情報(1学期必修)共通問題(2007)解答&解説

文責:亀甲

基本的に分からんとこは読み飛ばしてください。それでも分んなかったら聞いてください。

共通問題1

(1) 受信者

(2) (b)秘密鍵と公開鍵(c)公開鍵(d)公開鍵(e)秘密鍵

(3) 公開鍵によって秘密鍵の推測ができないこと

(4) 共通鍵を用いた場合これが伝達過程で外部に漏れたら機密性が失われるためその取扱いには十分気をつける必要がある。一方公開鍵暗号を用いる場合これが外部に漏れても秘密鍵を自分で保持してさえいれば他人が自分宛の通信を読むことは出来ないため比較的暗号の機密性が維持しやすい。

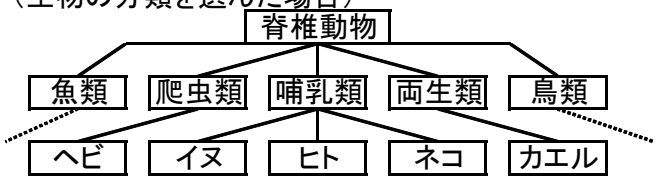
解説

解説と言っても(4)に書いた通りです。共通鍵暗号は鍵一個だけ。公開鍵暗号は暗号化用の鍵と解読用の鍵の二つを用います。共通鍵が外部に漏れた場合この暗号は自由に作れて自由に読まれるので全く意味はないのですが、公開鍵方式なら公開鍵だけが漏れても暗号の解読は行えません。もちろん暗号化は出来るので誰かが送信者を騙って通信することはあり得ますが、それだけなら情報だだ漏れよりはマシってことで。オレオレ詐欺みたいなのに引っ掛かったら知らん。

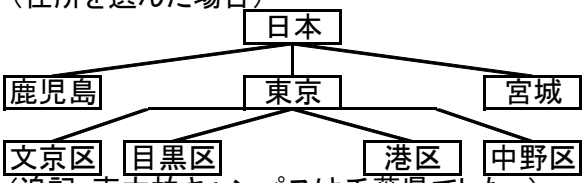
共通問題2

(1)

(生物の分類を選んだ場合)



(住所を選んだ場合)



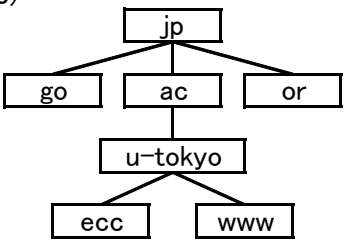
(追記:東大柏キャンパスは千葉県でした。)

一つの上位の要素に対して複数の要素が下位に存在し、各要素を一意に定義できるモデル。上図でヒトを例に考えると、脊椎動物-哺乳類-ヒトと定義出来る。

(2)

フォルダの中にサブフォルダを作って細かい仕分けができる。
フォルダを分けておけば、それぞれのフォルダのサブフォルダが混ざり合ってしまうことはない。
フォルダをたどることで、全てのフォルダとファイルを重複なく一度だけ処理することができる。
サブフォルダ以下の内容と構造を、そのサブフォルダで代表させることができる。たとえば、階層構造の中でサブフォルダを移動すればサブフォルダ以下を移動することができる。

(3)



右の方にあるドメイン名ほど木構造における上位の要素を意味する。木構造を用いることにより各マシンの属するマシン群が一意に定められ、分散管理を可能にする。左図の例で言えば、u-tokyo.ac.jp以下のドメイン名の管理を東京大学に任せることが可能となる。

解説

問題に挙がっている4つのモデルのうち階層モデルで表わされるのは生物の分類と住所です。路線図とウェブのリンクはクモの巣状のモデルで表わされます。
木構造において(俺的に)注目するべきは一意性。様々なものを管理するのに、その対象をただ一つに定義できるという性質は重要な気がします。
(2)の解答は簡単に言うと「綺麗にまとめられて美しい」「混乱が避けられる」くらいの意味です。(ごめん上の解答は教科書のまる写し・・・)フォルダの整理をしていたら便利ですよ〜ってことです。

共通問題3
問題A
(1)
著作権法
1970年に改正、制定された現行の著作権法では、私的使用を目的とした複製は認められていた。複製媒体がデジタル方式のものであっても装置・媒体購入時の値段に含まれる補償金を支払うことで私的使用の複製が同じく認められている。しかし情報技術の発展に伴い媒体の技術的保護手段いわゆるコピーガードが開発されたことで私的使用における複製に関しての事態は変化し、技術発展に伴いコピーガードを回避しての複製も可能となったが、この時はたとえ私的使用を目的とした複製であっても著作権者の承諾がない限り認められないとされた。

(2)
情報リテラシーとは「情報を自己の目的に適合するように使用出来る能力」のことを指す。効果的・効率的に必要な情報を見つけられるとともに、批判的に情報や情報探索過程を評価できることが重要である。現代の情報技術の急速な発展に伴い、情報が大量かつ複雑になり、一般人にとって情報にアクセスする装置がブラックボックス化していることもあって情報に対して真の理解を持って接することが難しくなった。

(3)
CUIは入力がアルファベットによるコマンド入力のため覚えなければならない事が多く、また出力も文字であるため初心者にはなじみにくい。一方で開発が容易であり、ネットワークへの負荷も低い。直接操作が容易であり、先行入力が可能である。
GUIは操作がCUIほど自由でなくまたコンピュータやネットワークへの負荷は大きいが、視覚的でありかつ操作性に優れているため初心者にも比較的容易に操作できる。

解説
この問題は手を出したらいけない気がする・・・
(1)ですが、何をもって情報技術に関連した法律と言うのかよく分からないので問題になりやすい著作権法を題材にしてみました。しかしいい例えが思いつかん・・・
(2)ですが、教科書の10章の下で情報リテラシーについての説明はコンピュータ・リテラシーと混同している気がします。この勘違いは結構多い（ってwikipediaに書いてました）。なので教科書の説明とは異なります。
(3)のCUIがどんなのか分かんないって人、学校で使ったターミナルがそれに当たります。Windowsを使ってる人はアクセサリ→コマンドプロンプトを起動してもいいです。昔の映画に出てくる黒い画面に白いチカチカの出てるコンピュータ画面みたいなのが現れると思います。あれがCUIだと思ってればいいです。対してGUIってのは今（ほとんど）みんなが使ってるパソコンです。（俺Linux使ってるよ～とか言われても知らんがな。）普通に生きてればCUIなんて縁ないと思うから知らなくてもいいです。まあ工学系に進んだら本郷で使うかも知れないけど。
何度も言いますが、持ち込み不可のこの試験でこれに手を出したらダメ。（一部除く。りんむ一とか）

問題B
(1) LLLL　0から63
　　LRLLR 288から319
(2) 0　　LLLLLLLLLL
　　100　LLLRRLLRLL
　　500　LRRRRRLRLL
(3) (c)は対象の山を数字の小さいものと大きいものとに二分する操作であり、それだけを繰り返しているため。
(4) (ア)　$p(1)=2$
　　(イ)　$p(n)=2p(n-1)+2^n$
　　(ウ)　$p(n)=n2^n$

解説
お気づきの方もいらっしゃるでしょう。2進数です。Lを0に、Rを1に置き換えたらまんま2進数です。
でも2進数だと気づかなくても書かれている通りに計算していけば答えにはたどり着けます。
最後は高校数学。