Scientist Engineer SC Computer

[The probability density function of a random variable X is

$$f(x) = ke^{-|x|}, -\infty < x < -\infty$$

The value of k and the mean of the X are:

a) 1, ½
b) 1 ,0
c) ½, ½
d) ½, 0

एक यादृच्छिक चर X का संभाव्यता घनता फलन निम्नानुसार है-

$$f(x) = ke^{-|x|}, -\infty < x < -\infty$$

k का मान और X का माध्य क्या होगा?

a) 1, ½
b) 1 ,0
c) ½,½
d) ½, 0

Given the matrix, A = $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, The trace of A, Tr(A) = 0. The value of $\text{Tr}(A^8) + \text{Tr}(A^9)$ is:

a) 8

b) 16

c) 32

d) 0

दिए गए मैट्रिक्स A = $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ में, A का अनुरेख Tr(A) =0 है। $\text{Tr}(A^8) + \text{Tr}(A^9)$ का मान क्या होगा?

a) 8

b) 16

c) 32

d) 0

What is the largest possible value for the rank of A and the smallest possible value for the nullity of A, if A is a 5 x 3 matrix?

a) 5,3
b) 3,0
c) 5,0
d) 5,2

यदि A 5x3 मैट्रिक्स है, तो A की कोटि का अधिकतम संभव मान और A की शून्यता का न्यूनतम संभव मान क्या होगा?

a) 5 , 3
b) 3 , 0
c) 5 , 0
d) 5 , 2

Consider a FIFO page replacement policy based memory unit. Which of the following statements are TRUE?

a) Increasing the number of page frames always results in fewer page faults
b) Increasing the number of page frames always results in higher page faults
c) Decreasing the number of page frames always results in increased page faults
d) Increasing the number of page frames may result in increase or decrease in number of page faults

FIFO पेज replacement policy आधारित मेमोरी इकाई पर विचार करें। निम्नलिखित में से कौन-सा कथन सही है?

a) पेज फ्रेमों की संख्या बढ़ाने के परिणामस्वरूप सदैव पेज दोषों की संख्या कम होती है।
b) पेज फ्रेमों की संख्या बढ़ाने के परिणामस्वरूप सदैव पेज दोषों की संख्या बढ़ती है।
c) पेज फ्रेमों की संख्या कम करने के परिणामस्वरूप सदैव पेज दोषों की संख्या बढ़ती है।
d) पेज फ्रेमों की संख्या कम करने के परिणामस्वरूप पेज दोषों की संख्या बढ़ती या कम होती है।

Consider a system where each process has a virtual address space of 2^v bytes. The physical address space of the system is 2^p bytes, and the page size is 2^k bytes. What is the number of logical pages of a process and number of physical frames in the system?

a) 2^{p-k} , 2^{v-k}

b) v, k

c) 2^{v-k} , 2^{p-k}

d) $2^{v-k}, p-k$

एक प्रणाली पर विचार करें जहाँ प्रत्येक प्रक्रम का आभासी एड्रेस स्पेस 2^v बाइट है। प्रणाली का भौतिक एड्रेस स्पेस 2^p बाइट है और पेज का आकार 2^k बाइट है। प्रक्रम के तर्कसंगत पृष्ठों की संख्या और प्रणाली के भौतिक फ्रेमों की संख्या क्या है?

a) 2^{p-k} , 2^{v-k}

b) v, k

c) 2^{v-k} , 2^{p-k}

d) $2^{v-k}, p-k$

Consider the following line of code in a function of a process.

*int *y = (int *)malloc(50 * sizeof (int)) ;*

Where is the memory of the variable *y* allocated within the memory image of the process when this function is invoked and executed?

a) Heap
b) Stack
c) PCB (Process Control Block)
d) None of the these

एक प्रक्रम के फलन में निम्नलिखित कोड रेखा पर विचार कीजिए।

*int *y = (int *)malloc(50 * sizeof (int)) ;*

इस फलन के प्रारंभ और कार्यान्वयन के दौरान प्रक्रम की मेमोरी इमेज में चर y के लिए मेमोरी कहाँ आबंटित की जाती है?

a) Heap
b) Stack
c) PCB (Process Control Block)
d) उपर्युक्त में से कोई नहीं।

Which of the following conditions best describes for *Bounded Waiting* in process synchronization?

a) When a thread is executing in its critical section, no other threads can be executing in their critical sections
b) If no thread is executing in its critical section, and if there are some threads that wish to enter their critical sections, then one of these threads will get into the critical section.
c) Several processes access and manipulate the same data concurrently
d) After a thread makes a request to enter its critical section, there is a limit on the number of times that other threads are allowed to enter their critical sections, before the request is granted.

Process synchronization में *Bounded Waiting* की निम्नलिखित में से कौन-सी स्थिति में सर्वश्रेष्ठ व्याख्या की जा सकती है?

a) जब एक thread अपने क्रांतिक सेक्शन में निष्पादित हो रहा है, तब कोई अन्य thread उनके क्रांतिक सेक्शन में निष्पादित नहीं हो सकता है।
b) यदि कोई thread अपने क्रांतिक सेक्शन में निष्पादित नहीं हो रहा है, और यदि कुछ धागे उनके क्रांतिक सेक्शन में प्रवेश करने के इच्छुक हैं, तो उनमें से एक thread क्रांतिक सेक्शन में प्रवेश करेगा।
c) कई प्रक्रम संगामी रूप से उसी डेटा को प्राप्त और परिवर्तित कर सकते हैं।
d) एक thread के अपने critical section में प्रवेश के अनुरोध करने के बाद, अनुरोध की अनुमति देने से पूर्व अन्य धागों को उनके critical section में प्रवेश करने की अनुमति देने की संख्याओं की एक सीमा होती है।

Which of the following statements is/are True?

I. Given a CFG $G = (N, \Sigma, P, S)$ and a string $x \in \Sigma^*$, $x \in L(G)$ is decidable

II. Given CFG's G_1 and G_2, is $L(G_1) = L(G_2)$ is undecidable.

III. Given CFG's G_1 and G_2, is $L(G_1) = L(G_2)$ is decidable.

IV. Given a CFG $G = (N, \Sigma, P, S)$ and a string $x \in \Sigma^*$, $x \in L(G)$ is undecidable

a) I and II

b) II and IV

c) I and III

d) III and IV

निम्नलिखित में से कौन-सा/से कथन सही है/हैं?

I. दिया गया एक CFG $G = (N, \Sigma, P, S)$ और एक स्ट्रिंग $x \epsilon \Sigma^*$, $x \epsilon L(G)$ decidable है।

II. दिया गया CFG's G_1 और G_2, $L(G_1) = L(G_2)$ है- जो undecidable है।

III. दिया गया CFG's G_1 और G_2, $L(G_1) = L(G_2)$ है- जो decidable है।

IV. दिया गया एक CFG $G = (N, \Sigma, P, S)$ और एक स्ट्रिंग $x \epsilon \Sigma^*$, $x \epsilon L(G)$ undecidable है।

a) I और II

b) II और IV

c) I और III

d) III और IV

Consider the grammar defined by the following production rules, with two operators * and +

$S \rightarrow T * P$

$T \rightarrow U \mid U * T$

$P \rightarrow Q + P \mid Q$

$Q \rightarrow Id$

$U \rightarrow Id$

a) + is left associative, while * is right associative

b) + is right associative, while * is left associative

c) Both + and * are right associative

d) Both + and * are left associative

दो ऑपरेटरों * और + के साथ निम्नलिखित उत्पादन नियमों द्वारा परिभाषित ग्रामर पर विचार कीजिए।

$S \rightarrow T * P$

$T \rightarrow U \mid U * T$

$P \rightarrow Q + P \mid Q$

$Q \rightarrow Id$

$U \rightarrow Id$

a) + बायां साहचर्य है, जबकि * दायां साहचर्य है

b) + दायां साहचर्य है, जबकि * बायां साहचर्य है

c) + और * दोनों दायें साहचर्य हैं

d) + और * दोनों बायें साहचर्य हैं

For any given transition in a finite automaton with Q states, the number of possible states for DFA and NFA are (respectively):

a) $Q, 2^Q$

b) $1, Q$

c) $2, Q$

d) $2^Q, 2^Q$

Q अवस्थाओं के साथ एक finite automaton में किसी दिए गए transition के लिए, DFA और NFA (क्रमशः) के लिए संभावित अवस्थाएं क्या होंगी?

a) Q, 2^Q

b) 1, Q

c) 2, Q

d) 2^Q, 2^Q

Consider the following Syntax Directed Translation Scheme(SDTS), with non-terminals {S, A} and terminals {a, b}.

