April 2025

Fundamental IT Engineer Examination (Subject B)

Questions must be answered in accordance with the following:

Question Nos.	Q1 – Q20
Question Selection	All questions are compulsory.
Examination Time	12:30 – 14:10 (100 minutes)

Instructions:

1. Use a pencil. If you need to change an answer, erase your previous answer completely and neatly. Wipe away any eraser debris.

2. Mark your examinee information and test answers in accordance with the instructions below. Your answer will not be graded if you do not mark properly. Do not mark or write on the answer sheet outside of the prescribed places.

    (1) **Examinee Number**

    Write your examinee number in the space provided, and mark the appropriate space below each digit.

    (2) **Date of Birth**

    Write your date of birth (in numbers) exactly as it is printed on your examination admission card, and mark the appropriate space below each digit.

    (3) **Answers**

    Mark your answers as shown in the sample question below.

    [Sample Question]
    Which of the following should be used for marking your answer on the answer sheet?

    Answer group
       a) Ballpoint pen   b) Crayon   c) Fountain pen   d) Pencil

    Since the correct answer is "d) Pencil", mark the answer as below:

    [Sample Answer]

Sample	ⓐ ⓑ ⓒ ● ⓔ ⓕ ⓖ ⓗ ⓘ ⓙ

Do not open the exam booklet until instructed to do so.
Inquiries about the exam questions will not be answered.

Pseudo programming language notations

In algorithm and programming questions that use pseudo programming language, the following notations are used unless otherwise stated:

[Pseudo programming language notations]

Notation	Description
○ *procedure*(*type*: *arg1*, ...)	Declares a *procedure* and its argument(s) *arg1*, ...
○ *ret-type*: *function*(*type*: *arg1*, ...)	Declares a *function*, its argument(s) *arg1*, ... , and type of return value *ret-type*.
type: *var1*, ... *type* []: *array1*, ...	Declares variables *var1*, ... and arrays *array1*, ... by data *type* such as integer, real, and string.
/* *comment* */	Describes a comment between /* and */.
// *comment*	Describes a comment after // till end of line.
variable ← *expression*	Assigns the value of the *expression* to the *variable*.
procedure(*arg1*, ...)	Calls a *procedure* by passing arguments *arg1*, ...
function(*arg1*, ...)	Calls a *function* by passing arguments *arg1*, ... , and receiving the return value.
output *arg1*, ...	Outputs values of *arg1*, ... to a printing device.
return *ret-val*	Finishes a function by passing back a return value *ret-val*.

if (*condition-i*)
　　process-i　　} *1
elseif (*condition-ei*)
　　process-ei　　} *2
else
　　process-e　　} *3
endif
	Indicates the selection process.
	*1 If *condition-i* is true, then execute *process-i*.
	　 Otherwise, proceed to the next elseif or else.
	*2 If *condition-ei* is true, then execute *process-ei*.
	　 Otherwise, proceed to the next elseif or else.
	*3 If all conditions are false, execute *process-e*.
	Note: *2 and *3 can be omitted.
	　　　 *2 may exist twice or more.

for (*sequence*)
　　process
endfor
	Indicates the "for" iteration process.
	In the order specified in the *sequence*, execute the *process* repeatedly.

while (*condition*)
　　process
endwhile
	Indicates the "while" iteration process.
	While the *condition* is true, execute the *process* repeatedly.

do 　　*process* while (*condition*)	Indicates the "do‑while" iteration process. Execute the *process* once, and then while the *condition* is true, execute the *process* repeatedly.

[Operators and their precedence]

Type of operator	Operators	Precedence	Note
Expression	( ), . (1)	High	(1) accessing member or method
Unary operator	+, -, not (2)		(2) logical negation
Binary operator	×, ÷, mod (3)		(3) remainder
	+, -		
	>, <, ≥, ≤, =, ≠		
	and (4)		(4) logical product
	or (5)	Low	(5) logical sum

[Boolean-type constants]

```
true, false
```

[Array reference]

	1-dimensional array	2-dimensional array	Array of arrays
Array declaration	*type* []: *name* ...	*type* [,]: *name* ...	*type* [][]: *name* ...
Example	integer []: a1 1 2 3 4 5 1 3 5 7 9	integer [,]: a2 1 2 3 1: 11 12 13 2: 14 15 16 3: 17 18 19	integer [][]: aa 1 2 3 1: 21 22 2: 23 24 25 3: 26
Data reference	Data 7 is referred to by a1[4]	Data 16 is referred to by a2[2,3]	Data 25 is referred to by aa[2][3]
Notation of array contents	{1, 3, 5, 7, 9}	{{11, 12, 13}, {14, 15, 16}, {17, 18, 19}}	{{21, 22}, {23, 24, 25}, {26}}

Note: The indexes of example arrays start at 1.

