令和4年度
京都工芸繊維大学 大学院工芸科学研究科
博士前期課程（修士課程）推薦入学特別入試
情報工学専攻　小論文　課題

［注意］

1. この課題冊子は合図があるまで中を開かないでください。
2. 課題は３題あり、課題１は必須です。課題２と３はどちらか一方を選択してください。課題１と、課題２と３のどちらか一方の、計２題について小論文を作成してください。
3. 配布物は、この課題冊子１部、解答用紙２枚、および下書き用紙２枚です。解答する課題毎に別の解答用紙を用いてください。汚損等でやむを得ない場合を除き、解答用紙および下書き用紙の追加配布はしません。
4. 解答用紙裏面を使用する場合は、おもて面右下に「裏面使用」と断り書きして使用してください。
5. 机の上には受験票以外に、次のものを置いてもよろしい：黒鉛筆またはシャープペンシル（黒）、プラスチック製の消しゴム、鉛筆削り（電動式・大型のもの・ナイフ類は不可）、計時機能のみの時計（秒針音のするもの・大型のものは不可）、眼鏡・ハンカチ・目薬・ティッシュペーパー（袋又は箱から中身だけ取り出したもの）。これら以外のものについては監督者の了解を得た場合に限り、置くことができます。
6. 試験時間は、９：３０～１１：３０の１２０分間です。中途退室は認めません。ただし、トイレなどやむを得ない場合は、一時退室を認めますので、挙手して知らせて下さい。試験終了後も退室の許可があるまで退室はできません。
7. 解答用紙２枚とも、上欄指定枠内に、課題番号（「科目」欄に記入すること）、志望専攻名、受験番号を忘れず記入してください。
8. 試験開始後、課題冊子印刷の不鮮明や落丁などに気づいたら申し出ること。この課題冊子はバラしても構いません。
9. 課題冊子と下書き用紙は持ち帰ってください。

［以上］

課題 1

問 1

「半分に分割することを繰り返す」ことにより時間計算量を削減することは情報科学における重要なアイディアの 1 つである。このアイディアを使ったアルゴリズムの名称を以下の選択肢中から 2 つ選びなさい。3 つ以上存在する場合でも、そのうちの 2 つだけを選べばよい。また、選択した 2 つのアルゴリズムの概略を箇条書き等を用いて簡潔に記しなさい（ソースコードや UML (Unified Modeling Language)ではなく、言葉で記して下さい)。1 つのアルゴリズムについて 100 文字程度で記すこと。時間計算量についても具体的に言及すること（その言及も含めて 100 文字程度とする)。

> アルゴリズムの名称の選択肢：
> 線形探索、二分探索、ハッシュ法、挿入ソート、選択ソート、バブルソート、クイックソート、バケツソート、ボイヤー・ムーアのアルゴリズム、コスト最小弾性マッチング、分枝限定法

問 2

C 言語に関する次の枠内の意見に対するあなたの見解を 200 文字程度で書きなさい。下記の意見のように箇条書きを用いて簡潔に分かりやすく書くこと。

> プログラムは、次の A)、B)に具体的な方針を例示するように、できるだけ短く簡潔に書くのがよい。
> A) 次の例に含まれるような不要な{}は削除すべきである。
>
> ```
> if (age <= 20){
>     happy_birthday(first_name);
> }
> ```
>
> B) 変数名はできるだけ短くした方がよい。短い方が速く入力できるのでプログラムの開発速度が上がる。また、変数名が短い分打ち間違いも減るのでデバッグの工数が減る。短い変数名は、そのプログラムの実行時に必要な記憶容量を削減する効果もある。

問 3

P=NP 問題（クラス NP に属すが クラス P には属さない問題があるかどうか）に対するあなたの見解を 150 文字程度で書きなさい。なお、クラス P とは、多項式時間で解くことができる判定問題の集まりである。判定問題とは答がイエスかノーのいずれかである問題である。また、クラス NP とは、答がイエスのときに非決定的計算機によって多項式時間で解くことができる判定問題の集まりである。非決定的計算機とは処理の分岐に達したとき、都合のよい枝を選ぶことができる計算機である。クラス NP に属すが、クラス P に属すかどうかが「今のところ」不明である問題が多数存在する。

課題 2

問 1　現在の大半のコンピュータのメインメモリは、命令用とデータ用が共通のアドレス空間や共通の物理デバイスを用いて実装されている。命令用とデータ用に異なるアドレス空間や異なる物理デバイスを用いてメインメモリを実装すると、セキュリティの面でどのような点が優れるかを、理由を付けて説明せよ。

問 2　現在の大半のコンピュータでは、メモリシステムに多階層のキャッシュメモリが実装されている。キャッシュメモリを多階層化する利点について、メモリシステムの性能と実装上の柔軟性の面から、理由とともにできるだけ多く述べよ。

課題3

問1

新型コロナウイルス感染症対策の1つとして在宅勤務が推奨されている。自宅からリモート業務を行うには、公衆回線を経由して社内の業務システムに安全にアクセスできる仕組みを用いるのが一般的である。ここで不正アクセスや盗聴を防ぐためにどのような情報通信技術が利用されているか詳しく説明せよ。

問2

ブロック暗号方式を利用する時、暗号化モードとしてECB (Electronic CodeBook) モード (メッセージをブロックごとに分割し、各ブロックを独立に暗号化する方式) が用いられることは通常ない。ECBモードを用いると、どのようなセキュリティ上の問題が考えられるのか説明せよ。

問3

TCP/IPを用いた通信では、TCP (Transmission Control Protocol) とUDP (User Datagram Protocol) が広く使われている。TCPよりも効率の良いコネクション指向型トランスポート層プロトコルの実現を目指したものとして、QUIC (Quick UDP Internet Connections) というプロトコルが開発されている。QUICは、UDPをトランスポート層とするアプリケーション層のライブラリとして実装されているが、使い勝手はTCPとほぼ同様に使用できる。

このような新たなトランスポート層のプロトコルを、UDPをベースにして実装している理由について、TCP/IPのプロトコル階層構造における、ネットワーク層 (IP) とトランスポート層 (UDP) の関係に触れつつ説明せよ。