情報　令和 4 年度試験　7 月 28 日（木）3 限

解答用紙 A4 判両面 2 枚（冊子）　持込不可

※問題の内容に関しては質問を一切受け付けない

共通問題 1

以下の**問 1-1** と**問 1-2** に答えよ．

問 1-1 次の文章の空欄を，以下の語群から最も適切な語を選んで埋めよ．同じ記号の空欄には同じ語が入るものとする．基本的に各語は高々 1 回の利用とするが，(*) のついた語に限っては 2 回まで用いて良いものとする．

盗聴を防ぐための技術として暗号がある．元のデータを［ A ］，暗号化したデータを暗号文といい，暗号文からもとの［ A ］に戻すことを［ B ］という．［ C ］暗号方式では，暗号化と［ B ］のための鍵ペアを作成する．暗号化用の鍵を［ C ］と呼び，［ B ］用の鍵を［ D ］と呼んで自分だけが所有する．［ C ］を知っている人は誰でも暗号化できるが，それを［ B ］できるのは［ D ］の所有者である受信者のみとなる．データの改ざん検知に利用できる技術として［ E ］がある．データに［ E ］を適用して得られた計算結果を，データの［ F ］と呼ぶ．送信者が作成したデータの［ F ］を送信者の［ G ］を用いて暗号化したものが［ H ］となる．受信者はデータと［ H ］の双方を受信して，データから作った［ F ］と［ H ］を［ I ］によって［ B ］した［ F ］とを比較する．これらが一致すればデータは確かに［ G ］の所有者が作成したものであり，改ざんされていないことが確認できる．［ C ］暗号方式の重要な点は，本当に意図した相手の［ C ］であることの保証にある．［ C ］が信頼できる人によって［ H ］されることで，［ C ］が保証される．ユーザの個人的な共通の知り合いなどを介して［ C ］を保証するモデルを［ J ］と呼ぶ．

語群：共通鍵 (*)，公開鍵 (*)，電子鍵 (*)，秘密鍵 (*)，圧縮，一方向ハッシュ関数，構文，信頼の輪，ディジタル署名，電子印鑑，電子指紋，認証局，パスワード，平文，標本化，復号，符号化，DRM，HTTPS，P2P，PKI

問 1-2 次の文章を読み，続く問に答えよ．

ネットワークモデルでは，順にたどっていけるエッジの列を**経路**という．特に，2 ノードを繋ぐ経路の中でエッジ数が最も少ないものを 2 ノード間の**最短経路**という．また，階層モデルをネットワークモデルの一種だとみなしたとき，ノード A から根までの最短経路上にある A 以外のノードを，ノード A の**祖先**という．2 つのノード A，B のどちらの祖先でもあるノードをノード A，B の**共通祖先**という．

1. インターネット上での，あるホスト P から別のホスト Q への通信を考える．以下の問にそれぞれ 2〜3 行程度で答えよ．
   a. ホスト名の具体例を挙げ，それがもつ階層構造を説明せよ．さらに，この階層構造のもとで，P と Q の共通祖先が何に対応するか述べよ．
   b. IP パケットの配送は，ルータをノードとしたネットワークモデルとしてモデル化できる．このモデル化におけるエッジが何に対応するか述べよ．さらに，このモデル化のもとで，P と Q に対応するノード間の最短経路が何に対応するか述べよ．
2. ある国における，ある郵便局 A から別の郵便局 B への郵便物の配送方法を考える．なお，各郵便局にはそれぞれ担当地域が決まっているものとする．
   a. 配送にあたって，郵便局 A，B 双方の担当地域を含む広い範囲を担当地域とする集配郵便局を介して，郵便物を集約・分配することを考える．様々な郵便局の間のこのような配送方法を階層モデルでモデル化したい．このモデル化におけるノードとエッジはそれぞれ何に対応するか述べよ．
   b. 適切な集配郵便局がない場合には，担当地域が隣接する郵便局に送ることにする．このとき，配送方法が経路に対応するように，ネットワークモデルでモデル化したい．このモデル化におけるノードとエッジはそれぞれ何に対応するか述べよ．

