Question Paper Name:	A Practical Refresher in Computer Science 16th February 2020 Shift 1
Subject Name:	A Practical Refresher in Computer Science
Creation Date:	2020-02-16 12:58:20
Duration:	180
Total Marks:	140
Display Marks:	Yes

A Practical Refresher in Computer Science

Group Number :	1
Group Id :	28860724
Group Maximum Duration :	0
Group Minimum Duration :	120
Show Attended Group? :	No
Edit Attended Group? :	No
Break time:	0
Group Marks:	140
Is this Group for Examiner?:	No

A Practical Refresher in Computer Science

Section Id :	28860727
Section Number :	1
Section type :	Online
Mandatory or Optional:	Mandatory
Number of Questions:	70
Number of Questions to be attempted:	70
Section Marks:	140

Sub-Section Number:	1
Sub-Section Id:	28860727
Question Shuffling Allowed :	Yes

Question Number : 1 Question Id : 2886072156 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

At the end of running the Ethernet spanning tree algorithm, which ONE of the following is determined by the participating switches?

a. root bridge ID
b. longest path length in the tree
c. number of leaves in the tree
d. number of hosts connected to each port

Options :

2886078615. 2

2886078616. 3

2886078617. 4

Question Number : 2 Question Id : 2886072157 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

The main purpose of the Ethernet spanning tree algorithm is ____ . (Choose the BEST option below).

a. to detect IP address duplicates
b. to detect Ethernet address duplicates
c. to form a loop-free topology
d. to find optimal paths to each destination

Options :

2886078618. 1

2886078619. 2

2886078620. 3

2886078621. 4

Question Number : 3 Question Id : 2886072158 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In an Ethernet extended LAN, what do "learning bridges" learn? (Choose one option below).

a. the forwarding table
b. mapping from ethernet address to IP address
c. whether other bridges are active/passive
d. whether there are duplicate ethernet addresses

Options :

2886078622. 1

2886078623. 2

2886078624. 3

2886078625. 4

Question Number : 4 Question Id : 2886072159 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In an Ethernet extended LAN, when a bridge looks at the source MAC address of a data frame, it _____. (Choose the BEST option below).

a. updates its path to the root bridge
b. updates its set of active ports
c. learns the outgoing port to use for frames destined to that source host
d. learns the number of hops in the path from that source host

Options :

2886078626. 1

2886078627. 2

2886078628. 3

2886078629. 4

Question Number : 5 Question Id : 2886072160 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following represents the columns of the forwarding table at an Ethernet bridge the best ?

a. (destination MAC address, next-hop bridge ID)
b. (destination IP address, next-hop IP address)
c. (destination MAC address, outgoing port)
d. (destination IP address, path to destination)

Options :

2886078630. 1

2886078631. 2

2886078632. 3

2886078633. 4

Question Number : 6 Question Id : 2886072161 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is the primary purpose of VLANs in Ethernet?

a. Connecting to non-Ethernet networks
b. Supporting virtual circuits
c. Supporting multiple virtual machines per port
d. Traffic isolation

Options :

2886078634. 1

2886078635. 2

2886078636. 3

2886078637. 4

Question Number : 7 Question Id : 2886072162 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is an advantage resulting from circuit switching (compared to packet switching)? Choose the BEST option below.

a. Fault tolerance
b. High channel utilization
c. Guaranteed bandwidth for flows
d. No flow setup delay

Options :

2886078638. 1

2886078639. 2

2886078640. 3

2886078641. 4

Question Number : 8 Question Id : 2886072163 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

How are packets forwarded toward the destination in packet switching? Choose the BEST option below.

a. By sending the incoming packet to all outgoing interfaces
b. By looking at the packet header
c. By sending the incoming packet to google.com
d. By looking at the packet contents

Options :

2886078642. 1

2886078643. 2

2886078644. 3

2886078645. 4

Question Number : 9 Question Id : 2886072164 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

When using circuit switching, what should the link capacity be (in kbps) if you want to support 10 users, each requiring 100kbps. Assume a user is active only 10% of the time.

a. 10kbps
b. 100kbps
c. 1Mbps
d. 10Mbps

Options :