$S \rightarrow Aa$ { print 1}

$S \rightarrow a$ { print 2 }

$A \rightarrow Sb$ { print 3 }

Using the above SDTS, the output printed by a bottom-up parser, for the input aba is

a) 2 3 1

b) 1 3 2

c) 2 1 3

d) 1 2 3

गैर-टर्मिनलों {S,A} और टर्मिनलों {a,b} के साथ निम्नलिखित Syntax Directed Translation Scheme (SDTS) पर विचार कीजिए-

$S \rightarrow Aa$ { print 1}

$S \rightarrow a$ { print 2 }

$A \rightarrow Sb$ { print 3 }

उपर्युक्त SDTS का उपयोग करते हुए, इनपुट aba के लिए, बॉटम अप पार्सर द्वारा प्रिंट किया गया आउटपुट क्या होगा?

a) 2 3 1
b) 1 3 2
c) 2 1 3
d) 1 2 3

Among simple LR (SLR), canonical LR, and look-ahead LR (LALR), which of the following pairs identify the order of the method that is very easy to implement and the method that is most powerful?

a) Canonical LR, LALR
b) SLR, LALR
c) LALR, Canonical LR
d) SLR, Canonical LR

Simple LR (SLR), Canonical LR और लुक-अहेड LR (LALR) में से, निम्नलिखित में से कौन-से युग्म क्रियान्वित करने में बहुत आसान विधि और सबसे शक्तिशाली विधि, दोनों का क्रम अभिनिर्धारित करते हैं?

a) Canonical LR, LALR
b) SLR, LALR
c) LALR, Canonical LR
d) SLR, Canonical LR

What happens when a bit-string is XORed with itself n-times as shown?

$[\, B \oplus (\, B \oplus (\, B \oplus (B \ldots\ldots\ldots$ n times$)]$

a) Complements when n is even
b) Remains unchanged when n is even
c) Divides by 2^n always
d) None of the above

जब एक बिट-स्ट्रिंग को नीचे दर्शाए अनुसार स्वयं के साथ n-times XOR किया जाता है, तो क्या होता है?

$[B \oplus (B \oplus (B \oplus (B$ .... n times)]

a) n के सम होने पर कॉम्प्लिमेंट होती है।

b) n के सम होने पर अपरिवर्तित रहती है।

c) हमेशा 2^n से विभाजित होती है।

d) उपर्युक्त में से कोई नहीं।

Consider the minterm list form of a Boolean Function F given below. F(P, Q, R, S) $= \Sigma m(0, 2, 8, 9, 11, 10, 12, 13, 15, 14)$ What is the equivalent Boolean expression in sum-of-products form?

a) $C + \overline{A}BD + \overline{B}\,\overline{D}$

b) $C + \overline{B}\,\overline{D}$

c) $C + \overline{B}\,\overline{C}\,\overline{D}$

d) None of the above

निम्नलिखित बूलियन फलन F के मिनटर्म लिस्ट प्रकार पर विचार कीजिए।

$F(P, Q, R, S) = \Sigma_m(0, 2, 8, 9, 11, 10, 12, 13, 15, 14)$

उत्पाद-के-योग के रूप में समान बूलियन अभिव्यक्ति क्या होगी?

a) $C + \overline{A}BD + \overline{B}\,\overline{D}$

b) $C + \overline{B}\,\overline{D}$

c) $C + \overline{B}\,\overline{C}\,\overline{D}$

d) उपर्युक्त में से कोई नहीं।

Consider the Boolean operator # with the following properties:

$x \# 0 = x$, $x \# 1 = \underline{x}$, $x \# x = 0$ and $x \# \underline{x} = 1$.

Then $x \# y$ is equivalent to

a) $\underline{x}y + x\underline{y}$

b) $\underline{x}y + \underline{y}$

c) $\underline{x}y + \underline{x}\,\underline{y}$

d) $\underline{x}\,\underline{y} + xy$

निम्नलिखित गुणधर्म के साथ बूलियन संचालक # पर विचार कीजिए।

$x \# 0 = x,\ x \# 1 = \underline{x},\ x \# x = 0$ and $x \# \underline{x} = 1.$

तब $x \# y$ किसके बराबर होगा?

a) $\underline{x}y + x\underline{y}$

b) $\underline{x}y + \underline{y}$

c) $\underline{x}y + \underline{x}\,\underline{y}$

d) $\underline{x}\,\underline{y} + xy$

Consider the following sequence of micro–operations. (MBR = Memory Base Register, PC = Program Counter, MAR = Memory Address Register.)

MBR ← PC

MAR ← X

PC ← Y

Memory ← MBR

Which one of the following is a possible operation performed by this sequence?

a) Instruction fetch

b) Operand fetch

c) Initiation of interrupt service

d) Conditional branch

सूक्ष्म-संचालकों के निम्नलिखित अनुक्रम पर विचार कीजिए।

(MBR = Memory Base Register, PC = Program Counter,
MAR = Memory Address Register)

$MBR \leftarrow PC$

$MAR \leftarrow X$

$PC \leftarrow Y$

$Memory \leftarrow MBR$

निम्नलिखित में से क्या इस अनुक्रम द्वारा निष्पादित संभावित प्रचालन है?

a) Instruction Fetch

b) Operand Fetch

c) Interrupt Service की शुरुआत

d) Conditional Branch

Instructions execution in a processor is divided into 5 stages. Instruction Fetch (IF), Instruction Decode (ID) , Operand Fetch (OF), Execute (EX), and Write Back (WB), These stages take 5, 4, 20, 10 and 3 nanoseconds (ns) respectively. A pipelined implementation of the processor requires buffering between each pair of consecutive stages with a delay of 2ns. The execution time for 20 instructions on this pipeline is:

a) 528 ns
b) 288 ns
c) 286 ns
d) 290 ns

एक प्रक्रम में निर्देश निष्पादनों को 5 चरणों- इंस्ट्रक्शन फेच (IF) इंस्ट्रक्शन डीकोड (ID), ओपरेंड फेच (OF), एक्सीक्यूट (EX) तथा राइट बैक (WB) में विभाजित किया गया है। ये चरण क्रमशः 5, 4, 20, 10 और 3 नैनोसेकेंड (ns) लेते हैं। प्रक्रम के पाइपलाइन क्रियान्वयन में क्रमागत चरणों के प्रत्येक युग्म के बीच 2ns के विलंब के साथ बफरिंग की आवश्यकता होती है। इस पाइपलाइन में 20 निर्देशों के निष्पादन में कितना समय लगेगा?

a) 528 ns
b) 288 ns
c) 286 ns
d) 290 ns

A processor can support a maximum memory of 8 GB, where the memory is word-addressable (a word consists of two bytes). The size of the address bus of the processor is at least ___ bits.

a) 31
b) 16
c) 32
d) None of the above

एक processor अधिकतम 8GB मेमोरी को सपोर्ट कर सकता है, जहाँ मेमोरी वर्ड एड्रेसेबल (एक वर्ड में दो बाइट हैं) है। processor की एड्रेस बस का आकार कम-से-कम _____ बिट होगा।

a) 31
b) 16
c) 32
d) उपर्यूक्त में से कोई नहीं।

Which of the following addressing mode is best suited to access elements of an array of contiguous memory locations?

a) Indexed addressing mode
b) Relative address mode
c) Base Register addressing mode
d) Displacement mode

Contiguous Memory locations के आव्यूह के घटकों का अभिगम करने के लिए निम्नलिखित में से सर्वाधिक उपयुक्त एड्रेसिंग मोड कौन-सा है?

a) इंडेक्स्ड एड्रेसिंग मोड
b) रिलेटिव एड्रेस मोड
c) बेस रजिस्टर एड्रेसिंग मोड
d) डिस्प्लेसमेंट मोड

Consider the schema R(S, T, U, V) and the dependencies S→T, T→U, U→V, V→S. Let R= {R1, R2} such that R1 ∩ R2 = Φ. Then the decomposition is:

a) not in 2NF
b) in 2NF but not in 3NF
c) in 3NF but not in 2NF
d) in both 2NF and 3NF

Schema R (S, T, U, V) और dependencies S→T, T→U, U→V, V→S पर विचार कीजिए। मान लें कि R= {R1, R2} इस प्रकार है कि R1 ∩ R2 = Φ. इसका वियोजन _____ होगा।

a) 2NF में नहीं
b) 2NF में, किंतु 3NF में नहीं
c) 3NF में, किंतु 2NF में नहीं
d) 2NF और 3NF दोनों में

A FAT (file allocation table) based file system is being used and the total overhead of each entry in the FAT is 4 bytes in size. Given a 100 x 10^6 bytes' disk on which the file system is stored and data block size is 10^3 bytes, the maximum size of a file that can be stored on this disk in units of 10^6 bytes is _________.

a) 99.35 to 99.45

b) 99.55 to 99.65

c) 100.5 to 101.4

d) 97.2 to 98.5

एक FAT (file allocation table) आधारित फाइल प्रणाली का प्रयोग किया जा रहा है और FAT में प्रत्येक प्रविष्टि के कुल शीर्ष का आकार 4 बाइट है। 100x10^6 आकार की डिस्क पर फाइल प्रणाली संग्रहित की गई है और डेटा ब्लॉक आकार 10^3 बाइट है। इस डिस्क पर 10^6 बाइट की इकाई में संग्रहित की जा सकने वाली फाइल का अधिकतम आकार क्या होगा?

a) 99.35 से 99.45

b) 99.55 से 99.65

c) 100.5 से 101.4

d) 97.2 से 98.5

Which of the following is are drawbacks of the Two-Phase Locking (2-PL) mechanism?

