2011年7月6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
2012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

$p = 37$ とする。また、

$$F(x) = x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

を、合同式

$$F(x) \equiv \prod_{1 \le i \le 6} (x + i) \bmod p$$

を満足する整数係数多項式とする。
以下の問いに答えよ。

(問 1) $F(x)$ の k 次係数 f_k を $k = 0, \ldots, 5$ に対して求めよ。なお、各係数 f_k は $0 \le f_k < p$ を満足するものとする。

(問 2) 合同式

$$a_j \equiv F(6j) \bmod p$$

を満足し、かつ $0 \le a_j < p$ を満足する整数 a_j を $j = 1, \ldots, 5$ に対して求めよ。

(問 3) 合同式

$$b \equiv (p-1)! \bmod p$$

を満足し、かつ $0 \le b < p$ を満足する整数 b を求めよ。

(問 4) c は合同式

$$c \equiv \prod_{2 \le i \le 18} (p - i) \bmod p$$

を満足する整数であるとする。合同式

$$cd \equiv 1 \bmod p$$

を満足し、かつ $0 \le d < p$ を満足する整数 d を求めよ。

II 情報数学B

n ビット文字列全体からなる集合を $\{0,1\}^n$ とかく。$\{0,1\}^n$ から $\{0,1\}^n$ への写像 f 全体からなる集合を F_n とおく:

$$F_n = \{f \mid f : \{0,1\}^n \to \{0,1\}^n : \text{写像}\}.$$

また、n 個の 0 を並べた文字列を 0^n $(\in \{0,1\}^n)$ とかく。

(問 1) 集合 F_n から写像 f をランダムに選ぶとき、$f(0^n) = 0^n$ である確率を求めよ。

(問 2) 集合 F_n から写像 f をランダムに選ぶとき、ある $v \in \{0,1\}^n$ があって $f(v) = 0^n$ である確率を求め、これは n が十分大きいとき 0.6 以上であることを示せ。

(問 3) 集合 F_n から写像 f をランダムに選ぶとき、ある異なる $v, w \in \{0,1\}^n$ があって $f(v) = f(w)$ である確率は、$1 - 2^{-2^{n-1}}$ 以上であることを示せ。

Ⅲ通信ネットワーク

下記の(問 1)と(問 2)は IP ネットワークの分割と集約に関する問題である。それぞれ解答しなさい。

(問 1)

LAN のネットワークアドレスは 192.168.1.0/24 などと表記される。ここで、24 はサブネットマスク長と呼ばれ、IP アドレス 192.168.1.0 を 32 ビットのビット列で表した場合のネットワークアドレス部の長さ（範囲）を表す。LAN に収容可能なホスト数は 32 からサブネットマスク長を引いた値から決定される。

(1)192.168.1.0/24 の LAN には 254 台のホストが収容できる。192.168.1.128/25 の LAN はいくつのホストを収容できるか答えなさい。

(2)192.168.1.0/24 の LAN が 180 台のホストを収容していたが、100 台、50 台、30 台ずつ別々に収容するため、LAN を 3 つに分割することになった。VLSM（Variable Length Subnet Mask）が利用できるものとして、3 つの LAN に付与するネットワークアドレスを全て答えなさい。ただし、ゼロサブネットの使用が許可されているものとし、192.168.1.0 は分割後のいずれかの LAN のネットワークアドレスに用いることとする。

(問 2)

ネットワークアドレスが 200.100.38.0/24、200.100.40.0/24、200.100.42.0/24、200.100.44.0/24、と示される 4 つの IP ネットワークがある。経路制御に CIDR（Classless Inter-Domain Routing）が適用されている場合、4 つのネットワークはルーティング上どのようなアドレスのネットワークに集約されると考えられるか答えなさい。

Ⅳ情報システム

次の４つの問いについて、各々５行程度で答えよ

(問 1)　二つのデータ構造、キューとスタックそれぞれについて、それを用いる目的と、具体的な応用例について述べよ

(問 2)　名前の付いた多くのファイルがあり、それぞれの配置アドレスが分かっており、それらの対応表があったとする。あるファイル名が与えられたとき、その表を用いて迅速にその配置アドレスを探す手法としてハッシュ法がある。その構造を示し、高速化が可能な理由について述べよ

(問 3)　プロセッサがプログラムを処理する場合、プロセッサハードウエアの中では、その高速実行のために分岐予測を行っている。分岐予測とは何か、また、何故それが高速化に繋がるかの理由を説明せよ

