Sl. No. : 10000065

DME1/16

Register Number

2016

Paper I

[Comprising Three Subjects]

(Degree Standard)

Time Allowed : 3 Hours] **[Maximum Marks : 300**

Read the following instructions carefully before you begin to answer the questions.

IMPORTANT INSTRUCTIONS

1. This Booklet has a cover (this page) which should not be opened till the invigilator gives signal to open it at the commencement of the examination. As soon as the signal is received you should tear the right side of the booklet cover carefully to open the booklet. Then proceed to answer the questions.
2. This Question Booklet contains 200 questions. Prior to attempting to answer the candidates are requested to check whether all the questions are there in series without any omission and ensure there are no blank pages in the question booklet. In case any defect in the Question Paper is noticed it shall be reported to the Invigilator within first 10 minutes.
3. Answer **all** questions. All questions carry equal marks.
4. You must write your Register Number in the space provided on the top right side of this page. Do not write anything else on the Question Booklet.
5. An Answer Sheet will be supplied to you separately by the Invigilator to mark the answers.
6. You will also encode your Register Number, Subject Code, Question Booklet Sl. No. etc. with Blue or Black ink Ball point pen in the space provided on the side 2 of the Answer Sheet. If you do not encode properly or fail to encode the above information, action will be taken as per commission's notification.
7. Each question comprises *four* responses (A), (B), (C) and (D). You are to select ONLY ONE correct response and mark in your Answer Sheet. In case you feel that there are more than one correct response, mark the response which you consider the best. In any case, choose ONLY ONE response for each question. Your total marks will depend on the number of correct responses marked by you in the Answer Sheet.
8. In the Answer Sheet there are **four** circles Ⓐ, Ⓑ, Ⓒ and Ⓓ against each question. To answer the questions you are to mark with Blue or Black ink Ball point pen ONLY ONE circle of your choice for each question. Select one response for each question in the Question Booklet and mark in the Answer Sheet. If you mark more than one answer for one question, the answer will be treated as wrong. *e.g.* If for any item, Ⓑ is the correct answer, you have to mark as follows :

   Ⓐ ● Ⓒ Ⓓ

9. You should not remove or tear off any sheet from this Question Booklet. You are not allowed to take this Question Booklet and the Answer Sheet out of the Examination Hall during the examination. After the examination is concluded, you must hand over your Answer Sheet to the Invigilator. You are allowed to take the Question Booklet with you only after the Examination is over.
10. The sheet before the last page of the Question Booklet can be used for Rough Work.
11. Failure to comply with any of the above instructions will render you liable to such action or penalty as the Commission may decide at their discretion.
12. Do not tick-mark or mark the answers in the Question booklet.

SEAL

▲

SPACE FOR ROUGH WORK

1. The reason for twisting the 2 wires together in a helical form in a twisted wire pair is that

(A) 2 parallel wires will act as an antenna and twisting them will cancel the antenna effect

(B) Twisting the wires is beautiful in shape

(C) Twisting increases the bandwidth

(D) Twisting increases the transmission rate

2. The drawback of class A address space is that

(A) the network id space is too large and host id space is too small

(B) the network id space is too small and host id space is too large

(C) it is suitable only for medium networks

(D) it is suitable only for small networks

3. The silly window syndrome can be solved by

(A) enabling the sender to send a few bytes periodically

(B) enabling the receiver to receive a few bytes

(C) preventing the sender from acknowledging data

(D) preventing the receiver from sending a window update for 1 byte

4. The reassembly of fragments of an IP datagram are reassembled in the destination host because

(A) The intermediate routers may further carry out fragmentation and also because these fragments may follow different paths

(B) ICMP in the intermediate routers will prevent reassembly

(C) Reassembly at intermediate routers will make the routers to crash

(D) Congestion may be occuring at the host machines

5. Circuit switching is inefficient for data traffic because

(A) data traffic is often bursty and hence bandwidth reserved will be wasted

(B) data traffic is smooth and requires a very large bandwidth

(C) various time delays are involved in circuit switching

(D) circuit switching equipments are complex

6. Consider an IP packet transferred from Host 1 to Host 2 where both are in same LAN but the packet passes through different intermediate LANs is called

(A) Forwarding
(B) Tunnelling
(C) Routing
(D) Bridging

7. Which of the following are tautologies?

(A) $((P \vee Q) \wedge P) \leftrightarrow P$
(B) $((P \vee Q) \wedge Q) \leftrightarrow Q$
(C) $((P \vee Q) \wedge P) \rightarrow Q$
(D) $(P \vee (P \rightarrow Q)) \rightarrow P$

8. If you want to retain the first 4 bits of given string of 8 bits and complement the last 4 bits, then the correct mask and the operation should be

(A) OR and 00001111
(B) XOR and 11110000
(C) XOR and 00001111
(D) AND and 00001111

9. In OSI model dialogue control and token management are responsibilities of

(A) Session layer
(B) Network layer
(C) Transport layer
(D) Physical layer

10. For the data word 1011 0010, write down the corresponding polynomial

(A) $M(x) = x^7 + x^5 + x^2$
(B) $M(x) = x^8 + x^6 + x^4 + x$
(C) $M(x) = x^7 + x^5 + x^4 + x$
(D) $M(x) = x^5 + x^4 + x^3 + x$