I. Deadlock
II. Serializability
III. Starvation
IV. Cascading Rollback

a) II only
b) I, II, III
c) I and IV
d) I, III, IV

द्वि-फेज लॉकिंग (2-PL) mechanism की कमियाँ क्या है/हैं?

I. डेडलॉक
II. सीरियलाइजेबिलिटी
III. स्टार्वेशन
IV. कास्केडिंग रोलबैक

a) केवल II
b) I, II, III
c) I और IV
d) I, III, IV

The given table has two attributes A and C where A is the primary key and C is the foreign key referencing A with on-delete cascade.

The set of all tuples that must be additionally deleted to preserve referential integrity when the tuple (4, 3) is deleted is

A	C
2	4
3	4
4	3
5	2
7	2
9	5
6	4

a) (3,4), (4,3) and (6,4)

b) (5,2), (7,2) and (9,5)

c) (2,4), (5,2), (7,2), (9,5), (3,4), (6,4)

d) (2,4), (3,4) and (6,4)

दी गई तालिका में A और C दो गुण हैं, जहाँ A primary key और C foreign key है, जो ऑन-डिलीट कास्केड के साथ A को संदर्भित करती है। जब ट्यूपल (4,3) को डिलीट किया जाता है तो संदर्भ अखंडता को बनाए रखने के लिए ट्यूपल्स के किन सभी सेट को भी डिलीट करना होगा?

A	C
2	4
3	4
4	3
5	2
7	2
9	5
6	4

a) (3,4), (4,3) और (6,4)

b) (5,2), (7,2) और (9,5)

c) (2,4), (5,2), (7,2), (9,5), (3,4), (6,4)

d) (2,4), (3,4) और (6,4)

Consider the relation scheme R = {E, F, G, H, I, J, K, L, M, N} and the set of functional dependencies {{E, F} → {G}, {F} → {I, J}, {E, K} → {H, L, M}, {L} → {N}} on R. What is the Key for R?

a) {E, F}
b) {E, K}
c) {E, F, L}
d) {E, F, K}

संबंध योजना R = {E, F, G, H, I, J, K, L, M, N} और functional dependencies के सेट {{E, F} → {G}, {F} → {I, J}, {E, K} → {H, L, M}, {L} → {N}} on R पर विचार कीजिए। R के लिए कुंजी क्या होगी?

a) {E, F}
b) {E, K}
c) {E, F, L}
d) {E, F, K}

Which of the following is/are TRUE?

I. No relation can be in both BCNF and 3NF

II. Every relation in BCNF is also in 3NF

III. A relation R is in 3NF if every non-prime attribute of R is fully functionally dependent on every key of R.

IV. Every relation in 3NF is also in BCNF

a) I and III

b) III

c) IV

d) II

निम्नलिखित में से क्या सही है/ हैं?

I. कोई relation BCNF और 3NF में एक सांथ नहीं हो सकता।

II. BCNF में प्रत्येक relation 3NF में भी होता है।

III. यदि R का प्रत्येक non-prime attribute R की प्रत्येक कुंजी पर पूर्ण रूप से functionally dependent है तो relation R 3NF में होगा।

IV. 3NF में होने वाला हर relation BCNF में भी होता है।

a) I और III

b) III

c) IV

d) II

The hamming distance between the octets of 0x0A and 0x05 is

a) 7
b) 5
c) 8
d) 4

0x0A और 0x05 के octets के बीच की हैमिंग दूरी कितनी होगी?

a) 7
b) 5
c) 8
d) 4

In a class B network on the internet, the subnet mask is 255.255.240.0. What is the maximum number of hosts per subnet?

a) 4096

b) 2046

c) 2048

d) 4094

इंटरनेट पर एक श्रेणी B नेटवर्क में, सबनेट मास्क 255.255.240.0 है। प्रति सबनेट अधिकतम कितने होस्ट हो सकते हैं?

a) 4096

b) 2046

c) 2048

d) 4094

A Pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces 1000 frames per second?

a) 250 frames
b) 150 frames
c) 80 frames
d) 135 frames

200 kbps के सहभागी चैनल पर एक Pure ALOHA नेटवर्क 200-बिट फ्रेम प्रसारित करता है। यदि प्रणाली (सभी स्टेशन एकसाथ) 1000 फ्रेम प्रति सेकंड उत्पादित करते हैं तो थ्रूपुट कितना होगा?

a) 250 फ्रेम
b) 150 फ्रेम
c) 80 फ्रेम
d) 135 फ्रेम

Count to infinity is a problem associated with

a) Link state routing protocol
b) TCP for congestion control
c) Distance vector routing protocol
d) DNS while resolving host name

काउंट टू इनफिनिटी (Count to Infinity) की समस्या किससे संबंधित है?

a) लिंक स्टेट रूटिंग प्रोटोकॉल
b) congestion नियंत्रण के लिए TCP
c) Distance vector रूटिंग प्रोटोकॉल
d) होस्ट नाम ज्ञात करने के दौरान DNS

ARP request and reply packets are

a) Broadcast and Unicast respectively
b) Broadcast and Broadcast respectively
c) Unicast and Multicast respectively
d) Multicast and Broadcast respectively

ARP अनुरोध और प्रत्युत्तर पैकेट ____ होते हैं।

a) क्रमशः ब्रॉडकास्ट और यूनिकास्ट
b) क्रमशः ब्रॉडकास्ट और ब्रॉडकास्ट
c) क्रमशः यूनिकास्ट और मल्टीकास्ट
d) क्रमशः मल्टीकास्ट और ब्रॉडकास्ट

Consider the following C language program

```
# include <stdio.h>
# define print(x)  printf ("%d", x)
int x;
void Q(int z) {
        z *= x;
        print(z);
}
void P(int *y) {
        int x = *y+2;
        Q(x);
        *y = x-1;
        print(x);
}
main(void) {
        x=6;
        P(&x);
        print(x);
        getchar();
}
```

The output of the program is:

a) 4887

b) 4886

c) 1248

d) 1246

निम्नलिखित C लैंग्वेज प्रोग्राम पर विचार कीजिए।

```
# include <stdio.h>
# define print(x)  printf ("%d", x)
int x;
void Q(int z) {
    z *= x;
    print(z);
}
void P(int *y) {
    int x = *y+2;
    Q(x);
    *y = x-1;
    print(x);
}
main(void) {
    x=6;
    P(&x);
    print(x);
    getchar();
}
```

प्रोग्राम का आउटपुट ____ होगा।

a) 4887

b) 4886

c) 1248

d) 1246

Consider the following C program:

```c
#include <stdio.h>

void first( ){
   printf("Hello World");
}
void main() {

   void *ptr() = first;
   ptr++;
   ptr();
}
```

Which of the following is TRUE about the program:

a) Program will compile successfully and run without error

b) Program will not compile successfully due to assignment to *ptr*

c) Program will not compile due to illegal increment operation on void pointer

d) Both b and c

निम्नलिखित C प्रोग्राम पर विचार कीजिए।

```
#include <stdio.h>
void first( ){
   printf("Hello World");
}
void main(){
   void *ptr() = first;
   ptr++;
   ptr();
}
```

प्रोग्राम के बारे में निम्नलिखित में से क्या सही है?

a) प्रोग्राम सफलतापूर्वक compile होगा और बिना त्रुटि के चलेगा।

b) *ptr* से असाइमेंट के कारण प्रोग्राम सफलतापूर्वक compile नहीं होगा।

c) वॉइड पाइन्टर पर अवैध इन्क्रीमेंट प्रचालन के कारण प्रोग्राम compile नहीं होगा।

d) b और c दोनों

What does the following C-statement declare?

*int (* f) (int *) ;*

a) A function that takes an integer as argument and returns an integer pointer.

b) A pointer to a function that takes an integer pointer as argument and returns an integer.

c) A function that takes an integer pointer as argument and returns an integer.

d) A function that takes an integer as argument and returns a function pointer.

निम्नलिखित C-कथन क्या दर्शाता है?

