2014年7月9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
2015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

(問1) m と n を整数とする。$\sin^m x$ および $\sin^m x \cos^n x$ を微分せよ。

(問2) m と n を整数とする。

$$I_{m,n} = \int \sin^m x \cos^n x \, dx$$

とおく。$m+n \neq 0$ のとき、

$$I_{m,n} = \frac{1}{m+n} \sin^{m+1} x \cos^{n-1} x + \frac{n-1}{m+n} I_{m,n-2}$$

が成り立つことを証明せよ。

(問3) $\sin^4 x \cos^2 x$ を積分せよ。

II 情報数学B

以下の問に答えよ。

(問 1)　$\zeta = (-1+\sqrt{-3})/2$ とする。変数 X,Y に関する多項式として

$$X^3 - Y^3 = (X-Y)(X-\zeta Y)(X-\zeta^2 Y)$$

であることを示せ。

(問 2)　すべての整数の集合を $\mathbb{Z}$ とかく。集合 $A = \{x^2+xy+y^2 \mid x,y \in \mathbb{Z}\}$ は乗法について閉じていること、すなわち、$a \in A$ かつ $b \in A$ ならば $ab \in A$ であることを示せ。

III 通信ネットワーク

TCP ではコネクション毎に送受信ホスト間の往復遅延時間 Round Trip Time(以下 RTT と示す)を測定する。この RTT に関連する以下の問 1 から問 5 に答えよ。

(問 1)通信路の帯域が 1Gb/s、RTT が 20ms の時、送受信ホスト間のスループットが最大になるウィンドウサイズはいくらか答えよ。

(問 2) ネットワークが輻輳して通信不能となることを避けるため、送信ホストは、RTT の増減に応じて送信速度を調整することがある。どのように調整するのか説明せよ。

(問 3) 送信ホストは、RTT の測定値を用いて、パケット再送のためのタイムアウト時間をコネクション毎に設定する。どのように設定するのか説明せよ。

(問 4)問 3 のタイムアウト値をコネクションによらず一定値に設定するとパケット転送上不都合が生じる。どのような不都合か説明せよ。

(問 5) 送受信ホスト間の RTT はネットワーク管理コマンド ping を用いても測定できる。一般に同コマンドによる RTT は TCP で測定した RTT よりも小さい。この理由を述べよ。

Ⅳ情報システム

次の問いのすべてについて、それぞれ6行程度で答えよ

(問 1) キューとスタックの動作と使い方について説明せよ。

(問 2) 複数のコンピュータを用いて情報システムの信頼性を高める方式例を示し、その利点と課題について述べよ。

(問 3) コンピュータ処理を高速化するための技術の一つであるキャッシュメモリの仕組みを説明せよ。また、どのような場合に高速化でき、どのような場合に高速化が難しいかを示せ。

(問 4) コンピュータにおける仮想化について、一つ以上の例を使って説明せよ。

Vソフトウェア

Base64 は、バイナリデータを印字可能な 64 種類の英数字に変換するエンコード方式で、電子メールなどで用いられる。
Base64 のエンコードのアルゴリズムは以下の通りである。Base64 では 3 バイトずつ変換する。
(1) 元データを 6 ビットごとに分割する。6 ビットに満たない分は 0 を追加して 6 ビットにする。
(2) 3 バイトのデータの先頭から 6 ビットずつの値を変換表により変換し、4 文字にする。4 文字に満たない分は'='記号を追加して 4 文字にする。 (変換表は次ページ表 1 を参照のこと)
(3)上記文字を 76 文字ずつ出力し、改行文字を入れる。 最後の行は 76 文字未満でも改行する。

デコードはこの逆を行う。

(問 1) 次の問に答えよ。但しここでは 改行は考慮しない。
(a) 4 バイトのデータ(16 進数) "0x29191E0C" を Base64 でエンコードした結果の文字列を示せ。
(b) エンコードした結果、"lhg=" となった。元のデータは何か。16 進数で示せ。

(問 2) 500 バイトのデータをエンコードした場合、何バイトになるか。 改行は 1 バイトとする。

(問 3) 配列 A[0], A[1], A[2]に変換前の 3 バイトのデータがある。これをエンコードするため大きさ 4 の配列 B [0], B[1], B[2], B[3]に切り出す処理について空欄を埋めよ。
なお x leftshift y は、x を y ビット左に論理シフトする演算、x rightshift y は、x を y ビット右に論理シフトする演算である。

B[0] ← A[0] rightshift 2
B[1] ← [(a)]
B[2] ← ((A[1] and 15) leftshift 2) or (A[2] rightshift 6)
B[3] ← [(b)]

(問 4) デコード処理の概要は以下のようになる。空欄を埋めよ。

```
i ← 0
while(ファイルの終わりでない){
    ch←次の 1 文字を読む。
    if (ch が改行でない){
        c[i] ← ch
        if(ch が'='でない) c[i]を変換表に基づきデコードした結果を b[i]に入れる
        i← i+1
        if ( [ (c) ] ) {
            n ←3
            if (c[3]が '=')      [ (d) ]
            if (c[2]が '=')      [ (e) ]
            b[0]..b[n]をそれぞれ 6 ビット取り出し、詰めて書き出す
            [ (f) ]
        }
    }
}
if( [ (g) ] ) 入力データが正しい形式でないというエラーメッセージ
```

表 1　Base64 の変換表　(元データは 10 進表現である)

元データ	変換後の文字	元データ	変換後の文字	元データ	変換後の文字	元データ	変換後の文字
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	M	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

小論文

総務省情報通信政策研究所が平成25年6月に公表した「青少年のインターネット利用と依存傾向に関する調査　調査結果報告書」によれば、スマートフォンを自分でも利用していると回答した青少年の割合が、小学4～6年生で16.0%、中学生で21.3%、高校生で51.1%となっており、低年齢層へのスマートフォンの普及が顕著となっている。

このような傾向を背景として、近時、地方公共団体の条例で小中学生の携帯電話の所持を規制したり、小中学校が夜間のスマートフォンの利用を生徒に禁止したりする事例がみられるが、青少年のスマートフォンの利用については、社会や学校、家庭はどのように対応すべきか。

自分自身の携帯電話やスマートフォンの利用経験にも即しながら、2,000字以上3,000字以内で小論文を作成せよ。