2886078646. 1

2886078647. 2

2886078648. 3

2886078649. 4

Question Number : 10 Question Id : 2886072165 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which among the following switching techniques is BEST for bursty user traffic, which technique supports more number of users?

a. Packet switching
b. Circuit switching
c. Virtual circuit switching
d. Short circuit switching

2886078650. 1

2886078651. 2

2886078652. 3

2886078653. 4

Question Number : 11 Question Id : 2886072166 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the source routing scheme, why is the packet header length variable? Choose the BEST option below.

a. Different destinations are at different hop counts
b. Different destinations have different resource requirements
c. Different destinations need different amount of data payload
d. Different destinations have different processing capabilities

Options :

2886078654. 1

2886078655. 2

2886078656. 3

2886078657. 4

Question Number : 12 Question Id : 2886072167 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which technique has the lowest per packet overhead?

a. Circuit switching
b. Virtual Circuit Switching
c. Datagram switching
d. Source routing

Options :

2886078658. 1

2886078659. 2

2886078660. 3

2886078661. 4

Question Number : 13 Question Id : 2886072168 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of Internet routing, a routing domain is called ____ . (Choose the BEST option below).

a. a routing island
b. a routing cloud
c. an autonomous system
d. a bounded region

2886078662. 1

2886078663. 2

2886078664. 3

2886078665. 4

Question Number : 14 Question Id : 2886072169 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following routing protocols is used by BGP (Border Gateway Protocol)?

a. Pure Distance Vector
b. Path Vector
c. Dynamic Source Routing
d. Link State

Options :

2886078666. 1

2886078667. 2

2886078668. 3

2886078669. 4

Question Number : 15 Question Id : 2886072170 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Routing using BGP (Border Gateway Protocol) focuses on _____. (Choose the BEST option below).

a. policy based routing
b. least delay routing
c. max throughput routing
d. multi-path routing

Options :

2886078670. 1

2886078671. 2

2886078672. 3

2886078673. 4

Question Number : 16 Question Id : 2886072171 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

g protocol used within an ISP (Internet Service Provider) is: (choose the BEST option below)

a. always the same as that used by BGP
b. always based on distance vector
c. always different from that used by BGP
d. independent of what is used by BGP

Options :

2886078674. 1

2886078675. 2

2886078676. 3

2886078677. 4

Question Number : 17 Question Id : 2886072172 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

When should an ISP export routes (IP prefix information) it has learnt from its provider ISP to another ISP with which it has a peering relation?

a. Always
b. Never
c. Only when it has exactly one provider
d. Only when it has at least two providers

Options :

2886078678. 1

2886078679. 2

2886078680. 3

2886078681. 4

Question Number : 18 Question Id : 2886072173 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is a relation between ISPs (Internet Service Providers) which DOES NOT usually involve money exchange?

a. Provider-customer
b. Router-forwarder
c. Peering
d. Firewall-protectee

Options :

2886078682. 1

2886078683. 2

2886078684. 3

2886078685. 4

Question Number : 19 Question Id : 2886072174 Question Type : MCQ Option Shuffling : No

How many peers can an ISP (Internet Service Provider) have? Choose the BEST option below.

a. At least one
b. At most one
c. Any number
d. Any even number

Options :

2886078686. 1

2886078687. 2

2886078688. 3

2886078689. 4

Question Number : 20 Question Id : 2886072175 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

When should an ISP export IP prefix information it has learnt from its peer ISP to its provider ISP?

a. Always
b. Never
c. Only when it has exactly one provider
d. Only when it has at least two providers

Options :

2886078690. 1

2886078691. 2

2886078692. 3

2886078693. 4

Question Number : 21 Question Id : 2886072176 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

A router in a particular Internet domain runs both EGP (Exterior Gateway Protocol) and an IGP (Interior Gateway Protocol). Its forwarding table will be based on ____.

a. Both EGP and IGP
b. Neither EGP nor IGP
c. Only EGP
d. Only IGP

Options :

2886078694. 1

2886078695. 2

2886078696. 3

2886078697. 4

How many root servers are present for DNS (Domain Name System)?

a. Exactly six: one per continent
b. About 200: one per country
c. Exactly 13: not uniformly distributed across continents
d. About 300: not uniformly distributed across countries