11. Which one of the following network uses dynamic routing?

(A) ARPANET
(B) TYMNET
(C) ALOHA
(D) MANET

12. Law of conservation of packets is used in

(A) Performance analysis
(B) DNS
(C) TCP congestion control
(D) UDP transmission

13. The technique of temporarily delaying outgoing acknowledgements so that they can be looked onto the next outgoing data frame is called

(A) Piggy backing
(B) Cyclic redundancy check
(C) Fletcher checksum
(D) Sampling

14. The presentation layer is concerned with

(A) Syntax and semantics of information transmitted

(B) Protocols commonly needed by users

(C) Application protocols

(D) Token management

15. Packet loss due to transmission errors is relatively rare because

(A) most long-haul trunks are fiber

(B) trunks are wireless

(C) trunks are coaxial

(D) trunks are made of twisted pairs

16. If the signal consists of V discrete levels, Nyquist's theorem states that maximum data rate is equal to

(A) $H \log_2 V$ bits/sec

(B) $2 H \log_2 V$ bits/sec

(C) $H \log_{10} V$ bits/sec

(D) $2 H \log_{10} V$ bits/sec

17. How many cross points are needed in a single stage switch with 40 inputs and 60 outputs?

(A) 40

(B) 60

(C) 2400

(D) 100

18. IPsec is used by VPNs for

(A) encryption and tunneling

(B) authentication and tunneling

(C) encryption and authentication

(D) encryption, authentication and tunneling

19. OSI model defines ———— types of transport classes.

(A) Four

(B) One

(C) Five

(D) Three

20. Which layer in SONET is responsible for the movement of a signal across a physical section?

(A) Photonic layer

(B) Path layer

(C) Line layer

(D) Section layer

21. The wavelength of a signal depends on

(A) frequencies of the signal

(B) medium of the signal

(C) phase of the signal

(D) frequencies and medium of the signal

22. ———— layer is the responsible for end-to-end delivery of the entire message.

(A) Physical layer (B) Data link layer

(C) Network layer (D) Transport layer

23. Match the following IP address with class :

(a)	4.23.145.90	1.	A
(b)	227.34.78.7	2.	B
(c)	246.7.3.8	3.	E
(d)	129.6.8.4	4.	D

	(a)	(b)	(c)	(d)
(A)	1	2	3	4
(B)	1	4	3	2
(C)	4	3	1	2
(D)	2	1	4	3

24. How many T-flip flops are needed to design a divide by 6 counter?

(A) 3 (B) 4

(C) 5 (D) 6

25. Power transistors are invariably provided with

(A) Soldered connections (B) Heat sink

(C) Metallic casing (D) Shield

26. A diode with a forward bias of 0.8V is carrying 2.6 mA of current at room temperature. If $\eta = 1$ for this diode, the dynamic resistance (r) of the diode will be

(A) 308 Ω (B) 10 Ω

(C) 20 Ω (D) 616 Ω

27. The cut in voltage of a Germanium semiconductor diode is nearly

(A) 0.7 V
(B) 0.3 V
(C) 0.5 V
(D) 0.6 V

28. The circuit symbol of a tunnel diode is

(A) 
(B) 
(C) 
(D) 

29. Feature of fetching the next instruction while the current instruction is in executing is called

(A) Bus cycle
(B) Queue
(C) Stack
(D) Pipelining

30. 8051 uses memory mapped I/O through a

(A) Set of special function registers
(B) Set of stack registers
(C) Program counter
(D) Accumulator

31. FET has the following property

(A) Bipolar, voltage controlled device
(B) Bipolar, current controlled device
(C) Unipolar, voltage controlled device
(D) Unipolar, current controlled device

32. A circuit that receives information on a single line and transmits this information on one of the 2^n possible output lines is

(A) Encoder
(B) Decoder
(C) Multiplexer
(D) Demultiplexer

33. A counter with n-flip flops has a maximum mod number

(A) 2^{n+1} (B) 2^{n-1}

(C) $2^{(2n)}$ (D) 2^n

34. The tpd for each flip flop is 50 ns, what is the maximum operating frequency for MOD-32 counter?

(A) 2 MHZ (B) 4 MHZ

(C) 8 MHZ (D) 16 MHZ

35. $(734)_8 = (\ )_{16}$

(A) C 1 D (B) D C 1

(C) 1 C D (D) 1 D C

36. In a very large scale integration IC the number of semiconductor devices of other components may be

(A) 20 to 100 (B) 100 to 1,000

(C) 1,000 to 10,000 (D) 10,000 to 1,00,000

37. When a ROM is designed to convert a binary word to a gray code, the number of input bits to the ROM is ———————— the number of output bits of ROM

(A) Greater than (B) Equal to

(C) Less than (D) Not related to

38. An SCR turns off from conducting state to blocking state on

(A) Reducing gate current

(B) Reversing gate voltage

(C) Reducing anode current below holding current value

(D) Applying ac to the gate

39. The diodes in which impurities are heavily doped is

(A) Varactor diode (B) P-N junction diode

(C) Tunnel diode (D) Zener diode

40. Which of the following statement is best suited for a Zener diode?

(A) It is rectifier diode (B) It works in the forward bias region

(C) It is a constant voltage device (D) It is mostly used in clipping circuit

41. Avalanche breakdown in a semiconductor diode occurs when

(A) Reverse bias exceeds a certain value (B) Forward bias exceeds certain value

(C) Forward current exceeds certain value (D) The potential barrier is reduced to zero