共通問題 2

反復処理と 2 分法の計算手順に関連して，以下の問い全てに答えよ．空欄には数，変数，配列，算術式やそれらの組合せなどが入りうる．

1. 教科書（図 5.5）のように，配列 $daymonth_m$ は，m 月（$1 \leq m \leq 12$）の日数を表す．

添字値 m	1	2	3	$\cdots$	12
要素値 $daymonth_m$	31	28	31	$\cdots$	31

春分を 2 月 4 日とし，88 夜（87 日後）が何月かを求めたい．2 月から順に調べる**反復処理**の計算手順を，空欄を埋めて完成させよ．

<残り日数> ← [11]
m ← [12]
while <残り日数> > [13] **do**
  <残り日数> ← <残り日数> − $daymonth_m$
  m ← [14]
done
<答> は m 月

---

2. 正の実数 x（$x > 1$）の平方根を精度 δ で求めたい．区間 (a, b) を解が存在する範囲，c を区間の中央として，**2 分法**による計算手順を，空欄を埋めて完成させよ．

---

a ← 0
b ← x
while [21] > δ **do**
  c ← $\frac{a+b}{2}$
  if [22] > x **then**
    [23] ← c
  else
    [24] ← [25]
  endif
done
<答> は a

---

3. 配列 $nedan_s$ が始発駅から s 駅（$1 \leq s \leq 100$）遠くまで行くのに必要な料金を表す．料金は駅数に対して単調に増加する．

添字値 s	1	2	$\cdots$	100
要素値 $nedan_s$	100	120	$\cdots$	100000

所持金を 1000 円としたときに，何駅先まで行けるかを求めたい．1 駅目から順に調べる反復処理の計算手順を，空欄を埋めて完成させよ．

$yosan$ ← 1000
s ← 0
while [31] ≥ [32] **do**
  s ← [33]
done
<答> は s 駅先

---

4. 2 分法の考え方を参考に，前問の答えを求める計算手順を，空欄を埋めて完成させよ．ただし，平方根の計算過程で $\sqrt{x}$ の解を区間 (a, b) 内に保ちながら区間を狭めたように，今回は半開区間 $[a, b)$ が a 駅先までは必ず行ける，b 駅先には行けないとなるように区間を狭める．また $\lfloor x \rfloor$ は x を越えない最大の整数とする．

$yosan$ ← 1000
a ← 1
b ← 101
while [41] > 1 **do**
  c ← $\lfloor \frac{a+b}{2} \rfloor$
  if $yosan$ ≥ [42] **then**
    [43] ← c
  else
    [44] ← [45]
  endif
done
<答> は a 駅先

---

5. 前問の計算手順は，$yosan$ の金額で反復回数が変わりうる．ただし，$yosan \geq nedan_1$ とする．反復が最大何回行われるかを回答せよ．

6. 実行時間を見積もるために計算量のオーダーが有用である．(1) オーダーの考え方を前問の事例を題材に説明せよ．(2) 実際の計算時間はハードウェアの性能などさまざまな条件に依存する．それにもかかわらずオーダーという考え方が実行時間の予想に役立つ典型的な状況を簡潔に説明せよ．

共通問題 3

以下の**問題 A** と**問題 B** のうち一方のみを選んで答えよ．ただし，いずれを選ぶべきか担当教員から指示があった場合には，その指示に従うこと．

問題 A

ある大学ではリテラシー試験を合格するまでは学内の計算機端末を利用することができない．リテラシー試験は 16 問の○×の二択問題からなり，合格するためにはすべて正解する必要がある．答案送信の試行は何回でも可能であり，試行のたびに正解数のみが情報として開示されるとする（何問目を誤答したかは不明である）．A 氏は無作為に○か×を選択して解答送信を一回試行した結果，「正解数が 14 であった」というメッセージを受け取った．以降でも A 氏は試験問題の本文からは一切メッセージを受け取らないと仮定して各設問に答えよ．

(1) A 氏が受け取った「正解数が 14 であった」というメッセージの情報量について正しいものを以下からすべて選べ．正しいものがない場合は「なし」と解答すること．

(あ)「正解数が 14 であった」というメッセージと「正解数が 2 であった」というメッセージの情報量は等しい．

(い) A 氏が二択問題へすべて○と解答していた場合と最初の 10 問に○，残りは×と解答していた場合を比較すると，前者では正解に含まれる○の数が確定するが後者では確定しないので前者の方が「正解数が 14 であった」というメッセージの情報量は大きい．