Options :

2886078698. 1

2886078699. 2

2886078700. 3

2886078701. 4

An Internet host can have both a hostname and an IP address as identities. Which ONE of the following is an ADVANTAGE of IP addresses compared to hostnames?

a. It is easier for humans to remember IP addresses
b. It is easier for routers to route based on IP address
c. IP addresses are hierarchical, hostnames are not
d. Number of IP addresses possible is much more than number of hostnames

Options :

2886078702. 1

2886078703. 2

2886078704. 3

2886078705. 4

Which ONE of the following information must ALWAYS be present at a local DNS server?

a. The IP address of www.google.com
b. The NS record of www.google.com
c. The IP address of the root DNS servers
d. The security credentials of at least one search engine

Options :

2886078706. 1

2886078707. 2

2886078708. 3

2886078709. 4

Which ONE of the following is TRUE with respect to a machine on the Internet?

a. A machine can have only one IP address but multiple hostnames
b. A machine can have only one hostname but multiple IP addresses
c. A machine can have only one IP address and only one hostname
d. A machine can have multiple IP addresses and also multiple hostnames

Options :

2886078710. 1

2886078711. 2

2886078712. 3

2886078713. 4

Which ONE of the following is the DNS record type relevant for sending emails to a particular email address?

a. A record
b. B record
c. EM record
d. MX record

Options :

2886078714. 1

2886078715. 2

2886078716. 3

2886078717. 4

The original DNS used a centralized hosts.txt file. In what significant way was this architecture changed to pave the way to the current DNS architecture?

a. The text file was replaced with database records
b. The text file was replaced with binary format
c. A distributed architecture was adopted for better fault tolerance
d. Multi-language support was added

Options :

2886078718. 1

2886078719. 2

2886078720. 3

2886078721. 4

How many top level domains does the DNS name hierarchy have?

a. Exactly six: one per each (inhabited) continent
b. Exactly 12: one primary + one backup per each (inhabited) continent
c. Exactly five: .com, .org, .edu, .gov, .net
d. Several 100s

Options :

2886078722. 1

2886078723. 2

2886078724. 3

2886078725. 4

Question Number : 29 Question Id : 2886072184 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of DNS, ICANN (Internet Corporation for Assigned Names and Numbers) is responsible for maintaining ____.

a. the web servers of each top level domain
b. the root server replicas
c. the mail gateways in each domain
d. the tier-1 autonomous systems

Options :

2886078726. 1

2886078727. 2

2886078728. 3

2886078729. 4

Question Number : 30 Question Id : 2886072185 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

The current DNS has a _____ implementation and _____ management.

a. centralized, centralized
b. distributed, distributed
c. centralized, distributed
d. distributed, centralized

Options :

2886078730. 1

2886078731. 2

2886078732. 3

2886078733. 4

Question Number : 31 Question Id : 2886072186 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

DNS uses ___ for queries and ___ for replies.

a. UDP, UDP
b. TCP, TCP
c. UDP, TCP
d. TCP, UDP

Options :

2886078734. 1

2886078735. 2

2886078736. 3

2886078737. 4

Question Number : 32 Question Id : 2886072187 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is true about the transport protocol used by HTTP ?

a. It uses only UDP
b. It uses only TCP
c. It uses UDP and TCP in every download
d. It uses TCP for download and UDP for upload

Options :

2886078738. 1

2886078739. 2

2886078740. 3

2886078741. 4

Question Number : 33 Question Id : 2886072188 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of HTTP, non-persistent connections refers to the use of:

a. unverified server certificate
b. UDP for some HTTP downloads
c. a separate TCP connection per-HTTP-object
d. different browser tabs at the HTTP client

Options :

2886078742. 1

2886078743. 2

2886078744. 3

2886078745. 4

Question Number : 34 Question Id : 2886072189 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

E of the following HTTP header lines is absolutely essential for a web proxy to work?

a. If-Modified-Since
b. If-None-Match
c. Host
d. User-agent

Options :

2886078746. 1

2886078747. 2

2886078748. 3

2886078749. 4

Question Number : 35 Question Id : 2886072190 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

A HTTP object refers to _____ (choose the BEST option below).

