情報　共通問題　０７年度前期試験

〔科目名：情報、試験実施日：７月 31 日（火）２限、答案用紙：両面１枚、計算用紙：１枚、持込：一切不可〕

共通問題１

盗聴の危険がある通信環境(例えば電子メール)で、秘密にしたいデータ(例えばクレジットカード番号)を相手に送る場合には、暗号化して送信することが行われる。暗号を用いた通信の手順を説明した以下の文章を読み、問いに答えよ。

＜事前準備＞

A. ある人(a)が鍵(b)を生成する。

B. A で生成した鍵(c)を相手に知らせる。

＜実際の通信＞

C. 送信者が、伝えたい文章を書き、鍵(d)で暗号化し、暗号文を受信者に送る。

D. 受信者が鍵(e)を用いて暗号文を復号し、もとの文章を読む。

共通鍵暗号の場合は、鍵は共通鍵一つである。即ち(b), (c), (d), (e)は共通鍵である。また受信者と送信者は対称であり、役割を入れ替えることができる。即ち(a)は送信者でも受信者でもよい。一方、公開鍵暗号の場合には、秘密鍵と公開鍵の二種類があり、また受信者と送信者に区別がある。

問題:

（１） 公開鍵暗号の場合について考える。上記の手順の(a) について、送信者、受信者のどちらが適切かを答えよ。

（２） 公開鍵暗号の場合について考える。上記の手順 (b), (c), (d), (e) について、適切な言葉を以下から選択せよ。

秘密鍵　　公開鍵　　秘密鍵と公開鍵　　秘密鍵もしくは公開鍵

（３） 上記の手順で、公開鍵暗号を用いて安全に通信ができる前提として、手順 A で生成する鍵(b)が満たしているべき性質を複数述べよ。

（４） 手順 B で鍵を相手に知らせる場合の注意点について、共通鍵暗号と公開鍵暗号を用いる場合の差を比較し、簡単に理由を説明せよ。

共通問題２　以下の問いに答えよ。

（１） 階層モデルの例となっているものを生物の分類、路線図、ウェブのリンク、住所のなかから一つ選び、その例を使って、「階層モデル」がどのようなモデルであるのかを図を用いて説明せよ。

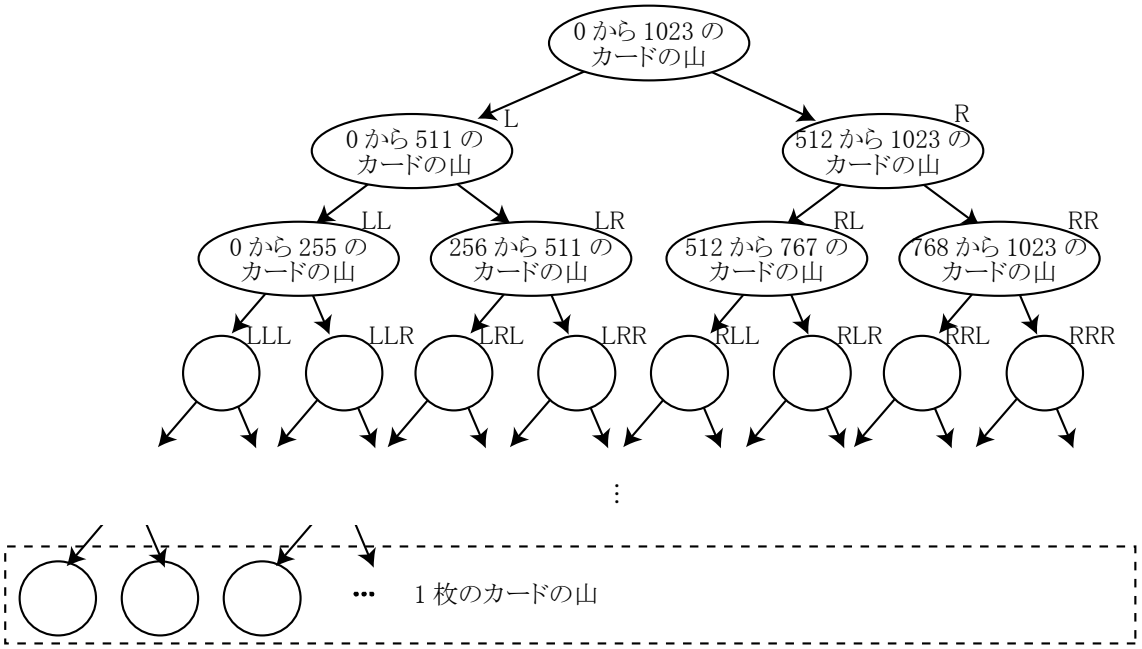
（２） 階層的ファイルシステムを木構造とみなして、その特徴を２つ述べよ。

（３） インターネットにおいて、マシンを特定するためにwww.u-tokyo.ac.jpのようなホスト名と呼ばれるものを使う。ホスト名の任意の「.」から右はドメイン名と呼ばれるもので、マシン群を表すために使われる。上の例では、jp、ac.jp、u-tokyo.ac.jpがドメイン名であり、それぞれ、日本、日本の高等教育機関、東京大学のマシン群を表している。このようなホスト名とドメイン名の構造は、木構造とどのように対応づけられるかを説明し、その管理に木構造の特徴がどのように使えると考えられるかを説明せよ。

共通問題３　以下の問題Aおよび問題Bのうちいずれか一方を選び、答えよ。

問題Ａ：
以下の問いに答えよ。
（１）　情報技術に関連した法律を１つ選び、どのように情報技術と関係するか概要をのべよ。
（２）　情報リテラシーとは何を指すか。情報における批判的思考をふくめて答えよ。
（３）　GUI と CUI のそれぞれの利点と欠点について考察せよ。

問題Ｂ：
0 から 1023 までの整数が書かれたカードが 1 枚ずつあり、でたらめな順序で重ねられている。教科書にある分割型の処理を応用して、下図のような手順で番号順に並べる方法を考える。



a)　最初は、全てのカードが 1 つの山に重ねられている。
b)　まず m を 512 として山のカードを 1 枚ずつめくり、m 未満なら左下の山 L、m 以上なら右下の山 R にふせて重ねる。これをカードがなくなるまで繰り返す。
c)　山 L に b と同じ手順を行い山 LL, LR を作る。このとき LL と LR の枚数が等しくなるように m を選ぶものとする。同様に山 R から枚数の等しい山 RL, RR を作る。
d)　c と同様の手順を繰り返し、すべてが 1 枚のカードの山だけになるまで続ける。
このとき、以下の問いに答えよ。
（1）山 LLLL, LRLLR を作ったとき、そこに含まれていたカードの数の範囲をそれぞれ答えよ。
（2）d の後、0, 100, 500 のカードが置かれた山の名前を答えよ。
（3）d の後、1 枚のカードの山を左から順に見てゆくと、カードの番号が小さい順に並んでいる。そうなる理由を説明せよ。
（4）カードの枚数について一般化し、カードが 0 から $2^n - 1$ まで 1 枚ずつあったときにaからdを通して行ったときの手間を求めたい。カードをめくった回数の合計を$p(n)$とする。このとき(ア) $p(1)$を求めよ。(イ) $n > 1$ のとき$p(n)$を$p(n - 1)$で表わせ。(ウ) $p(n)$を求めよ。