*int (* f) (int *) ;*

a) एक फलन जो तर्क के रूप में integer लेता है और integer pointer वापस करता है।

b) एक फलन का pointer जो तर्क के रूप में integer pointer लेता है और पूर्णांक वापस करता है।

c) एक फलन जो तर्क के रूप में integer pointer लेता है और integer वापस करता है।

d) एक फलन जो तर्क के रूप में integer लेता है और फलन pointer वापस करता है।

Given any two functions $f(\cdot)$ and $g(\cdot)$, which of the following is TRUE about $h(n) = f(n) + g(n)$

I. $h(n)$ is $\Theta(\max\{f(n), g(n)\})$.
II. $h(n)$ is $\Omega(\max\{f(n), g(n)\})$.
III. $h(n)$ is $O(\max\{f(n), g(n)\})$.

a) I only
b) II only
c) III only
d) All of the above

कोई दो फलन $f(\cdot)$ and $g(\cdot)$ दिए जाने पर, $h(n) = f(n) + g(n)$ के संबंध में निम्नलिखित में से क्या सही होगा?

I. $h(n)$ is $\Theta(\max\{f(n), g(n)\})$.
II. $h(n)$ is $\Omega(\max\{f(n), g(n)\})$.
III. $h(n)$ is $O(\max\{f(n), g(n)\})$.

a) केवल I
b) केवल II
c) केवल III
d) उपर्युक्त सभी

Let A1, A2, A3, and A4 be four matrices of dimensions 10 x 5, 5 x 20, 20 x 10, and 10 x 5, respectively. The minimum number of scalar multiplications required to find the product A1 x A2 x A3 x A4 using the basic matrix multiplication method is

a) 1500
b) 2050
c) 1550
d) 1750

क्रमशः 10 x 5, 5 x 20, 20 x 10, और 10 x 5, आयाम के चार मैट्रिक्स A1, A2, A3 और A4 लें। बेसिक मैट्रिक्स मल्टीप्लिकेशन विधि का प्रयोग कर A1 x A2 x A3 x A4 के उत्पाद का पता करने के लिए आवश्यक न्यूनतम अदिश गुणन संख्या क्या होगी?

a) 1500
b) 2050
c) 1550
d) 1750

Which one of the following inequalities hold asymptotically true?

a) $\log n < n \log n < n$

b) $\sqrt{(n)} < n \log n < n$

c) $\log n < \sqrt{(n)} < n \log n$

d) $\log n < n^{1.1} < n$

निम्नलिखित में से कौन सी असमानताएं asymptotically सही हैं?

a) $\log n < n \log n < n$

b) $\sqrt{(n)} < n \log n < n$

c) $\log n < \sqrt{(n)} < n \log n$

d) $\log n < n^{1.1} < n$

A hash function h defined as $h(key) = key \ \ mod \ \ 7$, with Linear Probing, is used to insert the keys 44, 45, 79, 55, 91, 18, 63 into a table indexed from 0 to 6. What will be the location of the key 91?

a) 0

b) 5

c) 1

d) 4

Linear Probing के साथ एक हैश फलन h को $h(key) = key$ mod 7 के रूप में परिभाषित किया जाता है, जिसे 0 से 6 तक इंडेक्स किए गए टेबल में keys 44, 45, 79, 55, 91, 18, 63 प्रविष्ट करने के लिए प्रयोग किया जाता है। key 91 का स्थान क्या होगा?

a) 0

b) 5

c) 1

d) 4

Consider a complete binary tree with 7 nodes. Let A denote the set of first 3 elements obtained by performing Breadth-First Search (BFS) starting from the root. Let B denote the set of first 3 elements obtained by performing Depth-First Search (DFS) starting from the root. The value of |A – B| is

a) 2
b) 1
c) 3
d) 0

विचार करें कि एक संपूर्ण बायनरी ट्री के 7 नोड्स हैं। मानें कि A, रूट से प्रारंभ करते हुए Breadth-First Search (BFS) द्वारा प्राप्त प्रथम 3 घटकों के सेट को निरूपित करता है। मानें कि B, रूट से प्रारंभ करते हुए Depth-First Search (DFS) द्वारा प्राप्त प्रथम 3 घटकों के सेट को निरूपित करता है। |A – B| का मान क्या होगा?

a) 2
b) 1
c) 3
d) 0

Which of these data structures can be used for efficiently storing the symbol table in a compiler implementation?

a) B+ Tree
b) Binary Search Tree
c) Hash Table
d) Heap

एक कंपाइलर क्रियान्वयन में सिंबल टेबल को प्रभावी रूप से स्टोर करने के लिए निम्नलिखित में से किस data structures का उपयोग किया जा सकता है?

a) B+ ट्री
b) बायनरी सर्च ट्री
c) हैश टेबल
d) हीप

A company needs to develop digital signal processing software for one of its newest inventions. The software is expected to have 40000 lines of code. The company needs to determine the effort in person-months needed to develop this software using the basic COCOMO model. The multiplicative factor for this model is given as 2.8 for the software development on embedded systems, while the exponentiation factor is given as 1.20. What is the estimated effort in Person-Months?

a) 234.25
b) 932.50
c) 287.80
d) 122.40

एक कंपनी को अपने एक नवीनतम आविष्कार के लिए डिजिटल सिग्नल प्रोसेसिंग विकसित करने की आवश्यकता है। इस सॉफ्टवेयर में 40000 लाइन कोड होने की संभावना है। कंपनी को बेसिक COCOMO मॉडल का उपयोग करते हुए इस सॉफ्टवेयर के विकास के लिए आवश्यक प्रयासों को Person-Months की इकाई में निर्धारण करने की आवश्यकता है। इस मॉडल के लिए एम्बेडेड सिस्टम पर विकसित सॉफ्टवेयर का गुणनात्मक घटक 2.8 दिया गया है, जबकि चरघातांकी घटक 1.2 के रूप में दिया गया है। Person-Months की इकाई में आकलित प्रयास कितना होगा?

a) 234.25

b) 932.50

c) 287.80

d) 122.40

How many onto (or surjective) functions are there from an n-element ($n >= 2$) set to a 2 -element set?

a) 2^n

b) $2^n - 1$

c) $2^n - 2$

d) $2(2^n - 1)$

एक n-element (n >= 2) सेट से एक 2-element सेट तक कितने onto (या surjective) फलन होते हैं?

a) 2^n
b) $2^n - 1$
c) $2^n - 2$
d) $2(2^n - 1)$

Read the following statements about principal components analysis (PCA)

A: The principal components are eigenvectors of the centred data matrix.

B: The principal components are right singular vectors of the centred data matrix.

C: The principal components are eigenvectors of the sample covariance matrix.

D: The principal components are right singular vectors of the sample covariance matrix

Which of these statements is/are true?

a) Only A
b) All except A
c) Only B and C
d) Only C and D

प्रिंसीपल कंपोनेंट एनालिसिस (PCA) के बारे में निम्नलिखित कथन पढ़ें-

A: प्रिंसीपल कंपोनेंट सेंटर्ड डेटा मैट्रिक्स के Eigen vectors हैं।

B: प्रिंसीपल कंपोनेंट सेंटर्ड डेटा मैट्रिक्स के दायें Singular vectorsहैं।

C: प्रिंसीपल कंपोनेंट सैंपल covariance मैट्रिक्स के Eigen vectors हैं।

D: प्रिंसीपल कंपोनेंट सैंपल covariance मैट्रिक्स के दायें Singular vectors हैं।

उपर्युक्त में से कौन-सा/से कथन सही है/हैं?

a) केवल A
b) A के अलावा सभी
c) केवल B और C
d) केवल C और D

A decision tree grown to full depth is more likely to

I. Fit the noise in the data.
II. Suffer from over fitting
III. Generalizes well on unseen data

a) Only I
b) Both I and II
c) Only III
d) Both I and III

पूर्ण गहराई तक विकसित डिसीज़न ट्री में अधिक संभावना किस चीज की होती है?