(問 4)　情報システムは様々な原因で故障したり止まったりすることがある。それらに対する原因と対策の概要を述べよ

Vソフトウェア

実数計算を2進浮動小数点で行うコンピュータで、2次方程式の係数を読み込んでその根を求めるプログラムを作成したところ、誤差が出るケースがあることがわかった。この誤差には二つの原因が存在する。

(問1) 誤差の第一の原因として係数の読み込み部に問題があることがわかった。この処理を簡単にしたものを図1に示す。係数を表す入力文字は文字配列 Ki (i = 1,2,...,n)に与えられ、小数点を必ず一つ含み、データの終わりには空白があるとする。また DEC( )は、数字1文字を数値に変換する関数である。　図1のなかでの誤差の発生個所は（＊）の処理である。この誤差はどんな誤差なのかについて説明せよ。

(問2) この誤差を取り除くために図2のように修正した。　図2中の　(a), (b)に適当な代入文をいれよ。

(問 3) 誤差の第二の原因は数値計算のプロセスで発生することがわかった。このプログラムでは2次方程式　$ax^2+bx+c=0 (a \neq 0)$の根を

$$x1 = \frac{-b+\sqrt{b^2-4ac}}{2a} \qquad x2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$$

で計算している。どんな場合、どのような誤差が発生するか述べよ。また、それに対応するためにはどのような手順のプログラムに変更すれば良いか述べよ。

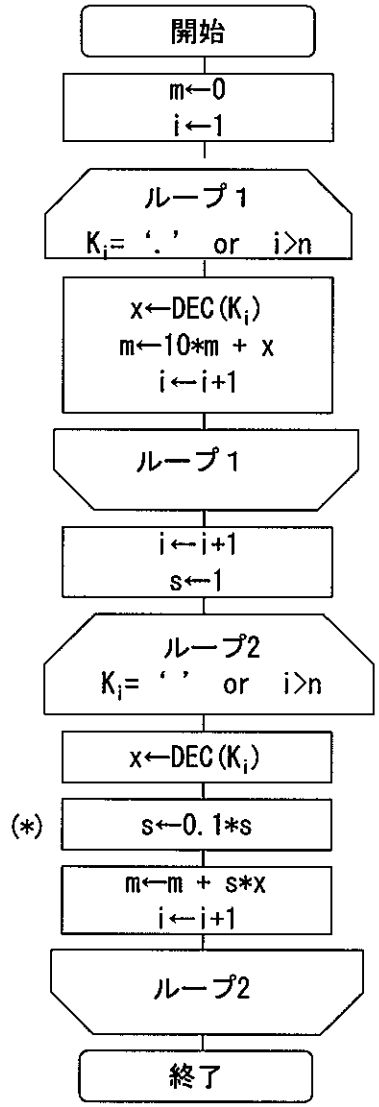

図1　係数読み込み部のフローチャート

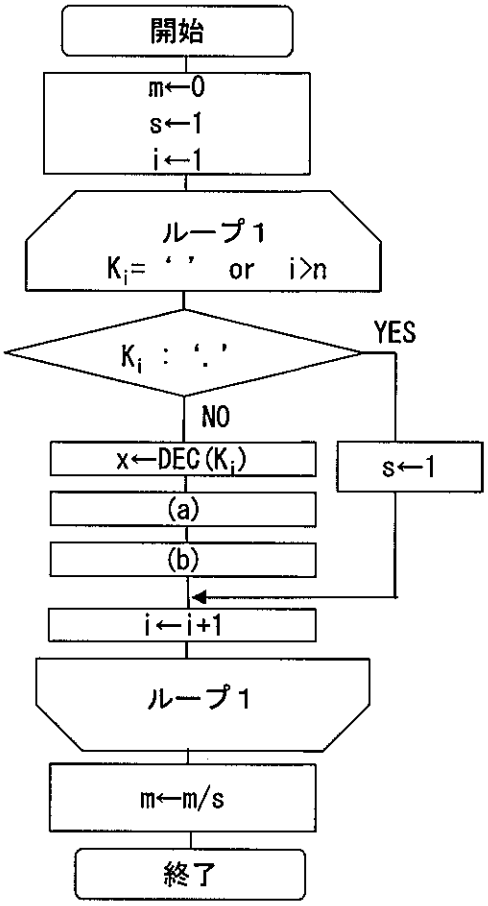

図2　修正後のフローチャート

小論文

これまでに学んだこと・経験したことを踏まえて、情報公開と風評をテーマとした小論文を２０００字以上３０００字以内で書け。