[undefined state]

undefined is a state in which no value is set to a variable (or an element of an array).

By setting undefined to a variable, the variable is transformed into undefined state.

Q1. From the answer group below, select the correct combination of answers to be inserted into [A] through [C] in the program.

Centurial years refer to the years that are divisible by 100. The centurial years are not leap years except for years that are exactly divisible by 400. The non-centurial years, that is, years that are not divisible by 100, refer to leap years that are divisible by 4. The function isLeapYear receives an integer number year and returns true if a given year is a leap year or false otherwise.

[Program]
```
O boolean: isLeapYear(integer: year) // returns true if the variable year
                                      // is a leap year; otherwise, returns false
  if (      A      )
    return      B
  elseif (    C    )
    return false
  elseif (year mod 4 = 0)
    return true
  else
    return false
  endif
```

Answer group

	A	B	C
a)	year mod 100 = 0	false	year mod 400 = 0
b)	year mod 100 = 0	true	year mod 400 = 0
c)	year mod 100 ≠ 0	false	year mod 400 ≠ 0
d)	year mod 100 ≠ 0	true	year mod 400 ≠ 0
e)	year mod 400 = 0	false	year mod 100 = 0
f)	year mod 400 = 0	true	year mod 100 = 0
g)	year mod 400 ≠ 0	false	year mod 100 ≠ 0
h)	year mod 400 ≠ 0	true	year mod 100 ≠ 0

Q2. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the program.

The function `isPerfect` receives positive number n, and returns whether n is a perfect number. Here, a number is a "perfect number" if the sum of its positive divisors (excluding the number itself) is equal to the number itself. For instance, 28 is a perfect number because 28 has divisors 1, 2, 4, 7, and 14, and $1 + 2 + 4 + 7 + 14 = 28$.

[Program]
```
○ boolean: isPerfect(integer: n)
    integer: k
    integer: sum ← 0
    integer: half ← integer part of (n ÷ 2)
    for (increase k from 1 to half by 1)
      if (      A      )
            B
      endif
    endfor
    if (sum = n)
      return true
    else
      return false
    endif
```

Answer group

	A	B
a)	n mod k ≠ 0	sum ← sum + 1
b)	n mod k ≠ 0	sum ← sum + k
c)	n mod k = 0	sum ← sum + 1
d)	n mod k = 0	sum ← sum + k

Q3. From the answer group below, select the correct answer to be inserted into [   ] in the description.

The greatest common divisor (GCD) of two numbers is the largest number that divides both of them. The function GCD receives two positive integer numbers and returns their GCD. When the function GCD is called as GCD(98, 56), the output is [   ] in (1)‐(4) below. Here, the output statement "output m, n" outputs the values of variables m and n, and subsequently starts a new line.

(1)	98 56	(2)	42 56	(3)	42 56	(4)	56 42
	42 14		42 14		42 28		42 14
	28 14		28 14		14 28		14 28
	14 7		14 14		14 14		14 14

[Program]
```
○ integer: GCD(integer: x, integer: y)
  integer: m ← x
  integer: n ← y
  while (m ≠ n)
    if (m > n)
      m ← m - n
    else
      n ← n - m
    endif
    output m, n
  endwhile
  return m
```

Answer group
  a) (1)   b) (2)   c) (3)   d) (4)

Q4. From the answer group below, select the correct combination of answers to be inserted into ☐ A ☐ and ☐ B ☐ in the program.

The following function receives an integer number and returns the result of interpreting the decimal representation of the number as a binary number. Note that the number is non-negative, and its decimal representation comprises only the digits 0 and 1. For instance, if it receives 1100, it returns 12.

[Program]
```
○ integer: convert(integer: number)
    integer: place, n, remainder, decimal
    decimal ← 0
    place ← 1
    n ← number
    while (n > 0)
      remainder ← n mod 10
      n ← integer part of (n ÷ 10)
      decimal ← decimal + │    A    │
      place ← │    B    │
    endwhile
    return decimal
```

Answer group

	A	B
a)	2 × place	n × place
b)	2 × place	remainder × place
c)	10 × place	2 × place
d)	10 × place	remainder × place
e)	n × place	2 × place
f)	n × place	remainder × place
g)	remainder × place	2 × place
h)	remainder × place	10 × place

Q5. From the answer group below, select the correct answer to be inserted into [   ] in the program.

The function `calc` receives the positive real numbers `x` and `y`, and returns the result of the calculation of $(\sqrt{x} + \sqrt{y})^2$. For instance, when the function `calc` is called as `calc(4, 9)`, the return value is 25. Here, the function `pow(a, b)` returns `a` raised to the power of `b`.