42. An IGBT is generally used in

(A) Low – power applications (B) RF applications

(C) High – voltage applications (D) Low – current applications

43. The diode used in voltage regulator is

(A) PN junction diode (B) Varactor diode

(C) Zener diode (D) GUNN diode

44. For a silicon PN junction, the maximum value of barrier potential is

(A) 0.3 V (B) 0.7 V

(C) 1.3 V (D) 1.7 V

45. The Boolean expression for the sum output of half adder circuit is

(A) $x\,y + \overline{x}\;\overline{y}$ (B) $\overline{x}\;y + x\,\overline{y}$

(C) $\overline{x}\,\overline{y} + x\,y$ (D) $x\,\overline{y} + \overline{x}\,y$

46. A form of virus explicitly designed to hide itself from detection by anti virus software is called ———————— virus.

(A) Encrypted
(B) Stealth
(C) Polymorphic
(D) Metamorphic

47. Which of the following represents the three goals of information security?

(A) Confidentiality, integrity, availability
(B) Prevention, detection, response
(C) People control, process control, technology control
(D) Network security, IP security, mainframe security

48. ———————— is a program that can monitor data traveling over a network.

(A) Mail bomb
(B) Sniffers
(C) Spam
(D) Worm

49. Man-in-the-middle attack is also known as ————————.

(A) Spoofing
(B) TCP hijacking
(C) Sniffer
(D) Denial of service

50. Which of the following replicates itself until it completely fills the available resources?

(A) Virus
(B) Worms
(C) Trojan horses
(D) Trap door

51. Sixteen rounds are used in DES to ensure that

(A) Confusion is provided in the algorithm
(B) Differential cryptanalysis requires less effort than brute-force attack
(C) Differential cryptanalysis is less efficient than brute-force attack
(D) Brute-force attack is diffused

Which of the following is not provided by digital signature?

(A) Integrity

(B) Authentication

(C) Non-repudiation

(D) Privacy

53. Which of the following is non-invertible?

(A) Difference

(B) Swap

(C) EX-OR

(D) Split and combine

54. Malicious software is a software that is

(A) intentionally included in a system for harmful purpose

(B) included by error in a system

(C) intentionally included in a system but does not have any harmful purpose

(D) not verified and validated

55. Which transmission media has the highest transmission speed in a network?

(A) Co axial cable

(B) Twisted pair cable

(C) Optical fiber

(D) Electrical cable

56. Which of the following denotes the Euler's totient functions $[\phi(37), \phi(35)]$?

(A) 36, 24 (B) 36, 26

(C) 36, 33 (D) 36, 34

57. In Vignere cipher, is a kind of

(A) mono alphabetic cipher (B) poly alphabetic cipher

(C) auto key cipher (D) affine cipher

58. Which of the following sequence is used in triple DES?

(A) Encrypt, Encrypt, Encrypt (B) Encrypt, Decrypt, Encrypt

(C) Encrypt, Encrypt, Decrypt (D) Encrypt, Decrypt

59. Brute-force attack is also called as

(A) statistical attack (B) pattern attack

(C) known-plain text attack (D) exhaustive-key-search method

60. The actual message is divided into ———— bit blocks in DES.

(A) 32 (B) 64

(C) 128 (D) 512

61. AES with 256 bit block size has ———— rounds.

(A) 10 (B) 12

(C) 14 (D) 16

62. Which of the following approaches yield a crypto graphically strong Pseudo Random Number Generator (PRNG)?

(A) Symmetric block ciphers (B) Brute force

(C) Non hash functions (D) DSA

63. X.509 certificates are encrypted with

(A) Private key of entities
(B) Public key of entities
(C) Private key of CA
(D) Public key of CA

64. In Diffie-Hellman alg, assume that $g = 7$ and $p = 23$, if A chooses $x = 3$ and B chooses $y = 6$, what will be the secret shared key generated between them?

(A) 14
(B) 18
(C) 24
(D) 36

65. EC-DSS (Elliptic Curve Digital Signature Scheme) is computationally ——— and provides ——— security than RSA-DSS.

(A) Cheaper, higher
(B) Cheaper, lesser
(C) Costly, higher
(D) Costly, lesser

66. Confusion hides relationship between ——— and ———.

(A) Cipher text, key
(B) Cipher text, plaintext
(C) Operation, key
(D) Plain text, operation

67. A cyclic group is ——— abelian and ———.

(A) Always, finite
(B) Always, infinite
(C) Always, may be finite or infinite
(D) Not abelian, finite

68. Which of the following block cipher modes is useful high speed requirements?

(A) Cipher block chaining
(B) Cipher feedback
(C) Output feedback
(D) Counter

69. Which of the following block cipher modes is used for transmission of an encryption key?

(A) Electronic code book
(B) Cipher block chaining
(C) Cipher feedback
(D) Output feedback

70. ———— can bypass custom logins to websites.