I. data में noise फिट करने की।

II. ओवर फिटिंग की।

III. अनदेखे डेटा पर भलीभांति Generalize करने की।

a) केवल I
b) I और II दोनों
c) केवल III
d) I और III दोनों

Consider the minimizer ω^* of the ℓ_2-regularized least squares objective $J(\omega) = |X\omega - y|^2 + \lambda|\omega|^2$ with $\lambda > 0$. Which of the following are true?

a) ω^* exists if and only if $X^T X$ is non-singular
b) $X\omega^* = y$
c) The minimizer ω^* is unique
d) $\omega^* = X^+ y$, where X^+ is the pseudoinverse of X

$\lambda > 0$ के साथ ℓ_2- regularized least squares objective $J(\omega) = |X\omega - y|^2 + \lambda|\omega|^2$ के मिनीमाइज़र ω^* पर विचार कीजिए। निम्नलिखित में से क्या सही है?

a) ω^* केवल तभी विद्यमान होता है यदि $X^T X$ गैर-एकल होता है

b) $X\omega^* = y$

c) मिनीमाइज़र ω^* unique होता है।

d) $\omega^* = X^+ y$, जहाँ X^+, X का pseudoinverse होता है।

A multiclass classification problem of K class can be solved wither via considering the multiclass case to be a 1-vs.-all scenario with K binary classifiers or via a multiclass classifier such as softmax regression. When would one prefer softmax regression as opposed to K 1-vs.-all logistic regression for multiclass classification?

a) When the classes are mutually exclusive

b) When the classes are not linearly separable

c) When the classes are not mutually exclusive

d) Both work equally well

K क्लास की मल्टीक्लास क्लासिफायर समस्या को या तो K बायनरी क्लासिफायर्स के साथ मल्टीक्लास केस को 1-vs.-all विचार करते हुए या फिर softmax regression जैसे मल्टीक्लास क्लासिफायर द्वारा हल किया जा सकता है। मल्टीक्लास क्लासिफिकेशन के लिए कोई व्यक्ति K 1-vs.-all logistic regression के मुकाबले softmax regression को कब वरीयता देगा?

a) जब क्लासेस पारस्परिक रूप से विशिष्ट होती हैं।
b) जब क्लासेस रेखीय तौर पर पृथक्करण योग्य नहीं होती हैं।
c) जब क्लासेस पारस्परिक रूप से विशिष्ट नहीं होती हैं।
d) दोनों विधियाँ समान रूप से भलीभांति कार्य करती हैं।

Sigmoidal activation function in neural networks suffer from which of the following practical problems?

a) It does not work well with entropy loss function
b) It can have negative values
c) Gradients are small for values away from 0, leading to the "vanishing Gradient" problem for large or recurrent neural nets.
d) It is convex, and convex functions cannot solve nonconvex problems

न्यूरल नेटवर्कों में Sigmoidal activation function में निम्नलिखित में से कौन-सी प्रायोगिक समस्या आती है?

a) यह entropy loss फलन के साथ भलीभांति कार्य नहीं करता है।
b) इसमें negative मान हो सकते हैं।
c) 0 से आगे के मान के लिए ग्रेडिएंट छोटे होते हैं, जिससे विशाल या recurrent न्यूरल नेट के लिए "vanishing Gradient" समस्या हो सकती है।
d) यह convex होता है, और convex फलन गैर-अवमुख समस्याओं को हल नहीं कर सकते हैं।

Consider one layer of weights (edges) in a convolutional neural network (CNN) for grayscale images, connecting one layer of units to the next layer of units. Which one of the type of layer has the fewest parameters to be learned during training?

a) A convolutional layer with 10, 3 x 3 filters.
b) A fully-connected layer from 20 hidden units to 4 output units.
c) A convolutional layer with 8, 5 x 5 filters.
d) A max-pooling layer that reduces a 10 x 10 images to 5 x 5

Grayscale प्रतिबिंबों के लिए एक संवलन न्यूरल नेटवर्क (CNN) में भारण (छोरों) के एक स्तर पर विचार कीजिए, जो इकाइयों के एक स्तर को इकाइयों के अगले स्तर से जोड़ता है। प्रशिक्षण के दौरान किस एक प्रकार के स्तर में कम-से-कम सीखने योग्य parameters होते हैं?

a) 10, 3 x 3 फिल्टर वाला convolutional layer
b) 20 प्रछन्न इकाइयों के fully-connected layer से 4 आउटपुट इकाइयाँ
c) 8, 5 x 5 फिल्टर वाला convolutional layer
d) Max-pooling layer जो 10 x 10 प्रतिबिंबों को 5 x 5 तक घटाता है

Which of the following statements on regularization are true?

I. Batch normalization can have an implicit regularizing effect, especially with smaller minibatches.
II. Using L-2 regularization enforces a Laplacian prior on your network weights.
III. Using L-2 regularization enforces a Gaussian prior on your network weights.
IV. Choice of regularization factor can cause your model to underfit.

a) II and IV
b) I, III and IV
c) I and III
d) IV only

नियमितीकरण पर निम्नलिखित में से कौन-से कथन सही हैं?

I. बैच regularization का अस्पष्ट प्रभाव हो सकता है, विशेषकर छोटे मिनीबैचों के साथ।

II. L-2 regularization का प्रयोग आपके नेटवर्क भारण पर Laplacian prior प्रवर्तित करता है।

III. L-2 नियमितीकरण का प्रयोग आपके नेटवर्क भारण पर Gaussian prior प्रवर्तित करता है।

IV. Regularization factor का चुनाव आपके मॉडल को अंडरफिट कर सकता है।

a) II और IV

b) I, III और IV

c) I और III

d) केवल IV

The logit function, L(x) is defined as the log of odds function. What is the range of the logit function in the domain x = [0,1]?

a) $(0, \infty)$

b) $(0, 1)$

c) $(-\infty, \infty)$

d) $(-\infty, 0)$

Logit function, L(x) को log of odds function के रूप में परिभाषित किया जाता है। डोमेन x = [0,1] में Logit function की सीमा क्या होगी?

a) $(0, \infty)$
b) $(0, 1)$
c) $(-\infty, \infty)$
d) $(-\infty, 0)$

In a Support Vector Machine (SVM) specified with weight W and bias b and the margin value fixed to 1, the distance of the support vectors from the separating hyperplane is:

a) $||W||_1$
b) $||W + b||_1$
c) $\frac{||W||_1}{||W + b||_2}$
d) $\frac{1}{||W||_2}$

भार W और बायस b के साथ विनिर्दिष्ट तथा सीमा मान 1 पर नियत की गई Support Vector Machine (SVM) में, separating hyperplane से support vectors की दूरी कितनी होगी?

a) $||W||_1$

b) $||W + b||_1$

c) $\frac{||W||_1}{||W + b||_2}$

d) $\frac{1}{||W||_2}$

The technique that combines the predictions from multiple machine learning algorithms together to make more accurate predictions than any individual model is called:

a) Reinforcement learning

b) Transfer learning

c) Ensemble learning

d) Inductive learning

एकाधिक मशीन लर्निंग algorithms से प्राप्त पूर्वानुमानों का संयोजन कर किसी भी एकल मॉडल से अधिक सटीक पूर्वानुमान लगाने वाले मॉडल को क्या कहा जाता है?

a) Reinforcement लर्निंग

b) Transfer लर्निंग

c) Ensemble लर्निंग

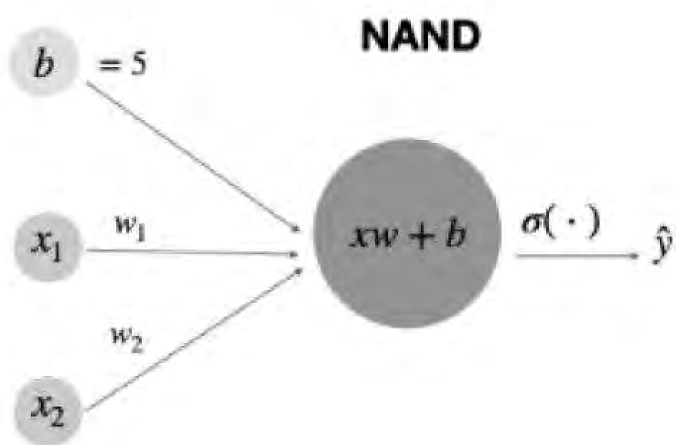
d) Inductive लर्निंग

Consider a single unit in a neural network that receives two binary inputs x1, x2 ∈ {0, 1} and computes a linear combination followed by a threshold activation function, namely,

$\sigma(z) = 1, z \geq 0$

$\quad\quad 0$, otherwise

The unit is illustrated below. We have chosen a bias term of b = 5. The weights w_1 and w_2 that allow to compute the NAND function are



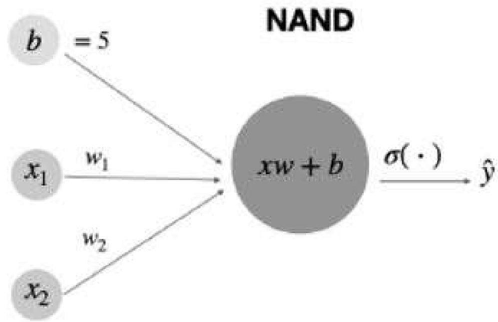
a) $w_1 = 0, w_2 = 0$

b) $w_1 = 1, w_2 = 1$

c) $w_1 = -1, w_2 = 1$

d) $w_1 = -3, w_2 = -3$

एक neural नेटवर्क में एकल इकाई पर विचार कीजिए जो दो बायनरी इनपुट x1, x2 ∈ {0, 1}2 प्राप्त करता है और एक थ्रेशोल्ड एक्टिवेशन फलन तथा रैखिक संयोजन का निम्नानुसार अभिकलन करता है-



$\sigma(z) = 1, z \geq 0$
अन्यथा 0,

उक्त इकाई का चित्र निम्नानुसार है। हमने बायस b = 5 का चयन किया है। NAND फलन का अभिकलन करने वाले भार w_1 और w_2 क्या होंगे?