[Program]
```
○ real: calc(real: x, real: y)
    return [          ]
```

Answer group
a) `pow(pow(x, 0.5) + pow(y, 0.5), 2)`
b) `pow(pow(x, 0.5), 2) + pow(pow(y, 0.5), 2)`
c) `pow(pow(x, 2) + pow(y, 2), 0.5)`
d) `pow(x, 0.5) + pow(y, 0.5)`
e) `pow(x, 0.5) + pow(y, 0.5) ÷ pow(2, 0.5)`
f) `pow(x, 2) + pow(y, 2) ÷ pow(2, 0.5)`

Q6. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the program.

Gray code is a sequence of binary numbers in which two successive values differ by only 1 bit. The function GrayBiCon converts the gray code to a binary code using bitwise operators. The bitwise operators operate on the individual bits of the variables. The function receives the 8-bit type argument x as a gray code, and returns a corresponding binary number of the given argument. The value of each bit after conversion is the exclusive OR of the most significant bit in the gray code up to the corresponding bit position and the converted value of the next higher bit position. For instance, when the function GrayBiCon is called as GrayBiCon(00001100), the return value is a binary number 00001000. The common bitwise operators are listed in the table below:

Table Operators

Operator	Name
&	Bitwise AND
|	Bitwise OR
^	Bitwise XOR (exclusive OR)
<<	Shift left
>>	Shift right

For instance, v << n performs a logical shift of the value of v by n bits to the left.

[Program]
```
○ 8-bit: GrayBiCon(8-bit: x)
    8-bit: y ← x
    8-bit: z ← x
    while (z ≠ 00000000)
        z ← z [   A   ] 1
        y ← [   B   ]
    endwhile
    return y
```

Answer group

	A	B
a)	&	y & z
b)	&	y ^ z
c)	&	y | z
d)	<<	y & z
e)	<<	y ^ z
f)	<<	y | z
g)	>>	y & z
h)	>>	y ^ z
i)	>>	y | z

Q7. From the answer group below, select the correct answer to be inserted into ☐ in the description. Here, the array index starts at 1.

The function binarySearch receives four arguments: the first argument is an array specified with the argument arr (the number of elements ≥ 1), the second argument is the value specified with the argument target, the third argument is the lower bound low of the array, and the fourth argument is the upper bound high of the array. The array arr has no duplicate elements and is sorted in ascending order. If arr has an element with the same value as target, this function returns the index of that element, and -1 otherwise.

When the function binarySearch is called as binarySearch({1, 2, 3, 4, 5, 6}, 5, 1, 6), the number of times the string "call" is output is ☐ .

[Program]
```
○ integer: binarySearch(integer []: arr, integer: target,
                        integer: low, integer: high)
  integer: mid
  if (low > high)
    return -1
  endif
  mid ← integer part of ((low + high) ÷ 2)

  if (arr[mid] > target)
    output "call"
    return binarySearch(arr, target, low, mid - 1)
  elseif (arr[mid] < target)
    output "call"
    return binarySearch(arr, target, mid + 1, high)
  else
    return mid
  endif
```

Answer group
a) 0   b) 1   c) 2   d) 3
e) 4   f) 5   g) 6

- 11 -

Q8. From the answer group below, select the correct combination of answers to be inserted into ☐ A ☐ and ☐ B ☐ in the program. Here, the array index starts at 1.

The function `reverse` takes a string `inputStr` as a parameter and returns the reversed string. Here, the length of the string given to `inputStr` is 100 or less. In the program, areas outside of the arrays must not be referenced and the undefined value must not be appended to a string.

[Program]
```
global: character []: stack ← {100 undefined}
global: integer: sp ← 0

○ string: reverse(string: inputStr)
    integer: n ← length of inputStr
    integer: i
    character: x, v
    string: outputStr ← ""
    for (increase i from 1 to n by 1)
      x ← the i-th character of string inputStr
      push(x)
    endfor
    while (sp ≠      A     )
      v ← pop()
      append v to outputStr
    endwhile
    return outputStr

○ push(character: x)
    sp ← sp + 1
    stack[sp] ← x

○ character: pop()
    character: retvar
        B
    return retvar
```

- 12 -

Answer group

	A	B
a)	-1	`retvar ← stack[sp]` `sp ← sp + 1`
b)	-1	`retvar ← stack[sp]` `sp ← sp - 1`
c)	-1	`sp ← sp + 1` `retvar ← stack[sp]`
d)	-1	`sp ← sp - 1` `retvar ← stack[sp]`
e)	0	`retvar ← stack[sp]` `sp ← sp + 1`
f)	0	`retvar ← stack[sp]` `sp ← sp - 1`
g)	0	`sp ← sp + 1` `retvar ← stack[sp]`
h)	0	`sp ← sp - 1` `retvar ← stack[sp]`

Q9. From the answer group below, select the correct combination of answers to be inserted into [A] through [C] in the program.