(A) Cookies
(B) SQL injection
(C) DDOS
(D) Scripts

71. Say true or false

1. Layer 3 switches are interchangeable with routers
2. Layer 3 switches are hardware based

(A) True, True
(B) True, False
(C) False, True
(D) False, False

72. ———— reorders the frames in TDS (Time Division Switches).

(A) Frame interchanger
(B) Time slot interchanger
(C) Cross bars
(D) Word map table

73. The ———— of a TSI holds the incoming input data in time division switches.

(A) Associative memory
(B) RAM
(C) Interchanger
(D) Hard disk

74. Consider a 3 stage space division switch with N input and N output. The cross bars in input and output stage have 'n' lines and the intermediate stage has 'k' cross bars. Find the number of cross points.

(A) $2kN + (N/n)^2$
(B) $2kN + k(N/n)^2$
(C) $2kNn$
(D) $k(N/n)^2$

75. In ———— the component lifetime does not exceed the whole's lifetime.

(A) association
(B) aggregation
(C) composition
(D) generalisation

76. The ARM processor enters the ———— mode when there is a failed attempt to access memory.

(A) FIR
(B) Supervisor
(C) Abort
(D) System

77. The data processing instruction that do not use barrel shifter.

(A) MUL
(B) ADD
(C) LSL
(D) MOV

78. Gate noise problems in SCR can be minimised

(A) by keeping the gate connecting leads short
(B) by use of capacitor
(C) by keeping the gate connecting leads long
(D) by use of inductor

79. Secret key algorithms are more useful if the secret key is used

(A) only once
(B) frequently
(C) with each pair of users sharing the secret key
(D) for short messages

80. Thumb–2 technology is implemented in which of the following?

(A) All ARM processors

(B) All ARMV7 processors

(C) ARMV7–A processors only

(D) ARMV7-A and ARMV7-R but not ARMV7-M

81. If there is more than one statement in the block of a for loop, which of the following must be placed at the beginning and ending of the loop block?

(A) parentheses ( )

(B) braces { }

(C) brackets [ ]

(D) arrows < >

82. A register in the microprocessor that keeps track of the answer or results of any arithmetic or logic operation is

(A) Stack pointer

(B) Program counter

(C) Instruction pointer

(D) Accumulator

83. Multithreading allowing multiple threads for sharing functional units of

(A) Multiple processor

(B) Single processor

(C) Dual core

(D) Corei5

84. A real time clock

(A) can be stopped or reset after system start and can be programmed

(B) cann't be stopped or reset after system start and uses the free running counter and clock source

(C) cann't be used for measuring timing interval between two events

(D) cann't be used by user programs

85. Which operations are not feasible to perform by simulator programs in accordance to real time programming?

(A) Memory operations
(B) I/O operations
(C) Register operations
(D) Debugging operations

86. Which development tool/program has the potential to allocate the specific addresses so as to load the object code into memory?

(A) Loader
(B) Locator
(C) Library
(D) Linker

87. For compiling source codes for another processor and vice versa

(A) compiler
(B) editor and compiler for target processor
(C) cross compiler
(D) prototyper is used

88. A system must have an interrupt handling mechanism for executing the interrupt service routines in case of the interrupt from

(A) physical devices
(B) interfaced circuits or systems, software interrupt instructions and software exceptions
(C) physical devices or interfaced circuit or systems
(D) physical devices or interfaced circuits or systems, software interrupt instructions and software exceptions

89. When a global variable may be modified by an exception handler, it should be declared as

(A) const
(B) static
(C) dynamic
(D) volatile

90. In which scheduling certain amount of CPU time is allocated to each process

(A) earliest deadline first scheduling

(B) proportional share scheduling

(C) equal share scheduling

(D) preemptive scheduling

91. A Thread

(A) is a lightweight process where the context switching is low

(B) is a lightweight process where the context switching is high

(C) is used to speed up paging

(D) is used to slow down paging

92. Time required to synchronous switch from the context of one thread to the context of another thread is called

(A) threads fly back time

(B) jitter

(C) context switch time

(D) thread sleep time

93. A do-while loop is useful when we want that the statement within the loop must be executed

(A) only once

(B) at least once

(C) more than once

(D) zero time only

94. What are software – generated interrupts in a Generic Interrupt Controller (GIC) generally used for?

(A) Causing a delay

(B) Entering a low power state

(C) Communicating between processors

(D) Calling an operating system function

95. Main approaches for development during edit-test-debug cycles are in sequence of

(i) Use an IDE prototype tool

(ii) Use RTOS

(iii) Uses a simulator without any hardware

(iv) Use emulator

(v) Use target system at last stage

(A) (ii), (i), (iv) and (v)

(B) (i), (iii), (iv) and (v)

(C) (v), (i), (iii) and (iv)

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

96. Which is not a dense instruction set?

(A) Thumb instruction set

(B) MIPS-16 instruction set

(C) 80X86 instruction set

(D) ARM instruction set

97. Message authentication ———————— two parties who exchange message from any third party. It ———————— the two parties against each other.