a. a HTML page or an embedded JPG image
b. only HTML pages and not embedded images
c. not HTML pages but only embedded images
d. only the web server certificate

Options :

2886078750. 1

2886078751. 2

2886078752. 3

2886078753. 4

Question Number : 36 Question Id : 2886072191 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is a HTTP method used to send HTML form data from the client to the server?

a. SEND
b. POST
c. SUBMIT
d. TRANSFER

Options :

2886078754. 1

2886078755. 2

2886078756. 3

2886078757. 4

Question Number : 37 Question Id : 2886072192 Question Type : MCQ Option Shuffling : No

Marks : 1 Wrong Marks : 0

The header of a HTTP response uses ____ format of ____ size.

a. text, fixed
b. text, variable
c. binary, fixed
d. binary, variable

Options :

2886078758. 1

2886078759. 2

2886078760. 3

2886078761. 4

Question Number : 38 Question Id : 2886072193 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

A response code of HTTP 200 refers to:

a. a DNS lookup error of a web server's name
b. a response from a web server indicating success
c. the web server being unreachable due to network outage
d. an unrecognized server certificate

Options :

2886078762. 1

2886078763. 2

2886078764. 3

2886078765. 4

Question Number : 39 Question Id : 2886072194 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In a HTML webpage there are two embedded JPG images. Which ONE of the following statements is TRUE?

a. Both JPG images have to come from the same HTTP server as the main HTML
b. Both JPG images have to come from the same HTTP server, but it can be different from that of the main HTML
c. At least one JPG image has to come from the same HTTP server as the main HTML
d. The JPG images and the main HTML can all come from three different HTTP servers

Options :

2886078766. 1

2886078767. 2

2886078768. 3

2886078769. 4

Correct Marks : 2 Wrong Marks : 1

Which ONE of the following protocols can potentially be used by a mail user agent to get a user's emails?

a. FTP
b. SNMP
c. ARP
d. IMAP

Options :

2886078770. 1

2886078771. 2

2886078772. 3

2886078773. 4

Question Number : 41 Question Id : 2886072196 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which transport protocol is used by SMTP ?

a. Only TCP
b. Only UDP
c. TCP for email headers and UDP for email body
d. SMTP itself is a transport protocol

Options :

2886078774. 1

2886078775. 2

2886078776. 3

2886078777. 4

Question Number : 42 Question Id : 2886072197 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

A process P1 has been running on the CPU for a while, and at time=t0 the OS decides that it is now time to schedule another process P2 as P1's turn with the CPU is now over (temporarily). Now when P2 is made to run by the OS, what is the STATE of P1 ? Choose the BEST option below.

a. Blocked
b. Ready
c. Forked
d. Signaled

Options :

2886078778. 1

2886078779. 2

2886078780. 3

Question Number : 43 Question Id : 2886072198 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In Linux, which system call is used to spawn a child process?

a. fork()
b. divide()
c. wait()
d. exit()

Options :

2886078782. 1

2886078783. 2

2886078784. 3

2886078785. 4

Question Number : 44 Question Id : 2886072199 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following best describes a "system call" in the context of a process running on a computer with an operating system?

a. a function call from application code into OS code
b. a function call from the OS to the application program's code
c. a function call from the OS code to the network administrator
d. a function call from the application code to the local Domain Name Server

Options :

2886078786. 1

2886078787. 2

2886078788. 3

2886078789. 4

Question Number : 45 Question Id : 2886072200 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In Linux, the root user's program's instructions run in _____ mode; a regular user's program's instructions run in _____ mode.

a. user, user
b. user, kernel
c. kernel, user
d. kernel, kernel

Options :

2886078790. 1

2886078791. 2

2886078792. 3

Question Number : 46 Question Id : 2886072201 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following CPU instructions is used to implement a system call?
Select the BEST option below.

a. stdio
b. schedule
c. trap
d. sync

Options :

2886078794. 1

2886078795. 2

2886078796. 3

2886078797. 4

Question Number : 47 Question Id : 2886072202 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of an Operating System for a multi-user system, what is a semaphore?

a. a process scheduling algorithm
b. a synchronization primitive
c. a space for storing inactive process state
d. a dynamic memory allocation scheme