Given the root of two binary trees, the aim of the following program is to check whether these two trees are identical. Two binary trees are defined as identical if they satisfy the following formal conditions:

- Structure: Both trees have the same structure, implying that for every corresponding node in the two trees, the arrangement of the left and right children is the same.
- Node Values: Each corresponding node in the two trees must contain the same value. Specifically, if tree T_1 has a node N_1 with value v_1 and tree T_2 has the corresponding node N_2 with value v_2, then $v_1 = v_2$.

The function `isSameTree` takes two instances of class `TreeNode` as the argument representing the root nodes of two binary trees, and returns `true` if the trees are identical, or `false` otherwise. The member variables of `TreeNode` are listed in the table below:

Table Explanation of the member variables of the class `TreeNode`

Member variable	Type	Description
val	integer	The integer value of a current node
left	TreeNode	Left child node
right	TreeNode	Right child node

[Program]
```
O boolean: isSameTree(TreeNode: p, TreeNode: q)
  boolean: checkLeft, checkRight

  if (p = undefined    A    q = undefined)
    return true
  endif
  if (p = undefined    B    q = undefined)
    return false
  endif
  if (p.val ≠ q.val)
    return false
  endif

  checkLeft ← isSameTree(p.left, q.left)
  checkRight ← isSameTree(p.right, q.right)

  return checkLeft    C    checkRight
```

- 14 -

Answer group

	A	B	C
a)	or	and	and
b)	and	or	or
c)	and	or	and
d)	or	and	or

Q10. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the program.

The procedure `deleteLast` removes an element at the end of a doubly linked list. Each element of the doubly linked list is represented by the class `ListElement`. The table shows the description of the class `ListElement`. The `ListElement`-type variable holds a reference to an instance of the class `ListElement`. The global variable `listHead` holds a reference to the head element of the doubly linked list. Remember that each element in the doubly linked list has a reference to its previous element and its next element. Here, if the list is empty, `listHead` is set to `undefined`.

The procedure handles three main cases: if the list is empty, it outputs "empty." If the list contains only one element, it becomes empty after deletion. If multiple elements are present, it only removes the last element.

Table Class ListElement

Member Variable	Type	Description
data	integer	The value of an element.
next	ListElement	Reference to the instance that holds the next element in the list.
prev	ListElement	Reference to the instance that holds the previous element in the list.

[Program]

```
global: ListElement: listHead    /* A reference to the first element of
                                     the list is stored.              */

○ deleteLast()
  ListElement: current
  if (listHead is undefined)
    output "empty"
  else
    current ← listHead
    while (    A     is not undefined)
      current ← current.next
    endwhile
    if (current.prev is not undefined)   // multiple elements are present
         B      ← undefined
    else                                 // only one element is present
      listHead ← undefined               // empty list
    endif
  endif
```

- 16 -

Answer group

	A	B
a)	current.prev	current.prev.next
b)	current.prev	current.next
c)	current	current.prev.next
d)	current	current.next
e)	current.next	current.prev.next
f)	current.next	current.next

Q11. From the answer group below, select the correct combination of answers to be inserted into [A] in the description and [B] in the program. Here, the array index starts at 0.

The procedure `sort` receives an integer array `arr` and prints all the integers in `arr` in ascending order, separated by commas. The number of elements in `arr` is ≥ 1. The values of all array elements are in the range of 0‑10.

If `arr` is {9, 3, 2, 0, 9, 3, 0, 1, 5, 3, 8}, at the end of the procedure, it outputs "0, 0, 1, 2, 3, 3, 3, 5, 8, 9, 9, " and the values of the elements of array `s` will be { [A] }

[Program]
```
○ sort(integer []: arr) // prints all the elements in arr in ascending order
    integer []: s ← {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}
    integer: i, j
    for (increase i from 0 to (the number of elements in arr) - 1 by 1)
      s[arr[i]] ← s[arr[i]] + 1
    endfor
    for (increase i from 0 to 10 by 1)
      if (s[i] > 0)
        for (increase j from 0 to s[i] - 1 by 1)
          output    B    and ", "
        endfor
      endif
    endfor
    return
```

Answer group

	A	B
a)	0, 0, 1, 2, 3, 3, 3, 5, 8, 9, 9	arr[i]
b)	0, 0, 1, 2, 3, 3, 3, 5, 8, 9, 9	i
c)	0, 0, 1, 2, 3, 3, 3, 5, 8, 9, 9	s[i]
d)	0, 1, 2, 3, 5, 8, 9	arr[j]
e)	0, 1, 2, 3, 5, 8, 9	i
f)	0, 1, 2, 3, 5, 8, 9	j
g)	2, 1, 1, 3, 0, 1, 0, 0, 1, 2, 0	i
h)	2, 1, 1, 3, 0, 1, 0, 0, 1, 2, 0	j
i)	2, 1, 1, 3, 0, 1, 0, 0, 1, 2, 0	s[j]

Q12. From the answer group below, select the correct answer to be inserted into [   ] in the program. Here, the array index starts at 1.