(A) protects, protects

(B) protects, does not protect

(C) does not protect, protects

(D) does not protect, does not protect

98. The distance vector routing is commonly called as

(A) Ford routing algorithm
(B) Bellman – Ford routing algorithm
(C) Bluetooth algorithm
(D) Adhoc algorithm

99. What is the error detection probability of adding a single bit even parity bit?

(A) Approximately 50%
(B) Approximately 0.7
(C) Approximately 0.2
(D) Exactly 0.75

100. The message polynomial $x^7 + x^5 + 1$ is to be divided by the generator $x^3 + 1$. The remainder is

(A) 010
(B) 101
(C) 100
(D) 011

101. What is the broadcast IP address for 193.140.141.128/26?

(A) 193.140.141.128
(B) 255.255.255.63
(C) 193.140.141.191
(D) 255.255.255.91

102. The drawback of NRZ-I coding scheme is that
(Assume that 1 is coded as a transition)

(A) a long sequence of 1's will cause a problem in clock recovery
(B) a long sequence of 0's will cause a problem in clock recovery
(C) an alternating 0's and 1's is difficult to handle
(D) its voltage levels are not convenient

103. The advantage of packet switching over circuit switching is that

(A) Packet switching does not involve extra overhead bits
(B) Packet switching does not reserve/waste the bandwidth
(C) Packet switching involves store and forward operation
(D) Its queuing operations are efficient

104. For single-bit error correction of 8-bit messages, the minimum no. of check bits (redundant bits) needed is

(A) 3 bits
(B) 4 bits
(C) 2 bits
(D) 1 bit

105. CSMA protocol is not suitable for wireless LANs because

(A) a peculiar problem called hidden station problem will result in collisions

(B) wireless LANs use high power stations

(C) wireless LAN is not really a network

(D) collisions will never occur in wireless LANs

106. One of the principles used to arrive at seven layers in OSI model is

(A) A layer should be used where a different abstraction is not needed

(B) A layer should be used to increase the information flow across the interfaces

(C) A layer should be used where a different abstraction is needed

(D) A layer should be used to club distinct functions together

107. The difference between services and interfaces is that

(A) Service definition tells the function of a layer and its interface definition tells how to access it

(B) They both are related to implementation and protocol

(C) The interface says how the layer works inside and the service does not mention it

(D) They never converge to a layer

108. The best case time delay in response to a request in a client-server system that uses a fibre optic cable of 100 km length (between the client and server) is

(A) 100 ms

(B) 0.66 ms

(C) 1 μs

(D) 6.66 μs

109. A client transmits a query of size 1 KB at the rate of 10 kbps to a server connected to it by a fibre optic cable of length 10 km. Assuming that the response by the server is of negligible size, the total time from the beginning of the query and the reception of response is

(A) 819.26 ms

(B) 824 s

(C) 256 ms

(D) 512 μs

110. In data link level, error detection is achieved by

(A) Packet switching

(B) Manchester code

(C) Non-return zero code

(D) Cyclic redundancy codes

111. The length of MAC address is ———— bits.

(A) 24 (B) 36

(C) 42 (D) 48

112. If end to end delay $d_{end\text{-}end} = N(d_{proc} + d_{trans} + d_{prop})$ in a non congested network, the number of routers between source and destination is

(A) $N/2$ (B) N

(C) $N-1$ (D) $2N$

113. FTP uses ———— parallel TCP connection(s) to transfer a file.

(A) 1 (B) 2

(C) 3 (D) 4

114. The header length of IPV6 datagram is ———— bytes.

(A) 10 (B) 24

(C) 32 (D) 40

115. FDDI Stands For

(A) Fast Data Delivery Interface (B) Fiber Distributed Data Interface

(C) Fiber Distributed Digital Interface (D) Fast Distributed Data Interface

116. A ———— is a TCP name for a transport service access point.

(A) Port (B) Pipe

(C) Node (D) (A) or (B)

117. Which of the following application layer protocol is used by electronic mail?

(A) SMTP (B) HTTP

(C) FTP (D) STP

118. A point-to-point protocol over Ethernet is a network protocol for

(A) encapsulating PPP frames inside Ethernet frames

(B) encapsulating Ethernet frames inside PPP frames

(C) for security of Ethernet frames

(D) for security of PPP frames

119. IEEE 802.11 is

(A) Token ring
(B) Token bus
(C) Wireless LAN
(D) Ethernet

120. Find the baud rate for a 72,000 bps 64-QAM signal

(A) 12,000 baud
(B) 1,125 baud
(C) 36,000 baud
(D) 6,000 baud

121. What is the maximum size of data that the applications layer can pass on to the TCP layer below?

(A) Any size
(B) 2^{16} bytes
(C) 1500 bytes
(D) 2^{8} bytes

122. Which of the following is correct?

(A) HDLC is character – oriented protocol
(B) HDLC is bit oriented protocol
(C) HDLC is byte oriented protocol
(D) HDLC is count oriented protocol

123. The bandwidth of an FM signal requires 10 times the bandwidth of the signal

(A) Carrier
(B) Modulating
(C) Bipolar
(D) Sampling

124. Match the following :

	Port No.		Protocol
(a)	21	1.	HTTP
(b)	23	2.	FTP
(c)	25	3.	Telnet
(d)	80	4.	SMTP

	(a)	(b)	(c)	(d)
(A)	1	2	3	4
(B)	2	3	1	4
(C)	2	3	4	1
(D)	1	2	4	3

125. Of all logic families, CMOS has become the most preferred, and exclusive, logic style for VLSI and ULSI circuits because

