2010年7月7日

情報セキュリティ大学院大学
情報セキュリティ研究科（博士前期課程）情報セキュリティ専攻
2011年度特待生選抜試験問題

1次選考（筆記試験）

10:00～11:30

(1)
- Ⅰ　情報数学A
- Ⅱ　情報数学B
- Ⅲ　通信ネットワーク
- Ⅳ　情報システム
- Ⅴ　ソフトウェア

(2)
- 小論文

【注意事項】

1. 指示があるまで、この問題冊子を開いてはならない。
2. この問題冊子の本文は全部で12ページある。落丁、乱丁があれば申し出ること。
3. (1)、(2)のいずれかを選択し、答案を作成せよ。ただし、技術系の研究テーマを希望する受験者は(1)を選択すること。
4. (1)を選択した受験者は、上記Ⅰ～Ⅴの5項目から2項目を選択し、解答すること。5項目中どの2項目を選択してもよい。
   (2)を選択した受験者は、与えられた課題について、2000字以上3000字以内の小論文を作成すること。
5. 解答用紙は計3枚（(1)用解答用紙2枚、(2)用解答用紙1枚）配布される。
   (1)を選択した受験者は、「筆記試験(1)用解答用紙」を、選択した項目ごとに1枚ずつ使用すること。必要があれば裏面を使用してよい。筆記試験(2)用解答用紙には何も記入しないこと。
   (2)を選択した受験者は、「筆記試験(2)用解答用紙」1枚のみを使用すること。筆記試験(1)用解答用紙には何も記入しないこと。
   同一受験者が(1)、(2)両方に解答した場合、いずれの解答用紙も無効となるので注意すること。
6. 解答用紙の指定欄に、選択した項目名（「ローマ数字＋科目名」※(1)を選択した受験者）、受験番号（全受験者）を必ず記入すること。解答用紙の回収前に、これらを記入したかを必ず確認すること。
7. 問題冊子、解答用紙、計算・下書き用紙は持ち帰ってはならない。

I 情報数学 A

整係数多項式 $f(x)$ を

$$f(x) = x^3 + x^2 + x + 1$$

と定める。以下の問いに答えよ。

(問 1)

$$g(x) \equiv f(x)^3 \bmod 3$$

を満足する多項式 $g(x)$ を求めよ。なお、$g(x)$ は係数を $\{0, 1, 2\}$ からとるものとする。

(問 2)

$$g(x) \equiv f(x)^9 \bmod 3$$

を満足する多項式 $g(x)$ を求めよ。なお、$g(x)$ は係数を $\{0, 1, 2\}$ からとるものとする。

(問 3)

$$g(x) \equiv f(x)^{36} \bmod 3$$

を満足する多項式 $g(x)$ を求めよ。なお、$g(x)$ は係数を $\{0, 1, 2\}$ からとるものとする。

(問 4)

$$g(x) \equiv f(x)^{36} \bmod 2$$

を満足する多項式 $g(x)$ を求めよ。なお、$g(x)$ は係数を $\{0, 1\}$ からとるものとする。

(問 5)

$$g(x) \equiv f(x)^{36} \bmod 6$$

を満足する多項式 $g(x)$ を求めよ。なお、$g(x)$ は係数を $\{0, \ldots, 5\}$ からとるものとする。

Ⅱ 情報数学Ｂ

感染症Ｘが流行しており、10万人に１人の割合で感染者が存在するとする。感染症Ｘに対する検査法Ｂが開発され、それによると、

- 感染者に対しては、100％確実に『陽性』と判定できるが、
- 0.1％の割合で、実際には感染していない者を『陽性』と誤判定してしまう

とする。

今、あなたが検査法Ｂを受診したところ『陽性』と判定された。あなたが実際に感染症Ｘに感染している確率を求めよ。

Ⅲ通信ネットワーク

インターネットプロトコルはIPv4からIPv6へ移行しつつある。下記の問１から問３はIPv4からIPv6への移行に関する問題である.問１から問３を読み、それぞれ解答しなさい。なお、図を作成して解答に用いてもよい。

(問１)　IPv4からIPv6に移行する主な理由を述べよ。

(問２)　移行過程ではラージスケールNAT (Network Address Translation) というアドレス変換方式の適用が計画されている。ラージスケールNATと従来のNATとの違いを述べよ。

(問３)　IPv4インターネットのままでIPv6パケットをトンネリングする代表的な技術を一つあげ、その概要を示せ。

Ⅳ情報システム

次の４項目について、各々5行程度で答えよ

(問１)　仮想アドレスとは何か、また、その実現方式について述べよ。

(問２)　商品やサービスをインターネットで販売するようなネットショップは、Web システムとして作られることが多い。その大まかな構成と動作について述べよ。

(問３)　オペレーティングシステムの重要な機能の一つは資源をそれぞれの処理に配分することで、そのためにハードウエアには Test and Set 命令が用意されている。この命令の動作について述べ、次いで資源配分との関係について考察せよ。

(問４)　銀行口座からお金を引き出す処理や、列車の座席を予約する処理などは、トランザクション処理と呼ばれる。その処理に求められる要件について述べよ。

Vソフトウェア

クィックソートは、以下のアルゴルズムを取る。

(1)ピボットを選ぶ。(ここでは、左端のデータとする)

(2)ピボットより小さいデータを左側に、ピボットより大きいデータを右側へ移動する。

(3)二分割されたそれぞれを、ソートする。

詳細アルゴリズムを擬似言語で記述する。

```
procedure QUICKSORT(m,n)
// レコード Ri のキーは Ki である。レコード Rm,... Rn を、K をキーに昇順にソートする。
ピボットは Km である。ここでは、Km <=Kn+1  と仮定する//
   if m < n
      then{  i ← m ;  j ← n + 1 ;  K ← Km
         loop
            repeat   i ← i + 1     until  Ki  >=  K;
            repeat   [(a)]         until  Kj  <=  K;
            if  i  <  j
               then    INTERCHANGE( i , j)
               else    break
         forever
         INTERCHANGE( [(b)] ,  j)
         QUICKSORT( m ,  j - 1)
         QUICKSORT( [(c)] , [(d)] ) }
end QUICKSORT
```

INTERCHANGE(*i, j*)は、　R_i と R_j の値を交換する関数である。

loop ... forever　は、繰り返し実行される。

break は、最も内側の **loop** から抜け出る働きがある。

(問 1)上記(a), (b), (c), (d)に適切な字句をいれよ。

(問 2)　上記アルゴリズムで、「4　8　7　6　1　3　2　5　9」とキーが並んでいるデータをソートした場合のデータの並び順の変化を逐次示せ。

(問 3)　上記アルゴリズムのコメント内の　「$K_m <= K_{n+1}$」という仮定は　なぜ必要か？

(問 4)　クィックソートは不安定なソートである。(不安定なソートとは、キーに同じ値があった場合、ソートの前後でその並び順が保たれないソートである) キーの並び順が保たれないデータの例をあげよ。(データ数は 6 個とする)

小論文

これまでに学んだこと・経験したことを踏まえて、「安全・安心」をテーマとした小論文を２０００字以上３０００字以内で書け。