Options :

2886078798. 1

2886078799. 2

2886078800. 3

2886078801. 4

Question Number : 48 Question Id : 2886072203 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is NOT an objective in an Operating System's process scheduling policy?

a. Maximizing CPU utilization
b. Minimizing process turn-around time
c. Minimizing scheduling overhead
d. Maximizing the OS's swap space utilization

Options :

2886078802. 1

2886078803. 2

2886078804. 3

2886078805. 4

Question Number : 49 Question Id : 2886072204 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

A TLB is used to store VA-PA mappings because:

a. It increases security and isolation amongst processes
b. It's cheaper than main memory
c. It makes the address translation faster, on average
d. None of the other options

Options :

2886078806. 1

2886078807. 2

2886078808. 3

2886078809. 4

Question Number : 50 Question Id : 2886072205 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In a process's virtual address space: (choose the BEST option below).

a. The stack grows from higher address toward lower address, while the heap grows from lower address to higher address
b. The stack grows from lower address toward higher address, while the heap grows from higher address to lower address
c. Both the stack and heap grow from higher address toward lower address
d. Both the stack and heap grow from lower address toward higher address

Options :

2886078810. 1

2886078811. 2

2886078812. 3

2886078813. 4

Question Number : 51 Question Id : 2886072206 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is one of the roles of the OS dring address translation?

a. Converting the VA to the PA
b. Maintaining free space information
c. Generating traps
d. Converting the PA to the VA

Options :

2886078814. 1

2886078815. 2

2886078816. 3

2886078817. 4

Question Number : 52 Question Id : 2886072207 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of paging in an OS, "internal fragmentation" refers to: (choose the BEST option below)

a. Unusable space between pages
b. Unused space within pages
c. Break-up of a page into integer variable locations
d. Break-up of a page into stack frames

Options :

2886078818. 1

2886078819. 2

2886078820. 3

2886078821. 4

Question Number : 53 Question Id : 2886072208 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of memory paging, the term "swap space" refers to: (choose the BEST option below)

a. a portion of OS memory used to copy variable values across processes
b. the top part of each page used to store dirty variable values
c. a partition of hard disk where temporarily unused memory pages are stored
d. a subset of CPU registers used for synchronization variables

Options :

2886078822. 1

2886078823. 2

2886078824. 3

2886078825. 4

Question Number : 54 Question Id : 2886072209 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is NOT shared across multiple threads of the same process?

a. Instruction memory
b. File descriptors
c. Stack memory
d. Heap memory

Options :

2886078826. 1

78827. 2

2886078828. 3

2886078829. 4

Question Number : 55 Question Id : 2886072210 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is a CPU instruction which can be used by the OS or an application to implement mutual exclusion locks?

a. TestAndSet
b. bzero
c. malloc
d. double.add

Options :

2886078830. 1

2886078831. 2

2886078832. 3

2886078833. 4

Question Number : 56 Question Id : 2886072211 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which among the following is NOT an advantage of modern cryptography, compared to classical cryptography?

a. Analyzed by best minds
b. Low cost in implementation
c. Can work over images, not just text
d. Secrecy of the algorithm gives better security

Options :

2886078834. 1

2886078835. 2

2886078836. 3

2886078837. 4

Question Number : 57 Question Id : 2886072212 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of server security, which type of defence is "logging and monitoring a server"?

a. Detect
b. Recover
c. Prevent
d. Deter

Options :

2886078838. 1

2886078839. 2

2886078840. 3

2886078841. 4

Question Number : 58 Question Id : 2886072213 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Using English alphabets, monoalphabetic cipher key space is about: (choose the BEST option below)

a. 26
b. 52
c. 26 factorial
d. 2 power 26

Options :

2886078842. 1

2886078843. 2

2886078844. 3

2886078845. 4

Question Number : 59 Question Id : 2886072214 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In cryptoanalysis, global deduction means: (choose the BEST option below)

a. finding the key
b. finding an alternate algorithm that helps in decryption
c. deriving plaintext (in full) from ciphertext
d. deriving partial plaintext from ciphertext

Options :