The function `hammingDistance` compares the two-character arrays `s1` and `s2` that are given as arguments. `s1` and `s2` have one or more elements. If `s1` and `s2` do not have the same number of elements, the function returns -1. Otherwise, it returns the number of indices where two arrays have different element values at the same index. The figure shows an example of two character arrays. APPLE and APRIE have different element values at two indices.

A	P	P	L	E
A	P	R	I	E

Figure Example of two-character arrays

The table lists examples of `s1` and `s2` given to the function `hammingDistance` and the return values. In the program, areas outside of the arrays must not be referenced.

Table Examples of `s1` and `s2` given to the function `hammingDistance`
and the return values

s1	s2	Return value
{"a", "p", "p", "l", "e"}	{"a", "p", "p", "l", "e"}	0
{"a", "p", "p", "l", "e"}	{"a", "p", "r", "i", "l"}	3
{"a", "p", "p", "l", "e"}	{"m", "e", "l", "o", "n"}	5
{"a", "p", "p", "l", "e"}	{"p", "i", "e"}	-1

[Program]
```
○ integer: hammingDistance(character[]: s1, character[]: s2)
    integer: i, cnt ← 0
    if (the number of elements in s1 ≠ the number of elements in s2)
      return −1
    endif
    for (increase i from 1 to the number of elements in s1 by 1)
      if ([          ])
        cnt ← cnt + 1
      endif
    endfor
    return cnt
```

Answer group
   a) s1[cnt] = s2[cnt]   b) s1[cnt] ≠ s2[cnt]
   c) s1[cnt] = s2[i]   d) s1[cnt] ≠ s2[i]
   e) s1[i] = s2[cnt]   f) s1[i] ≠ s2[cnt]
   g) s1[i] = s2[i]   h) s1[i] ≠ s2[i]

Q13. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the program. Here, the array index starts at 1.

The procedure `maximumSubarray` calculates the maximum sum of the subarray of the array T (the number of elements ≥ 1). A subarray is a contiguous portion of the array, for instance, from `T[1]` to `T[3]`. It can be as short as one element or as long as the entire array. The procedure finds one of the subarrays with the largest sum of values, and outputs the sum, the first, and the last indices of the subarray. For instance, if the content of the array is `{-2, 1, -3, 4, -1, 2, 1, -5, 4}`, the output will be 6, 4, and 7 representing the sum, first index, and last index, respectively. Here, the subarray from `T[4]` to `T[7]` is `{4, -1, 2, 1}`.

[Program]
```
○ maximumSubarray(integer []: T)
    integer: n ← the number of elements in T
    integer: i, j
    integer: first, last   /* the first and last indices of the subarray */
    integer: sum
    integer: max ← T[1] - 1

    for (increase i from 1 to n by 1)
      sum ← 0
      for (increase j from [    A    ] to n by 1)
        sum ← sum + T[j]
        if (sum > max)
          first ← i
          last ← [    B    ]
          max ← sum
        endif
      endfor
    endfor

    output max, first, last
```

Answer group

	A	B
a)	1	j
b)	1	j - 1
c)	i	j
d)	i	j - 1
e)	i + 1	j
f)	i + 1	j - 1

Q14. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the program.

The function `cosine(z)` returns an approximate value of the cosine value of `z` degrees. The function uses Maclaurin series expansion for the cosine shown below and can be used to determine cos(y) for values of y radians.

$$\cos(y) = 1 - \frac{y^2}{2!} + \frac{y^4}{4!} - \frac{y^6}{6!} + \cdots$$

[Program]
```
○ real: cosine(real: z)
    real: y ← z × π ÷ 180 //  convert from degrees to radians
    real: term ← 1
    real: cosy ← term
    integer: n ← 0
    while (absolute value of [    A    ] > 0.000000001)
      n ← n + 1
      term ← term × (-1 × (y[    B    ]) ÷ (2 × n × (2 × n - 1)))
      cosy ← cosy + term
    endwhile
    return cosy
```

Answer group

	A	B
a)	cosy	raised to the power of `(2 × n)`
b)	cosy	raised to the power of 4
c)	cosy	squared
d)	term	raised to the power of `(2 × n)`
e)	term	raised to the power of 4
f)	term	squared

Q15. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the description. Here, the array index starts at 1.