(う) 正解数は 0 から 16 までの 17 通りあるので，「正解数が 14 であった」というメッセージの情報量は $\log_2 17$ ビットである．

(え) A 氏はこの後間違った問題の番号を 2 つ受け取ることですべて正解することができるので，全問正解に必要なメッセージの持つ情報量 n と 0 から 15 までの整数値を 1 つ送るのに必要なメッセージの情報量 m を用いて，「正解数が 14 であった」というメッセージの情報量は $n - 2m$ と書ける．

(お)「正解数が 14 であった」というメッセージを受け取った後も第一問の正解が特定されないため，「正解数が 14 であった」というメッセージを受け取る前と後で，第一問の解答を知らせるメッセージ全体（「第一問の正解は○」と「第一問の正解は×」）に関するエントロピーは変化しない

(か)「正解数が 14 であった」というメッセージを受け取る前と後で，全問題の解答を知らせるメッセージ全体に関するエントロピーは増大する

(2) A 氏は二回目の解答送信において，最初の 4 問に対してのみ一回目と異なる選択肢に変更して答案を送信した．二回目の試行において「正解数は 12 である」というメッセージを受け取った場合，このメッセージの情報量は何ビットか．小数点以下を切り捨てて整数部を答えよ．

(3) A 氏は三回目の試行で，最初の 4 問のうち 3 つを無作為に選び一回目で選択した選択肢に戻し，残りの 12 問のうち 1 つを無作為に選び選択肢を変更した．三回目の試行の後に受け取るメッセージは「正解数が 12 である」「正解数が 14 である」「正解数が 16 である」の三種類であると考えたときに，これらのメッセージに関する平均情報量を I ビットとする．

$$I = W + X\log_2 3 + Y\log_2 7 + Z\log_2 11$$

となる有理数 W, X, Y, Z を求めよ．

問題 B

情報技術の進展と普及に関して，下記の問に答えよ．

1. インターネットやソーシャルメディアについて以下の問に答えよ．
   （a）これらが民主主義を加速しうる側面を 3 つ挙げよ．
   （b）これらが民主主義を阻害しうる側面を 3 つ挙げよ．

2. 著作権法とプログラム，そしてデジタルコンテンツについて，以下の問に答えよ．
   （a）次のうち，著作権法において，プログラムの著作物に関して保護されているものをすべて挙げよ．
   アプリケーションプログラム，オブジェクトプログラム，
   解法，規約，ソースプログラム，プログラミング言語
   （b）電子媒体のコンテンツ普及により，DRM が議論となる．DRM は何の略称であるか，答えよ．

3. 情報セキュリティの 3 要素（confidentiality，integrity，availability）のそれぞれについて，日本語での名称と 30 字以内の簡潔な説明を示せ．

4. 個人情報保護のための方策が，国家や社会のセキュリティを脅かす場合がある．2015 年の米国カリフォルニア州での銃乱射事件の捜査過程を例に，個人情報保護を優先する側の主張と，国家や社会のセキュリティを優先する側の主張について簡潔に説明せよ．

5. 2020 年 6 月に公布され，2022 年 4 月から施行された改正個人情報保護法では，従来の個人情報に加えて，個人関連情報についても保護対象（規制の対象）となる場合が生じることになった．この改正法における個人関連情報とは，「生存する個人に関する情報であって，個人情報，仮名加工情報及び匿名加工情報のいずれにも該当しないもの」である．これには，氏名と結びついていないインターネットの閲覧履歴，位置情報，Cookie 情報などが該当する．改正法では，個人関連情報取扱事業者によるこのような情報の第三者への提供において，個人情報と同様にあらかじめ本人の同意取得が必要となる場合があることが記されている．
   （a）このような情報の売買が企業で盛んになる背景について，考えられる主な理由を簡潔に述べよ．
   （b）このような情報が本人の同意なしに第三者に提供または販売されるのを規制した方がよりよい社会になると思われるのはなぜか．特にこのような情報のもつ性質の観点から，2 行程度で論ぜよ．
   （c）このような情報が本人の同意なしに第三者に提供または販売された場合に，個人の不利益となりうる場合としてはどのようなものが考えられるか．できる限り具体的な状況を例示しつつ，簡潔に説明せよ．