a) $w_1 = 0, w_2 = 0$
b) $w_1 = 1, w_2 = 1$
c) $w_1 = -1, w_2 = 1$
d) $w_1 = -3, w_2 = -3$

संवलन नेटवर्क संरचना में *ड्रॉपआउट* का मुख्य उद्देश्य क्या होता है?

a) आउटपुट आयामों को घटाना
b) नेटवर्क को vanishing gradient से बचाना
c) ट्रेनिंग डेटा पर की ओवरफिटिंग को रोकना
d) Learning rate को बढ़ाना

What is the main purpose of *Dropout* in a neural network architecture?

a) Reduce the output dimensions

b) Prevent network from vanishing gradient

c) Prevent overfitting of on the training data

d) Increase learning rate

संवलन नेटवर्क संरचना में *ड्रॉपआउट* का मुख्य उद्देश्य क्या होता है?

a) आउटपुट आयामों को घटाना

b) नेटवर्क को vanishing gradient से बचाना

c) ट्रेनिंग डेटा पर की ओवरफिटिंग को रोकना

d) Learning rate को बढ़ाना

Which of the following statements about using convolutional layers instead of fully connected ones for visual tasks are TRUE:

A. They reduce the number of hidden layers

B. They enable spatial context modelling

C. The model becomes translation invariant

D. The number of parameters in the model increases

E. Enables increased parameter sharing

a) All of the above

b) B, C, E

c) B, D, E

d) A, B, D, E

दृश्य संबंधी कार्यों के लिए पूर्णतः संबंधित स्तरों के स्थान पर convolutional layers के प्रयोग के संबंध में निम्नलिखित में से कौन-से कथन सही हैं?

A. ये hidden layers की संख्या घटाते हैं।

B. ये spatial context modelling को प्रवर्तित करते हैं।

C. मॉडल translation invariant बन जाता है।

D. मॉडल में parameters की संख्या बढ़ जाती है।

E. बढ़ी parameters sharing प्रवर्तित करते हैं।

a) उपर्युक्त सभी

b) B, C, E

c) B, D, E

d) A, B, D, E

Let,

p = a number from {8, 9, 10, 11, 12}

q = not a composite number

r = a square number

s = a prime number

Then, what is the value of $\sim ((p \rightarrow \sim q) \wedge (\sim r \vee \sim s))$?

a) { 9, 11 }

b) { 8, 9, 10, 11, 12 }

c) { 9 }

d) { 11 }

मान लें कि,

$p = \{8, 9, 10, 11, 12\}$ में से कोई एक संख्या

q = एक भाज्य संख्या नहीं

r = एक वर्ग संख्या

s = एक अभाज्य संख्या

तो $\sim((p \rightarrow \sim q) \wedge (\sim r \vee \sim s))$ का मान क्या होगा?

a) { 9, 11 }

b) { 8, 9, 10, 11, 12 }

c) { 9 }

d) { 11 }

Which search uses the problem specific knowledge beyond the definition of the problem?

a) Informed search

b) Iteratively deepening search

c) both (a) and (b)

d) Breadth-first search

कौन-सा सर्च, समस्या विशिष्ट ज्ञान का उपयोग समस्या की परिभाषा से परे भी करता है?

a) इन्फॉर्मड सर्च
b) इटरेटिवली डीपनिंग सर्च
c) (a) एवं (b) दोनों
d) ब्रेडथ-फर्स्ट सर्च

Which of the following statements are true for benefits of using the backpropagation algorithm to compute gradients?

I. Compared to native gradient computation, it improves the speed of each iteration of gradient descent by eliminating repeated computations of the same subproblem.
II. Its running time is linear in the total number of units (neurons) in the network.
III. Compared to native gradient computation, it reduces the number of iterations required to get close to a local minimum, by protecting against sigmoid unit saturation (vanishing gradients).
IV. Its running time is linear in the total number of edges in the network.

a) Only I
b) II and III
c) I and IV
d) Only III

ग्रेडिएंट के अभिकलन के लिए बैकप्रोपोगेशन कलनविधि का उपयोग करने के लाभ के बारे में निम्नलिखित में से कौन-से कथन सही हैं?

I. नेटिव ग्रेडिएंट अभिकलन की तुलना में, यह समान सब-प्रॉब्लम के पुनरावृत्त अभिकलनों को हटाकर ग्रेडिएंट अवरोहणों की प्रत्येक पुनरावृत्ति की गति में संशोधन करता है।

II. इसका नेटवर्क में इकाइयों की कुल संख्या (न्यूरॉन्स) में रनिंग टाइम रैखिक होता है।

III. नेटिव ग्रेडिएंट अभिकलन की तुलना में, यह सिग्मॉइड यूनिट सेच्युरेशन (vanishing gradients) के समक्ष सुरक्षा प्रदान कर, लोकल न्यूनतम के निकट पहुँचने के लिए आवश्यक पुनरावृत्तियों की संख्या को कम करता है।

IV. नेटवर्क में edges की कुल संख्या में रनिंग टाइम रैखिक होता है।

a) केवल I

b) II और III

c) I और IV

d) केवल III

In terms of the bias-variance decomposition, a 1-nearest neighbour classifier has _______ than a 3-nearest classifier. Choose the correct option.

I Higher variance

II Higher bias

III Lower variance

IV Lower bias

a) I and IV
b) II and III
c) Only I
d) III and IV

बायस-वेरियंस विघटन के संबंध में, 1-nearest neighbour में 3-nearest neighbour की तुलना में ________ होता है। सही विकल्प चुनें।

I उच्चतर वेरियंस

II उच्चतर बायस

III निम्नतर वेरियंस

IV निम्नतर बायस

a) I और IV
b) II और III
c) केवल I
d) III और IV

If the posterior distribution has the same distribution family as the prior, the term most aptly describing this condition is called

a) Subjugate prior.
b) Conjugate posterior.
c) Conjugate Prior.
d) Alternate prior.

यदि एक posterior distribution और prior distribution का समान परिवार हो, तो इस स्थिति की सटीक रूप से व्याख्या करने वाला पारिभाषिक शब्द कौन-सा होगा?

a) Subjugate prior.
b) Conjugate posterior.
c) Conjugate Prior.
d) Alternate prior.

For a feature map ϕ and a kernel function $k(X_i, X_j) = \langle \Phi(X_i), \Phi(X_j) \rangle$, ($\langle . , . \rangle$ is the inner product), which of the statements are true?

I. The kernel trick implies we do not explicitly compute $\Phi(X_i)$ for any sample point X_i.

II. Running times of kernel algorithms do not depend on the dimension D of the feature space $\Phi(.)$

a) I

b) II

c) Both I and II

d) None of these

फीचर मैप ϕ और अष्टि फलन $k(X_i, X_j) = \langle \Phi(X_i), \Phi(X_j) \rangle$ ($\langle . , . \rangle$ आंतरिक उत्पाद है), के लिए निम्नलिखित में से कौन-से कथन सही हैं?

I. kernel trick का तात्पर्य है कि हम किसी sample point X_i के लिए $\Phi(X_i)$ का स्पष्ट रूप से अभिकलन न करें।

II. kernel Algorithms का रनिंग टाइम फीचर स्पेस $\Phi(.)$ के आयाम D पर निर्भर नहीं करता है।

a) I

b) II

c) I और II दोनों

d) उपर्युक्त में से कोई नहीं

In the RSA public key cryptosystem, the private and public keys are (e, n) and (d, n) respectively, where $n = p*q$ and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that $0 < M < n$ and $f(n) = (p - 1)*(q - 1)$. Now consider the following equations.

I. $M' = M^e \bmod n$

   $M = (M')^d \bmod n$

II. $e*d \equiv 1 \bmod n$

III. $e*d \equiv 1 \bmod f(n)$

IV. $M' = M^e \bmod f(n)$

   $M = (M')^d \bmod f(n)$

Which of the clauses are required for RSA to work:

a) I only

b) III only

c) IV only

d) I and III

RSA पब्लिक की क्रिप्टोसिस्टम में, प्राइवेट और पब्लिक कीज़ क्रमशः (e, n) तथा (d, n) हैं, जहाँ $n = p*q$ और p तथा q विशाल अभाज्य संख्याएँ हैं। इसके अलावा, n पब्लिक है और p तथा q प्राइवेट हैं। मान लें कि M ऐसा पूर्णांक है जहाँ $0 < M < n$ और $f(n) = (p - 1)*(q - 1)$ है। अब निम्नलिखित समीकरणों पर विचार करें-

I. $M' = M^e \bmod n$
   $M = (M')^d \bmod n$

II. $e*d \equiv 1 \bmod n$

III. $e*d \equiv 1 \bmod f(n)$

IV. $M' = M^e \bmod f(n)$
   $M = (M')^d \bmod f(n)$

RSA के कार्य करने के लिए उपर्युक्त में से कौन-से खंड आवश्यक हैं?

a) केवल I
b) केवल III
c) केवल IV
d) I और III

The remainder when $3^{100,000}$ is divided by 53 is:

a) 1
b) 2
c) 5
d) 28

जब $3^{100,000}$ को 53 से भाग दिया जाए, तो शेष क्या बचेगा?

a) 1

b) 2

c) 5

d) 28

Which of the following is NOT the aim of the Digital Signature scheme?