The `calcDistance` returns a value based on array p1, p2 and positive integer n. Assuming that the number of elements in arrays p1 and p2 are the same. The function `abs(x)` returns the absolute value of x, and `pow(a, b)` returns a raised to the power of b.
In the case of p1 is {3, 1, 5, 2} and p2 is {4, 6, 2, 3}, the `calcDistance(p1, p2, 1)` returns [A], whereas `calcDistance(p1, p2, 2)` returns [B]. As the value of n increases, those of `calcDistance(p1, p2, n)` converges to 5.

[Program]
```
○ real: calcDistance(real []: p1, real []: p2, integer: n)
    integer: i
    real: distance ← 0
    real: ex
    for (increase i from 1 to number of elements in p1 by 1)
      distance ← distance + pow(abs(p1[i] - p2[i]), n)
    endfor
    ex ← 1 ÷ n /* Division is performed in data type real */
    distance ← pow(distance, ex)
    return distance
```

Answer group

	A	B
a)	4	4
b)	4	6
c)	4	10
d)	4	18
e)	10	4
f)	10	6
g)	10	10
h)	10	18

Q16. From the answer group below, select the correct combination of answers to be inserted into [A] through [C] in the program.

Craps is a casino dice game in which players bet on the outcomes of the roll of a pair dice. In the rules of the game, a player rolls two dice and finds their sum. There possible outcomes could lead to a win or loss.

1. If the sum is 7 or 11, the player wins.
2. If the sum is 2, 3 or 12, the player loses.
3. Otherwise (the sum is 4, 5, 6, 8, 9 or 10), the player neither wins nor loses. However, the player continues rolling the dice until they either roll the same (initial) sum again (in which case they win the game) or roll a sum of 7 (in which case they lose the game).

The following program approximates the chance of winning a game of Craps using Monte Carlo method and outputs it. The Monte Carlo method is a technique used to estimate the probability of certain outcomes of an experiment by running multiple trial runs, using random numbers. In the program, the playing Craps is illustrated simply by generating random numbers rather than actually rolling a pair of dice. The function `random_int(1, 6)` generates a random integer number between 1 and 6, and returns it.

The program also calculates and outputs the relative error of the measured approximate probability of winning Craps. In general, the relative error *Er* is calculated using the following formula:

$$Er = |\ (Pm - Pt)\ /\ Pt\ |$$

where *Pm* denotes the measured approximate probability and *Pt* denotes the theoretical probability. The theoretical probability of winning Craps is known to be 244/495.

[Program]

```
integer: wins_sum ← 0
integer: lose_sum ← 0
integer: n ← 10000
integer: i, dice1, dice2, sum, newsum
real: result, pt ← (244 ÷ 495)
for (increase i from 1 to n by 1)
  dice1 ← random_int(1, 6)
  dice2 ← random_int(1, 6)
  sum ← dice1 + dice2
  if (sum = 7 or sum = 11)
```

```
        wins_sum ← wins_sum + 1
    elseif (sum = 2 or sum = 3 or sum = 12)
        lose_sum ← lose_sum + 1
    else
        do
            dice1 ← random_int(1, 6)
            dice2 ← random_int(1, 6)
            newsum ← dice1 + dice2
            if (newsum = sum)
                wins_sum ← wins_sum + 1
            elseif (newsum = 7)
                lose_sum ← lose_sum + 1
            endif
        while (     A     )
    endif
  endfor
  result ←       B
  output result, absolute value of (      C      )
```

Answer group

	A	B	C
a)	newsum ≠ sum and newsum ≠ 7	wins_sum ÷ lose_sum	(result − pt) ÷ pt
b)	newsum ≠ sum and newsum ≠ 7	wins_sum ÷ lose_sum	result ÷ pt
c)	newsum ≠ sum and newsum ≠ 7	wins_sum ÷ n	(result − pt) ÷ pt
d)	newsum ≠ sum and newsum ≠ 7	wins_sum ÷ n	result ÷ pt
e)	newsum ≠ sum or newsum ≠ 7	wins_sum ÷ lose_sum	(result − pt) ÷ pt
f)	newsum ≠ sum or newsum ≠ 7	wins_sum ÷ lose_sum	result ÷ pt
g)	newsum ≠ sum or newsum ≠ 7	wins_sum ÷ n	(result − pt) ÷ pt
h)	newsum ≠ sum or newsum ≠ 7	wins_sum ÷ n	result ÷ pt

Q17. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the description.