2886078846. 1

2886078847. 2

2886078848. 3

2886078849. 4

Question Number : 60 Question Id : 2886072215 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In DES, each round key is of size (in bits):

a. 32
b. 48
c. 64
d. 96

Options :

2886078850. 1

2886078851. 2

2886078852. 3

2886078853. 4

Question Number : 61 Question Id : 2886072216 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In CBC mode, if cipher block *i* is corrupted, which blocks of plaintext are also necessarily corrupted?

a. *i-1*
b. *i+1*
c. *i+k* where *k* is the key length in bits
d. *i+k-1* where *k* is the key length in bits

Options :

2886078854. 1

2886078855. 2

2886078856. 3

2886078857. 4

Question Number : 62 Question Id : 2886072217 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

In the context of cryptography, what is the modular inverse of 7 mod 13?

a. 1
b. 2
c. -7
d. -13

Options :

2886078858. 1

2886078859. 2

2886078860. 3

2886078861. 4

Question Number : 63 Question Id : 2886072218 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following is true of Merkel-Damagard construction? c is a input to the compression function and d is the hash output.

a. c0 has to be private
b. c < d
c. Compression function collision resistant means hash is collision resistant
d. Padding of messages is not allowed in hash construction

2886078862. 1

2886078863. 2

2886078864. 3

2886078865. 4

Question Number : 64 Question Id : 2886072219 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

If there are 23 people in a room, what is the chance two have the same birthday? Choose the BEST option below.

a. About 50%
b. About 25%
c. About 4%
d. About 1%

Options :

2886078866. 1

2886078867. 2

2886078868. 3

2886078869. 4

Question Number : 65 Question Id : 2886072220 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

For a 1000 bit message and 160 bit hash, how many messages on average map to the same output?

a. 160
b. 2 power 160
c. 840
d. 2 power 840

Options :

2886078870. 1

2886078871. 2

2886078872. 3

2886078873. 4

Question Number : 66 Question Id : 2886072221 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which of the following observations is/are correct with respect to error functions?

a. The sum of squares error function is more sensitive to outliers than the sum of absolute values error function
b. The sum of cubes error function is preferred to the sum of squares error function
c. The sum of absolute values error function is differentiable at all values of w
d. The sum of absolute values error function is discontinuous at some value of w

Options :

2886078874. 1

2886078875. 2

2886078876. 3

2886078877. 4

Question Number : 67 Question Id : 2886072222 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Which ONE of the following statements is correct?

a. Maximum likelihood Estimation (MLE) takes into account prior belief/knowledge about the parameters
b. Maximum Aposteriori estimation (MAP) takes into account prior belief/knowledge about the parameters
c. Maximum Likelihood Estimate of a parameter will always be lower than the Maximum Aposteriori estimate
d. Maximum Likelihood Estimate of a parameter will always be higher than the Maximum Aposteriori estimate

Options :

2886078878. 1

2886078879. 2

2886078880. 3

2886078881. 4

Question Number : 68 Question Id : 2886072223 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Suppose you are given the following prior probabilities for coin with parameter p as the probability of heads. p has only two possible values as per the prior: Pr(p=0.4) = 0.6 and Pr(p=0.8)=0.4. We observe three coin tosses landing twice on heads and once on tail. Use this prior to find the MAP estimate of p instead of the MLE estimate.

a. 0.4
b. 0.8
c. 0.25
d. 0.5

Options :

2886078882. 1

2886078883. 2

2886078884. 3

2886078885. 4

Question Number : 69 Question Id : 2886072224 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

What kind of behavior is expected when a graph between mean squared error (on the test set) and degree of polynomial to fit is plotted?

a. Monotonically increasing
b. Monotonically decreasing
c. First increases then decreases
d. First decreases then increases

Options :

2886078886. 1

2886078887. 2

2886078888. 3

2886078889. 4

Question Number : 70 Question Id : 2886072225 Question Type : MCQ Option Shuffling : No
Correct Marks : 2 Wrong Marks : 1

Regression is called linear when (choose the BEST option below)

a. it is capable of fitting y as a linear function of x
b. it is linear in the *w* vector
c. it can address linearly separable dataset
d. error decreases linearly with dataset size

Options :

2886078890. 1

2886078891. 2

2886078892. 3

2886078893. 4