I. Authenticity

II. Non-Repudiation

III. Confidentiality

IV. Integrity

a) II and IV

b) II and III

c) II

d) III

निम्नलिखित में से क्या डिजिटल सिग्नेचर स्कीम का उद्देश्य नहीं है?

I. Authenticity

II. Non-Repudiation

III. Confidentiality

IV. Integrity

a) II और IV

b) II और III

c) II

d) III

In security, Sandboxing is a mechanism used for

a) Confidentiality

b) Authentication

c) Isolation

d) Non-repudiation

Security में, Sandboxing युक्ति का प्रयोग किसलिए किया जाता है?

a) Confidentiality
b) Authentication
c) Isolation
d) Non-repudiation

In a public cloud environment, out of the following, the key cyber-security concerns are

A. Virtualization
B. Data Access
C. Denial of service
D. Misconfiguration
E. Data Leakage

a) All of the above
b) All except B
c) All except A
d) All except D

पब्लिक क्लाउड परिवेश में, निम्नलिखित में से साइबर-सुरक्षा की प्रमुख समस्याएँ कौन-सी हैं?

A. Virtualization

B. Data Access

C. Denial of service

D. Misconfiguration

E. Data Leakage

a) उपर्युक्त सभी

b) B के अतिरिक्त सभी

c) A के अतिरिक्त सभी

d) D के अतिरिक्त सभी

IPSec is designed to provide security at which of these layers of the stack?

a) Applications layer

b) Network layer

c) Data link layer

d) Physical layer

IPSec को स्टैक के किस स्तर पर संरक्षा प्रदान करने के लिए डिजाइन किया गया है?

a) Applications layer
b) Network layer
c) Data link layer
d) Physical layer

Elliptic key cryptography is based on which of the following premises

a) Structure of an ellipse over finite fields
b) Algebraic structure of elliptic curves over finite fields
c) Prime number decomposition theorem
d) Both a. and c.

Elliptic key cryptography निम्नलिखित में से किस परिसीमा पर आधारित है?

a) Structure of an ellipse over finite fields
b) Algebraic structure of elliptic curves over finite fields
c) Prime number decomposition theorem
d) Both a. and c.

Choose all the correct statements for the following code snippet

```
void func( char *buf1, char *buf2, unsigned int len1, unsigned int
len2){
   char temp[256];
   if (len1 + len2 > 256 ) { return -1}    // length check
   memcpy(temp, buf1, len1); //cat buffers
   memcpy(temp+len1, buf2, len2);
   do-something(temp); // do stuff
}
```

I. It is safe from buffer overflow due to bound check

II. memcpy() is safeguarded from overflowing the heap

III. It has an integer overflow bug

IV. The length checking is weak in safeguarding against memcpy() to overflow heap

a) I

b) II and III

c) III and IV

d) I, II and III

निम्नलिखित कोड स्निपेट के लिए सभी सही कथनों का चयन कीजिए-

```
void func( char *buf1, char *buf2, unsigned int len1, unsigned int
len2){
    char temp[256];
    if (len1 + len2 > 256 ) { return -1}    // length check
    memcpy(temp, buf1, len1); //cat buffers
    memcpy(temp+len1, buf2, len2);
    do-something(temp); // do stuff
}
```

I. बाउंड जाँच के कारण यह बफर ओवरफ्लो से सुरक्षित होता है।

II. memcpy() हीप को ओवरफ्लो से बचाता है।

III. इसमें integer ओवरफ्लो बग होता है।

IV. memcpy() हीप को ओवरफ्लो से बचाने में लेंथ चेकिंग कमजोर होती है।

a) I

b) II और III

c) III और IV

d) I, II और III

Suppose UID is the unique integer User ID for a user, then choose all the correct statements with respect to the processes,

I. Processes run by the same UID have different permission.

II. Processes run by the same UID have same permission.

III. Processes can access any files that the UID has access to.

IV. Processes started by root can reduce their privileges by changing their UID to a less privileged UID.

a) I, III and IV

b) III and IV

c) II, III and IV

d) II and III

मान लें कि UID एक उपयोगकर्ता के लिए unique integer User ID है, तो Processes के संबंध में सभी सही कथनों का चयन कीजिए-

I. समान UID द्वारा रन की जाने वाली Processes में भिन्न अनुमतियां होती हैं।

II. समान UID द्वारा रन की जाने वाली Processes में समान अनुमतियां होती हैं।

III. Processes UID द्वारा अभिगम की गई किसी भी फाइल को अभिगम कर सकती हैं।

IV. रूट से प्रारंभ की गई Processes अपनी UID को कम विशेषाधिकार वाली UID में परिवर्तित कर अपने विशेषाधिकार कम कर सकती हैं।

a) I, III और IV

b) III और IV

c) II, III और IV

d) II और III

What is the size of the key space in the substitution cipher assuming 26 letters?

a) $|\kappa| = 26$

b) $|\kappa| = 26^{26}$

c) $|\kappa| = 2^{26}$

d) $|\kappa| = 26!$

26 वर्णों को मानते हुए, substitution cipher में 'key space' का आकार क्या होगा?

a) $|\kappa| = 26$

b) $|\kappa| = 26^{26}$

c) $|\kappa| = 2^{26}$

d) $|\kappa| = 26!$

For a one time pad (OTP) cipher (E, D) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, given a message $m \in \mathcal{M}$ and $c \in \mathcal{C}$, can the OTP key be computed from m and c ? $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ are key, message and ciphered text space respectively.

a) Yes, the key $k = m \oplus m$.

b) No, the key cannot be computed.

c) Yes, the key $k = m \oplus c$.

d) Only partial bits of the key can be recovered.

$(\mathcal{K}, \mathcal{M}, \mathcal{C})$ पर वन टाइम पैड (OTP) सिफर (E, D) के लिए, दिया गया संदेश $m \in \mathcal{M}$ और $c \in \mathcal{C}$ है, तो क्या m तथा c से OTP कुंजी का अभिकलन किया जा सकता है? $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ क्रमशः कुंजी, संदेश और सिफर टेक्स्ट स्पेस हैं।

a) हाँ, कुंजी $k = m \oplus m$ है।

b) नहीं, कुंजी का अभिकलन नहीं किया जा सकता है।

c) हाँ, कुंजी $k = m \oplus c$ है।

d) कुंजी के मात्र कुछ अंशों को पुनःप्राप्त किया जा सकता है।

Which of the following statements is or are true if a cipher (E, D) over ($\mathcal{K}$, $\mathcal{M}$, $\mathcal{C}$) has perfect secrecy? ($\mathcal{K}$, $\mathcal{M}$, $\mathcal{C}$) are key, message and ciphered text space respectively.

I. Most powerful adversarial learners can learn about plain text message from the ciphered text.

II. Given a ciphered text, one cannot tell if the message was m_0 or m_1 where $\forall m_0, m_1 \in \mathcal{M}$.

III. A cipher has perfect secrecy if $\forall m_0, m_1 \in \mathcal{M}$ having $|m_0| = |m_1|$ and $\forall c \in \mathcal{C}$, $\Pr[E(k, m_0) = c] = \Pr[E(k, m_1) = c]$ where $k \in \mathcal{K}$.