Recently, an e-commerce company X was cyber-attacked by an attacker. Mr. Y, the security team leader at the company, is investigating the incident and considering future countermeasures. The following is the summary of the incident:

The first half of the attack: An attacker visited company X's website to collect valuable information and knew the name of a senior worker of the IT department who was only responsible for system administration. One day, a receptionist for Company X received a phone call from a man with a fantastic voice. He asked some personal questions about the senior IT guy, Mr. Z. The caller skillfully manipulated the receptionist into giving him personal information about the IT guy. The caller was the attacker who got helpful information for further attacks on the company's server.

The second half of the attack: After that, the attacker dug into social sites and other resources to get additional information about Mr. Z and the servers of Company X, and then he created a password file based on Mr. Z's information and a file with the company server's IP address list. Then, the attacker remotely attacked a server of the company using the password list and an IP address of the server.

Mr. Y implemented two measures as future countermeasures for a similar attack. The measure for the first half of the attack is [A]. The other for the second half is [B].

Answer group

	A	B
a)	abolition of company-wide telephone use	encrypting access to websites using HTTPS
b)	abolition of company-wide telephone use	implement account lock for consecutive incorrect password attempts on the server
c)	abolition of company-wide telephone use	prohibit employees from using social networking services
d)	education for the employees against social engineering	encrypting access to websites using HTTPS
e)	education for the employees against social engineering	implement account lock for consecutive incorrect password attempts on the server
f)	education for the employees against social engineering	prohibit employees from using social networking services
g)	restricting access to the websites using IP address-based block lists	encrypting access to websites using HTTPS
h)	restricting access to the websites using IP address-based block lists	implement account lock for consecutive incorrect password attempts on the server
i)	restricting access to the websites using IP address-based block lists	prohibit employees from using social networking services

Q18. From the answer group below, select the most appropriate combination of answers to be inserted into [A   ] and [B   ] in the description.

Company Z wants to provide secure file transfer service especially for very large files for their customers. Mr. K, the system architect of the company, designed the sequence of uploading, storing, and downloading customer files on the web service. In this system, customers register their email addresses and their public keys during sign up. The associated private keys reside on the customers' computers and the email address is used as the user id. The requirements for the file transfer service are as follows:

-   Customers transfer files between each other by uploading files to or downloading them from the web service provided by Company Z.
-   When uploading a file, the sender supplies the recipient's email address and the password that will be used with the particular file (Upload function).
-   The file uploaded by the sender is encrypted with the supplied password and then stored in the database of the web service. (StoreFile function).
-   The web service assigns a file id to the uploaded file and notifies the sender of it upon uploading.
-   The encrypted file can only be decrypted by the sender and the recipient of the file using the password supplied by the sender.
-   The password is encrypted and sent to the recipient as an email message along with the file id (Message function).
-   When downloading the file, the recipient supplies the file id and the password. The web service then decrypts the stored file and provides it for the recipient.
-   Even if the database is leaked, it will be difficult to decrypt the uploaded files stored in the database.

Figure 1 shows the sequence of uploading file by customer P for customer Q.
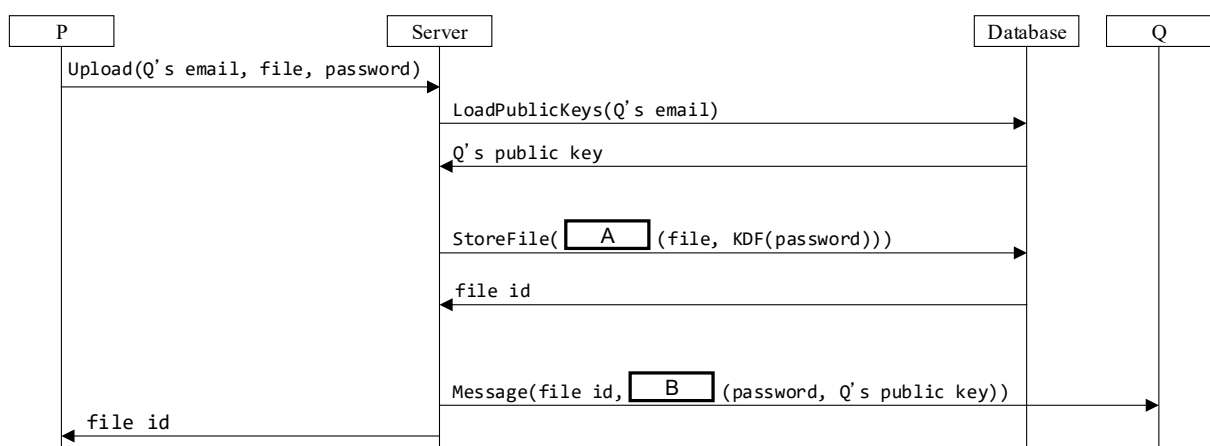

Figure 1 Sequence on file uploading

In this system, Mr.K uses KDF (Key Derivation Function) to improve the strength of the supplied password and uses [A] and [B] algorithms to accomplish above requirements. Note that the format of encryption algorithms used here is algorithm(data, key).