(A) It is the fastest of all logic families

(B) It is the most immune to noise

(C) All types of logic gates can be designed in it easily

(D) It consumes no static power

126. An 8-bit D/A converter has an output of voltage range 0 to 2.55 V, its resolution is

(A) 10 mV (B) 1 mV

(C) 0.1 mV (D) 1.1 mV

127. The programmable peripheral interface in 8085 is

(A) 8254 B (B) 8255 A

(C) 8237 B (D) 8259 A

128. Shorting all the inputs of a NAND or NOR gate to get a one input-one output circuit yields a

(A) Inverter (B) EX-OR

(C) EX-NOR (D) AND

129. The no. of memory chips needed to design 8 K – byte memory if the memory chip size is 1024×1 is

(A) 8 (B) 16

(C) 32 (D) 64

130. The no. of registers/memory locations having 12 address lines and 8 data lines is

(A) 1024 (B) 2048

(C) 4096 (D) 8192

131. An example of a shift register counter is

(A) Ring counter (B) Ripple counter

(C) Decade counter (D) Up/down BCD counter

132. The addition of 3F 8_{16} and 5B 3_{16} is

(A) 9 $AB_{(16)}$ (B) 8 $AB_{(16)}$

(C) 7 $AB_{(16)}$ (D) 75 $D_{(16)}$

133. 8085 processor is called an 8 bit processor, because 8085 has

(A) 8 bit ALU (B) 8 bit data bus

(C) (A) and (B) (D) 8 bit storage

134. A device that does not exhibit negative resistance characteristics is

(A) FET (B) UJT

(C) Tunnel diode (D) SCR

135. How many flip-flops are required for mod-16 counter?

(A) 5 (B) 6

(C) 3 (D) 4

136. The leakage current across a p^n junction is due to

(A) Minority carriers (B) Majority carriers

(C) Junction capacitance (D) Immobile ions

137. How many clock cycles are needed for the conversion process in a successive approximation A/D converter?

(A) n^2 (B) n

(C) 2^n (D) 2^{2n}

138. Match the following

	Laws of Boolean		Relational Algebra
(a)	Distributive Law	1.	X + X = X
(b)	De Morgan's Law	2.	X (Y + Z) = XY + XZ
(c)	Idempotent Law	3.	(X) = X
(d)	Involution Law	4.	(X + Y) = XY

	(a)	(b)	(c)	(d)
(A)	1	2	3	4
(B)	2	4	1	3
(C)	3	4	1	2
(D)	4	1	2	3

139. A BCD counter, is called a decade counter when it counts from

(A) 0 to F
(B) 0 to 9
(C) 0 to 10
(D) 0 to A

140. Which of the following state is true?

(A) FET and BJT, both are unipolar
(B) FET and BJT, both are bipolar
(C) FET is bipolar, BJT unipolar
(D) FET is unipolar, BJT bipolar

141. In a Bipolar Transistor at room temperature, if the emitter current is doubled, the voltage across its base-emitter junction

(A) Doubles
(B) Halves
(C) Increases by about 20 mV
(D) Decreases by about 20 mV

142. The internal RAM memory of 8051 is

(A) 32 bytes
(B) 64 bytes
(C) 128 bytes
(D) 256 bytes

143. A BJT is said to be operating in the saturation region if

(A) Both the junctions are reverse biased
(B) Base-emitter junction is reverse biased and base collector junction is forward biased
(C) Base-emitter junction is forward biased and base collector junction is reverse biased
(D) Both the junctions are forward biased

144. The frequency limit of Tunnel diode is

(A) 10^4 Hz
(B) 10^8 Hz
(C) 10^{12} Hz
(D) 10^2 Hz

145. The output color of the GaAS PLED is

(A) Yellow
(B) Green
(C) Amber
(D) Red

146. The Boolean expression for the sum output of full adder is

(A) $\bar{x}\,\bar{y}\,z+\bar{x}\,y\,\bar{z}+x\,\bar{y}\,\bar{z}+x\,y\,z$ (B) $\bar{x}\,\bar{y}\,\bar{z}+x\,y\,\bar{z}+x\,\bar{y}\,\bar{z}+x\,y\,z$

(C) $\bar{x}\,\bar{y}\,z+\bar{x}\,y\,\bar{z}+\bar{x}\,\bar{y}\,\bar{z}+x\,y\,\bar{z}$ (D) $\bar{x}\,\bar{y}\,z+\bar{x}\,y\,\bar{z}+x\,\bar{y}\,\bar{z}+\bar{x}\,\bar{y}\,\bar{z}$

