89. If p is a prime number and a is an integer not divisible by p, then which one is correct according to Fermat's Little Theorem ?

(A) $a^p \equiv 1 \pmod{p}$

(B) $a^{p-1} \equiv 1 \pmod{p}$

(C) $a^{p+1} \equiv 1 \pmod{p}$

(D) $a^{p-1} \equiv 0 \pmod{p}$

90. Fermat's Little Theorem requires which of the following conditions ?

(A) a is prime

(B) p is composite

(C) p is prime and g c d (a, p) = 1

(D) a and p both are prime

91. Which one is the general form of Fermat's Little theorem that works even if p divides a ?

(A) $a^p \equiv 1 \pmod{p}$

(B) $a^p \equiv a \pmod{p}$

(C) $a^{p-1} \equiv a \pmod{p}$

(D) $a^{p+1} \equiv a \pmod{p}$

92. Which statement stands for Euler's Theorem ?

(A) $a^n \equiv 1 \pmod{\phi(n)}$

(B) $a^{\phi(n)} \equiv \phi(n) \pmod{n}$

(C) $a^{\phi(n)} \equiv 1 \pmod{n}$

(D) $a^{\phi(n)} \equiv a \pmod{n}$

93. Euler's Theorem is a generalization of which theorem ?

(A) Wilson's Theorem

(B) Chinese Remainder Theorem

(C) Prime Number Theorem

(D) Fermat's Little Theorem

94. What is the main idea of the Chinese Remainder Theorem ?

(A) Solving quadratic equations

(B) Factoring large numbers

(C) Working with irrational numbers

(D) Solving a system of congruence's with co-prime moduli

95. In Chinese Remainder Theorem, if $147 \equiv 3 \pmod{R}$, find the largest possible value of R.

(A) 150

(B) 144

(C) 140

(D) 48

96. Which algorithm is commonly used to find modular inverse in Chinese Remainder Theorem ?

(A) Extended Euclidean Algorithm

(B) Quick Sort

(C) Binary Search

(D) None of the above

97. In Chinese Remainder Theorem, what is the solution of congruence relation $2x \equiv 1 \pmod{7}$.

(A) 4

(B) 3

(C) 2

(D) 1

98. In cryptography, the computation of the discrete logarithm forms the basis of which cryptographic system ?

(A) Symmetric cryptography

(B) Asymmetric cryptography

(C) Diffie-Hellman key exchange

(D) Secret key cryptography

99. Using discrete logarithm, solve $2^{x+3} = 5^{x+2}$ for x.

(A) ln (24/8)

(B) ln (25/8) / ln (2/5)

(C) ln (32 / 5) / ln (2/3)

(D) ln (3/25)

100. What is the block size used in the Advanced Encryption Standard ?

(A) 64 bits

(B) 128 bits

(C) 256 bits

(D) 512 bits

(Only for Rough Work)

4. Four alternative answers are mentioned for each question as—A, B, C & D in the booklet. The candidate has to choose the correct answer and mark the same in the OMR Answer-Sheet as per the direction :

Example :

Question :

Q. 1 (A) ● (C) (D)
Q. 2 (A) (B) ● (D)
Q. 3 (A) ● (C) (D)

Illegible answers with cutting and over-writing or half filled circle will be cancelled.

5. Each question carries equal marks. Marks will be awarded according to the number of correct answers you have.
6. All answers are to be given on OMR Answer Sheet only. Answers given anywhere other than the place specified in the answer sheet will not be considered valid.
7. Before writing anything on the OMR Answer Sheet, all the instructions given in it should be read carefully.
8. After the completion of the examination candidates should leave the examination hall only after providing their OMR Answer Sheet to the invigilator. Candidate can carry their Question Booklet.
9. There will be no negative marking.
10. Rough work, if any, should be done on the blank pages provided for the purpose in the booklet.
11. To bring and use of log-book, calculator, pager and cellular phone in examination hall is prohibited.
12. In case of any difference found in English and Hindi version of the question, the English version of the question will be held authentic.

Impt. : On opening the question booklet, first check that all the pages of the question booklet are printed properly. If there is any discrepancy in the question Booklet, then after showing it to the invigilator, get another question Booklet of the same series.

4. प्रश्न-पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर—A, B, C एवं D हैं। परीक्षार्थी को उन चारों विकल्पों में से सही उत्तर छाँटना है। उत्तर को OMR आन्सर-शीट में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

उदाहरण :

प्रश्न :

प्रश्न 1 (A) ● (C) (D)
प्रश्न 2 (A) (B) ● (D)
प्रश्न 3 (A) ● (C) (D)

अपठनीय उत्तर या ऐसे उत्तर जिन्हें काटा या बदला गया है, या गोले में आधा भरकर दिया गया, उन्हें निरस्त कर दिया जाएगा।

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।
6. सभी उत्तर केवल ओ. एम. आर. उत्तर-पत्रक (OMR Answer Sheet) पर ही दिये जाने हैं। उत्तर-पत्रक में निर्धारित स्थान के अलावा अन्यत्र कहीं पर दिया गया उत्तर मान्य नहीं होगा।
7. ओ. एम. आर. उत्तर-पत्रक (OMR Answer Sheet) पर कुछ भी लिखने से पूर्व उसमें दिये गये सभी अनुदेशों को सावधानीपूर्वक पढ़ लिया जाये।
8. परीक्षा समाप्ति के उपरान्त परीक्षार्थी कक्ष निरीक्षक को अपनी OMR Answer Sheet उपलब्ध कराने के बाद ही परीक्षा कक्ष से प्रस्थान करें। परीक्षार्थी अपने साथ प्रश्न-पुस्तिका ले जा सकते हैं।
9. निगेटिव मार्किंग नहीं है।
10. कोई भी रफ कार्य, प्रश्न-पुस्तिका के अन्त में, रफ-कार्य के लिए दिए खाली पेज पर ही किया जाना चाहिए।
11. परीक्षा-कक्ष में लॉग-बुक, कैलकुलेटर, पेजर तथा सेल्युलर फोन ले जाना तथा उसका उपयोग करना वर्जित है।
12. प्रश्न के हिन्दी एवं अंग्रेजी रूपान्तरण में भिन्नता होने की दशा में प्रश्न का अंग्रेजी रूपान्तरण ही मान्य होगा।

महत्वपूर्ण : प्रश्नपुस्तिका खोलने पर प्रथमतः जाँच कर देख लें कि प्रश्न-पुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सिरीज की दूसरी प्रश्न-पुस्तिका प्राप्त कर लें।