Answer group

	A	B
a)	asymmetric key encryption	cryptographically secure hash
b)	asymmetric key encryption	symmetric key encryption
c)	cryptographically secure hash	asymmetric key encryption
d)	cryptographically secure hash	symmetric key encryption
e)	symmetric key encryption	asymmetric key encryption
f)	symmetric key encryption	cryptographically secure hash

Q19. From the answer group below, select the correct combination of answers to be inserted into [A   ] and [B   ] in the description.

Company V, a small-sized company specializing in manufacturing and selling home appliances, has recently expanded its team of website administrators to five. In addition, they have renovated their website to allow customers to download user manuals for their products. One day, an external security researcher highlighted that files containing a watermark with "For Internal Use" were publicly accessible in the public directory of the company's website and available for download. Company V has a system that ensures all documents stored in the internal folder have this watermark by default, and a rule exists stating that the watermark must be removed when files are published or shared external. The website administrator immediately confirmed the issue and removed the document from the public directory. Then, the website administrator reported this issue to Company V's security team. The investigation of the security team revealed that the issue was caused by a website administrator accidentally uploading internal documents instead of the intended public catalog files. Those publicly accessible files were a draft version of the catalogs, and they did not contain credential information such as API keys for website management. When uploading files to the website's public directory, another website administrator, other than the uploader, was supposed to verify the correctness of the files. However, they failed to notice the mistake. To prevent similar issues in the future, the security team suggested implementing [A   ] to the website administrators. Additionally, to quickly detect issues, the security team suggested implementing [B   ].

Answer group

	A	B
a)	a system to check all file upload destinations and ensure they are not public directories before allowing the uploads	a policy where all configuration changes on Company V's website are checked by at least two website administrators
b)	a system to check all file upload destinations and ensure they are not public directories before allowing the uploads	monitoring tools that alert administrators to any unauthorized access to the public directory
c)	a system to check all file upload destinations and ensure they are not public directories before allowing the uploads	periodic checks of the files in the public directory to identify any files that may be mistakenly exposed
d)	an automated credential scanner to scan files for credentials and API keys before uploading them to the website public directory	a policy where all configuration changes on Company V's website are checked by at least two website administrators
e)	an automated credential scanner to scan files for credentials and API keys before uploading them to the website public directory	monitoring tools that alert administrators to any unauthorized access to the public directory
f)	an automated credential scanner to scan files for credentials and API keys before uploading them to the website public directory	periodic checks of the files in the public directory to identify any files that may be mistakenly exposed
g)	an automated tool to prevent the upload of files containing a watermark with "For Internal Use" to the website's public directory	a policy where all configuration changes on Company V's website are checked by at least two website administrators
h)	an automated tool to prevent the upload of files containing a watermark with "For Internal Use" to the website's public directory	monitoring tools that alert administrators to any unauthorized access to the public directory
i)	an automated tool to prevent the upload of files containing a watermark with "For Internal Use" to the website's public directory	periodic checks of the files in the public directory to identify any files that may be mistakenly exposed

Q20. From the answer group below, select the correct combination of answers to be inserted into [A] and [B] in the description.

Company A recently experienced a security incident where confidential data were exfiltrated by a compromised employee account. Ms. T, a security analyst at Company A, investigated the compromised employee account and found that the password used by the employee's account involved in this breach was a complex password that met the company's password policy. However, the same password was used across several web services. Additionally, Ms. T investigated the login logs of Company A's system and discovered 1,000 failed login attempts recorded within 3 hours before a successful login was recorded. These failed login logs included attempts to log in with different account IDs and password sets. These login attempts occurred from a county where Company A does not have an office. Company A has no employees who travel abroad.

To prevent future account compromise by the same attack pattern, Ms. T suggested that the system administrators of Company V implement [A]. Additionally, to quickly detect any account compromise, she suggested implementing a monitoring system to alert administrators of [B].

Answer group

	A	B
a)	a more complex password policy	login attempts from locations where the account is not usually logged in.
b)	a more complex password policy	overwhelmed network traffic in Company A's system
c)	a more complex password policy	unpatched servers in Company A's system
d)	encryption of all files stored on employees' computers	login attempts from locations where the account is not usually logged in.
e)	encryption of all files stored on employees' computers	overwhelmed network traffic in Company A's system
f)	encryption of all files stored on employees' computers	unpatched servers in Company A's system
g)	Multi-Factor Authentication to all employee accounts	login attempts from locations where the account is not usually logged in.
h)	Multi-Factor Authentication to all employee accounts	overwhelmed network traffic in Company A's system
i)	Multi-Factor Authentication to all employee accounts	unpatched servers in Company A's system