147. In 8086 the over flow flag is set when

(A) The sum is more than 16 bits

(B) Signed numbers go out of their range after an arithmetic operation

(C) Carry and sign flags are set

(D) Subtraction operation is performed

148. In a micro processor, which bus is a bidirectional bus?

(A) Address bus (B) Data bus

(C) Control bus (D) Address decoder bus

149. What type of circuit is used at the interface point of an input point?

(A) Decoder (B) Latch

(C) Tristate buffer (D) Encoder

150. The software used to drive micro processor based systems is called

(A) Assembly language (B) BASIC interpreter instructions

(C) Firm ware (D) Machine language code

151. The instruction of the μC 8051 MOV A, @ R1 will

(A) Copy R1 to the accumulator

(B) Copy the accumulator to R1

(C) Copy the contents of memory whose address is in R1 to the accumulator

(D) Copy the accumulator to the contents of memory whose address is in R1

152. An n-channel D-MOSFET with a positive V_{GS} is operating in

(A) the depletion mode (B) the enhancement mode

(C) cut off (D) saturation

153. The purpose of diffusion is to ensure that

(A) statistical structure of the plain text is dissipated over many cipher text digits

(B) the relation between the key and cipher text is unbreakable

(C) statistical structure of the key is not known

(D) the key size is made as large as possible

154. Encrypt the message "victorytoyou" using vigenere cipher algorithm with the key "win".

(A) rqppweubbuwh

(B) rpqpuewhtstc

(C) qprtsefpqelm

(D) pqtsrwyzubdf

155. Identify the encryption algorithm, which is unconditionally secure?

(A) Monoalphabetic cipher

(B) Playfair cipher

(C) Polyalphabetic cipher

(D) One-time pad

156. The Avalanche effect means that

(A) Change in many input bits must result in change in less no. of output bits

(B) Change in one input bit must result in change in one output bit

(C) Change in one input or key bit must result in many bits of the output changing

(D) Change in many key bits must result in less no. of changes in output bits

157. If the cipher generated by the encryption scheme does not contain enough information to find uniquely the corresponding plain text, no matters how much cipher text is available, then the encryption scheme is

(A) computationally secure

(B) conditionally secure

(C) unconditionally secure

(D) provably secure

158. Ticket granting server in Kerberos will issue token to use the service of

(A) Authentication server
(B) KDC
(C) Autherization server
(D) Actual data server

159. Protocol used to provide security at network layer level is

(A) SSL
(B) TSL
(C) PGP
(D) IP sec

160. ECC is a asymmetric crypto system which provides

(A) conditionaly secured system
(B) computationally secured system
(C) high security with less complexity
(D) low security with high complexity

161. Mix columns operation is performed in

(A) DES
(B) AES
(C) RSA
(D) Elgamol

162. The AES key expansion algorithm takes an input of

(A) Four word key
(B) Two word key
(C) Eight word key
(D) Single (one) word key

163. The cipher text produced by a simple stream cipher method for the plain text 11001100 with the key stream of 01101100 is

(A) 10100000
(B) 10101010
(C) 11100000
(D) 10110000

164. Cipher block chaining and counter (CTR) finds its application in

(A) General-purpose block-oriented transmission

(B) General-purpose stream oriented transmission

(C) Stream-oriented transmission over noisy channel

(D) Secure transmission of single values (encryption key)

165. What is $f(x) \times g(x) \mod m(x)$ used in AES with the finite field $GF(28)$ with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ and $f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1$

(A) $x^7 + x^6 + 1$

(B) $x^7 + x^5 + 1$

(C) $x^7 + x^4 + 1$

(D) $x^7 + x^6 + x^5 + 1$

166. Differential cryptanalysis is the attack that is capable of breaking DES in less than

(A) 2^{55} encryptions

(B) 2^{47} encryptions

(C) 2^{25} encryptions

(D) 2^{10} encryptions

167. Which of the following is the plain text of the cipher text "ANKYODKYUREPFJBYO JDSPLREYIUNOF DOIUERFPLUYTS " with the key "pxlmvmsydofuyrvzwctnlebnecvgdup ahfzzlmnyih"

(A) mr mustard with the candle stick in the hall

(B) mr mustard with the knife in the library

(C) miss scarlet with the knife in the library

(D) miss scarlet with the candle stick in the hall

168. The time required at 10^6 decryption / μs for exhaustive key search of 168 bits key size is

(A) 5.9×10^{30} years

(B) 5.4×10^{18} years

(C) 10.01 hours

(D) 2.15 milliseconds

169. ———— states that if p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 (\text{mod } p)$.

(A) Euler's theorem
(B) Fermat's theorem
(C) Krichoff's principle
(D) Diffie-Hellman key exchange principle

170. ———— states that for every a and n that are relatively prime $a^{\phi(n)} \equiv 1 (\text{mod } n)$.

(A) Fermat's theorem
(B) Euler's theorem
(C) Miller Rabin test for primality
(D) Krichoff's principle

171. Which of the following can be used to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli?

(A) Miller Rabin algorithm
(B) Euler's theorem
(C) Chinese Remainder theorem
(D) Discrete logarithms

172. Diffie-Hellman key exchange is a ———— algorithm based on ————.

(A) Symmetric, discrete logarithms
(B) Public-key, discrete logarithms
(C) Symmetric, Chinese remainder theorem
(D) Public-key, Chinese remainder theorem

173. ———— switches perform packet forwarding in hardware.

(A) Layer-3
(B) Layer-2
(C) Traditional
(D) Routers

174. ———— are access points of neighbouring LANs that operate in overlapping channels.