IV. A cipher has perfect secrecy if $\forall m_0, m_1 \in \mathcal{M}$ having $|m_0| = |m_1|$ and $\forall c \in \mathcal{C}$, $\Pr[E(k, m_0) = c]$!= $\Pr[E(k, m_1) = c]$ where $k \in \mathcal{K}$.

a) I and III
b) III
c) II and III
d) II and IV

यदि एक सिफर(Cipher) (E, D) की ($\mathcal{K}$, $\mathcal{M}$, C) पर पूर्ण गोपनीयता हो तो निम्नलिखित में से कौन-सा/से कथन सही है/हैं? ($\mathcal{K}$, $\mathcal{M}$, C) क्रमशः कुंजी, संदेश और सिफर(ciphered) टेक्स्ट स्पेस हैं।

I. अत्यधिक शक्तिशाली एडवर्सेरियल लर्नर सिफर्ड टेक्स्ट से प्लेन टेक्स्ट मैसेज के बारे में सीख सकते हैं।

II. सिफर्ड टेक्स्ट देने पर , कोई यह नहीं बता सकता कि संदेश m_0 या m_1 था, जहाँ $\forall m_0, m_1 \in \mathcal{M}$ है।

III. एक सिफर में पूर्ण गोपनीयता रहेगी, यदि $|m_0| = |m_1|$ होने पर $\forall m_0, m_1 \in \mathcal{M}$ है और $\forall c \in C$, $\Pr[E(k, m_0) = c] = \Pr[E(k, m_1) = c]$ है, जहाँ $k \in \mathcal{K}$ है।

IV. एक सिफर में पूर्ण गोपनीयता रहेगी, यदि $|m_0| = |m_1|$ होने पर $\forall m_0, m_1 \in \mathcal{M}$ है और $\forall c \in C$, $\Pr[E(k, m_0) = c] != \Pr[E(k, m_1) = c]$ है, जहाँ $k \in \mathcal{K}$ है।

a) I और III

b) III

c) II और III

d) II और IV

Let N be an odd integer, the modular inverse of 2 in $\mathbb{Z}_N$ is

a) $\frac{1}{2}$

b) $\frac{(N+1)}{2}$

c) 1

d) None

मान लें कि N एक विषम पूर्णांक है, तो $\mathbb{Z}_N$ में 2 का modular inverse क्या होगा?

a) $\frac{1}{2}$
b) $\frac{(N+1)}{2}$
c) 1
d) कोई नहीं।

HTTP connections are secured using which one of the following protocol?

a) Transport layer security (TSL)
b) Explicit congestion notification (ECN)
c) Stream control transmission protocol (SCTP)
d) Resource reservation protocol

निम्नलिखित में से किस प्रोटोकॉल का उपयोग कर HTTP connections संरक्षित रहते हैं?

a) ट्रांस्पोर्ट लेयर सिक्योरिटी (TSL)
b) एक्स्प्लिसिट कंजेशन नोटिफिकेशन (ECN)
c) स्ट्रीम कंट्रोल ट्रांस्मिशन प्रोटोकॉल (SCTP)
d) रिसोर्स रिज़र्वेशन प्रोटोकॉल

In public key encryption, if Alice wants to send an encrypted message to Bob then,

a) Alice encrypts message using her private key
b) Alice encrypts message using Bob's private key
c) Alice encrypts message using his public key
d) Alice encrypts message using Bob's public key

Public key encryption में एलिस बॉब को गूढ़लेखित संदेश किस प्रकार भेजेगी?

a) एलिस अपनी प्राइवेट कुंजी से संदेश को encrypt करेगी।
b) एलिस बॉब की प्राइवेट कुंजी से संदेश को encrypt करेगी।
c) एलिस अपनी पब्लिक कुंजी से संदेश को encrypt करेगी।
d) एलिस बॉब की पब्लिक कुंजी से संदेश को encrypt करेगी।

Which of the following statements are correct?

I. It is not known if computing $\phi(N)$ is harder then computing the prime factors of $\mathbb{N}$, where $\mathbb{N}$ is an RSA modulus.

II. Finding prime factors of $\mathbb{N}$ and computing $\phi(N)$ are equivalent, where $\mathbb{N}$ is RSA modulus.

a) I

b) II

c) Both are false

d) Both are true

निम्नलिखित में से कौन-सा/से कथन सही है/हैं?

I. यह ज्ञात नहीं है कि $\phi(N)$ का अभिकलन $\mathbb{N}$ के अभाज्य घटकों के अभिकलन से अधिक कठिन है, जहाँ $\mathbb{N}$ एक RSA मॉड्यूलस है।

II. $\mathbb{N}$ के अभाज्य घटकों को ज्ञात करना और $\phi(N)$ का अभिकलन समान हैं, जहाँ $\mathbb{N}$ एक RSA मॉड्यूलस है।

a) I

b) II

c) दोनों गलत हैं।

d) दोनों सही हैं।

Define $h(x) = g(x^2) \pmod{p}$ where p is a large prime and g is deterministic generator mod p. The function h is collision-resistant.

a) Statement is true
b) Statement is false
c) Information for g is insufficient
d) Statement will be true for a specific value of p

$h(x) = g(x^2) \pmod{p}$ को परिभाषित करें, जहाँ p एक बृहद अभाज्य है और g deterministic generator mod p है। फलन h collision-resistant ।

e) कथन सही है।
f) कथन गलत है।
g) g के लिए सूचना अपर्याप्त है।
h) कथन p के एक निर्धारित मान के लिए सही होगा।

Which of the following statement is/are correct?

I. If h(.) is collision-resistant, then h(h(.)) is also collision-resistant.

II. If it is feasible to find a collision x, x’ under h(h(.)), then x, x’ is also a collision under h.

III. If it is feasible to find a collision x, x’ under h(h(.)), then x, x’ does not necessarily have collision under h.

IV. If h(.) is collision-resistant, then h(h(.)) is not collision-resistant.

a) III

b) I

c) I and II

d) IV

निम्नलिखित में से कौन-सा/से कथन सही है/हैं?

I. यदि h(.) collision-resistant है, तो h(h(.)) भी collision-resistant होता है।

II. यदि h(h(.)) के अंतर्गत collision x, x' को ज्ञात करना संभव है, तो x, x' भी h के अंतर्गत एक collision होता है।

III. यदि h(h(.)) के अंतर्गत collision x, x' को ज्ञात करना संभव है, तो x, x' का h के अंतर्गत एक collision होना आवश्यक नहीं है।

IV. यदि h(.) collision-resistant है, तो h(h(.)) collision-resistant नहीं होता है।

a) III

b) I

c) I और II

d) IV

Suppose a login form from your company uses following implementation for login authentication,

```
$login  = $_POST['login'];
$pass   = $_POST['password'];
$sql  = "SELECT if FROM users WHERE username = '$login' AND
            password = '$pass' "
$rs  =  $db->executeQuery($sql);
if $rs.count > 0 ) {
    // success
}
```

Which of the following statements will be correct with respect to the above pseudocode snippet?

I. The inputs, login = candidate and password = candidate@123' will result SQL syntax error.

II. The inputs, login = candidate'-- and password = candidate@123 will trigger SQL injection attack.

III. The inputs, login = ' or 1 = 1 -- and password = candidate@123 will trigger SQL injection attack.

a) I and II

b) II and III

c) III

d) I, II and III

मानें कि आपकी कंपनी के एक लॉगइन फॉर्म में लॉगइन authentication के लिए निम्नलिखित क्रियाविधि का प्रयोग होता है,

```
$login  = $_POST['login'];
$pass  = $_POST['password'];
$sql  = "SELECT if  FROM users WHERE username = '$login' AND
            password = '$pass' "
$rs  =  $db->executeQuery($sql);
if  $rs.count > 0 ) {
    // success
}
```

उपर्युक्त स्यूडोकोड स्निपेट के संबंध में निम्नलिखित में से कौन-सा कथन सही होगा?

I. इनपुट, लॉगइन= candidate और पासवर्ड= candidate@123' के परिणामस्वरूप SQL syntax error आएगा।

II. इनपुट, लॉगइन= candidate'—और पासवर्ड= candidate@123 से SQL injection attack होगा।

III. इनपुट, लॉगइन= ' या 1 = 1 – और पासवर्ड= candidate@123 से SQL injection attack होगा।

a) I और II

b) II और III

c) III

d) I, II और III

Suppose a system developer of your company website has implemented an executable **viewTop100** using the following implementation,

```
int main( int argc, char **argv) {
    char *cmd = malloc(strlen(argv[1] + 100);
    strcpy(cmd, "head -n 100 ");
    strcat(cmd, argv[1]) ;
    system(cmd);
}
```

Which of the following statements will be correct with respect to the above code snippet?

I. The above function is safe from any kind of injection attack.

II. An adversary can take control of the remote shell using **viewTop100**.

III. An adversary can execute deletion of files for which program has access permission to using **viewTop100**.

a) I

b) II

c) III

d) II and III

मानें कि आपकी कंपनी वेबसाइट के एक सिस्टम डेवलपर ने निम्नलिखित executable द्वारा प्रचालन **viewTop100** क्रियान्वित किया है,

```
int main( int argc, char **argv) {
    char *cmd = malloc(strlen(argv[1] + 100);
    strcpy(cmd, "head -n 100 ");
    strcat(cmd, argv[1]) ;
    system(cmd);
}
```

उपर्युक्त कोड स्निपेट के संबंध में निम्नलिखित में से कौन-सा कथन सही होगा?

I. उपर्युक्त फलन किसी भी प्रकार के injection attack से सुरक्षित है।

II. एक एडवर्सिरी **viewTop100** का उपयोग करते हुए रिमोट शेल का नियंत्रण ले सकती है।

III. एक एडवर्सिरी **viewTop100** का उपयोग करते हुए उन फाइलों को डिलीट कर सकती है जिनके लिए प्रोग्राम को अभिगम अनुमति प्राप्त है।

a) I

b) II

c) III

d) II और III