(A) Friend access points
(B) Enemy access points
(C) Rogue access points
(D) Theft access points

175. Match

(a)	Pre image resistance	1.	two messages should not hash to same MD
(b)	Second image resistance	2.	hard to create a 2nd message with same MD as 1st
(c)	Collision resistance	3.	hard to create message from digest

	(a)	(b)	(c)
(A)	3	2	1
(B)	3	1	2
(C)	2	3	1
(D)	1	2	3

176. Find 6^{24} mod 35

(A) 6 (B) 1

(C) 35 (D) 24

177. Which of the following cryptographic algorithm is slow?

(A) Blow Fish (B) IDEA

(C) RC5 (D) Triple DES

178. In DES, which of the following is the total number of weak, semi weak and possible weak keys?

(A) 64 (B) 28

(C) 32 (D) 16

179. Identify the type of p-box shown by the following permutation table.

1	1	2	3	4	4

(A) Linear (B) Expansion

(C) Compression (D) Non-linear

180. Inline assembly

(A) avoid unaligned data

(B) use bit fields

(C) reduces portability between architectures

(D) unroll loops

181. Which of the following type of function is an ideal candidate for being declared inline?

(A) a function that is small and is not called frequently

(B) a function that is small and is called frequently

(C) a function that is not small and is not called frequently

(D) a function that is not small and is called frequently

182. ———————— scheduling mechanism is efficient for less number of periodic tasks.

(A) cooperative with precedence constraints

(B) cyclic

(C) preemptive

(D) preemptive with precedence

183. Which is the type of memory for information that does not change on your computer?

(A) RAM

(B) ROM

(C) ERAM

(D) RW/RAM

184. The ARM processor registers R13, R14 and R15 are architecturally used for special purposes. Which is the correct respective sequence of special purpose registers?

(A) PC, LR, SP

(B) LR, PC, SP

(C) SP, LR, PC

(D) LR, SP, PC

185. Because micro processor CPUs do not understand mnemonics as they are, they have to converted to

(A) hexadecimal machine code

(B) assembly language

(C) binary machine code

(D) high level language

186. An operating system contains 3 user processor each requiring 2 units of resource R. The minimum number of units of R such that no deadlocks will ever arise is

(A) 4 (B) 3

(C) 5 (D) 6

187. Memory manager in RTOS for hard real time system must provide

(A) Memory protection among the tasks

(B) Dynamic block allocation

(C) Memory management unit functions

(D) Fixed blocks allocations

188. Performance of a system is accelerated by additional

(A) Processor of high speed

(B) Coprocessor and IPs

(C) Device drivers

(D) Large size memory buffers

189. Which component is replaced by an incircuit emulator on the development board for testing purposes?

(A) RAM (B) I/O ports

(C) Micro controller IC (D) ROM

190. A four message reliable IPC protocol for client server communication work as

(A) request, reply, acknowledgement

(B) request, acknowledgement, request, acknowledgment

(C) request, acknowledgement, reply, acknowledgement

(D) request, request, reply, acknowledgement

191. Semaphore functions can be used for

(i) a token

(ii) an event flag

(iii) a mutex

(iv) a lock for all other processes

(v) a counting semaphore

(vi) using a bounded buffer

(vii) using a shared memory

(A) (i), (ii), (iii) and (v)

(B) all except (iv)

(C) all except (i) and (vii)

(D) all except (vi)

192. In priority scheduling algorithm, when a process arrives at the ready queue, its priority is compared with the priority of

(A) all process

(B) currently running process

(C) parent process

(D) int process

193. An instruction that is used to move data from ARM register to a status register is called

(A) MRC

(B) MRS

(C) MSR

(D) MCR

194. Match

(a)	Abstraction	1.	Register transfer level
(b)	Top Down Design	2.	HDL
(c)	Control hierarchy	3.	ADL

	(a)	(b)	(c)
(A)	1	2	3
(B)	1	3	2
(C)	2	1	3
(D)	2	3	1

195. A watchdog timer is timing device such that it is

(A) set for a preset time interval by program and an event must occur during that interval else the device will generate the time out signal for the failure to get that event

(B) can be used as real time clock

(C) internally preset for a time interval in a microcontroller and generates the timeout signal for the event occurrence in the watched time interval

(D) can be used to find variation in processor clock rate during watched interval

196. On populating code in a child process which of the following conditions hold:

(A) The process becomes independent of the parent-its PPID is destroyed

(B) A new subdirectory is created to locate the new process

(C) The environment variables remain unchanged

(D) A new stack is defined for the new process

197. Which of the following are required when a shared memory area is used for IPC?

(A) Pointer to data area

(B) Data size in bytes

(C) First attach time

(D) Last attach time

198. Performance of a system accelerates by additional

(A) Processors of high speed

(B) Coprocessors and the IPs such as Java accelerator

(C) Linux device drivers

(D) Bigger size memory buffers

199. Which one of the following is True?

(A) Object file is the binary image of embedded software

(B) Locator output file is binary image in Intel Hex format

(C) Linker output file is binary image in Intel Hex format

(D) Cross assembled file is binary image in Intel Hex format

200. Processor less systems are used when requirements are

(A) Ease to change the system when new hardware version become available

(B) Less then 1 kB memory for the program

(C) Secure internally embedded codes

(D) Very low computational ability, but very strong interfacing capability with its multiple inputs and outputs

---

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK

SEAL