情報過去問解答解説

2008 年度版

共通問題 1

問題解説

暗号化は、教科書 p.49 の 3.2.3（a）にひっそりと解説してあります。共通鍵暗号と公開鍵暗号だけ理解しておけば十分でしょう。しかも教科書の解説はそれなりにわかりやすく書いてあるので、内容についてはそちらに譲ってサボることにします。

共通鍵暗号は、とにかく暗号を「二人だけの秘密」にしておく必要があります。暗号化の方法を知られてしまったらそれだけでアウトなので。一方、公開鍵暗号はもう少し他人に漏れても大丈夫、というかそれを見越して**片方の鍵を公開しておく**のです。この時点で送信者と受信者には格差が生じることになります。送信する側は自分の送りたい内容を**公開された鍵で暗号化**し送るわけです。一度暗号化してしまったら最後、暗号化された文章は自分ですら元に戻すことができません。元に戻せるのは唯一、受信者が持っている**秘密鍵**を使ってのみです。この暗号を作る際に英語Ⅰの 4 章のリスニングでもやったように素数の積を使っていたり、量子コンピュータを使うとその暗号が脅かされたりするという話もありますが、ここでは割愛します。

問題に入ると、（a. 受信者）（b. 秘密鍵と公開鍵）（c. 公開鍵）（d. 公開鍵）（e. 秘密鍵）はすぐにわかります。（3）については、「公開されている鍵では復号が不可能」という絶対条件と、「秘密鍵は他人に知られてはならない」というこれも絶対条件があります。後者は言い換えれば「公開鍵から秘密鍵が予測できてはならない」ということです。素因数分解を用いた暗号が有効であるのは、素因数の積（公開鍵）から元の二つの素因数（秘密鍵）を予測するのが極めて難しく、現在の方法では非常に時間が掛かるため事実的に不可能であるからです。

（4）は相手に鍵を伝える際の注意点について。共通鍵暗号は、暗号が二人だけの秘密であることが絶対条件だったので、伝える際に他人に漏れてはいけません。一方公開鍵暗号は公開鍵が他人に知られる分には全く問題がありません。前者が他人に漏れてはいけない理由は、暗号化と復号を同じ鍵で行っているからで、鍵がばれると他人に暗号を解読されてしまうからです。また後者が他人に知られても平気な理由は、復号は公開鍵とは異なる秘密鍵を用いて行われていて、公開鍵から秘密鍵を予測するのが極めて困難で事実的に不可能であるからです。

共通問題 2

問題解説

階層モデルについての問題です。階層モデルの説明は 08 年度で行っているので参照してください。それっぽいことを書いておけば平気なはずです。ってか路線図は階層モデルじゃない気がするのですが…。

（3）について。ホスト名とドメイン名の構造について、どのように木構造と対応できるかを説明する問題ですが、図を描ければ図を描いて一瞬で済みます。また管理上の利点ですが、教科書にありますが「例えば u-tokyo.ac.jp 以下のドメイン名の管理は東京大学に任せる、といったように、ドメインを分散管理することができる」のようになります。

共通問題 3

問題解説

問題 A

（2）は今年度の範囲外（文系では範囲内）。（3）は 08 年度の解説参照。（1）は省略

だんだん手抜きが激しくなって参りました…。だって論述めんどいし。

問題 B

面倒すぎる…。こんなもの機械にやらせておけばいいものを。これは情報の問題ではなくて算数の問題なような気がしてきます。この年の問題 3 はきついですね。

解く際に注意すべき点は、この分割の仕方が二進数と大きく関係しているということ。いきなり例を出してしまえば、LRLRRRRLRR の山に置かれている数字は何か？と聞かれたときに、その数字が $(0101111011)_2$＝256+64+32+16+8+2+1＝379 だとわかるということです。この作業ではひたすら二分割を繰り返していくので、0=$(0000000000)_2$ から 1023＝$(1111111111)_2$ までの 1024 個の数字は、一回目の分割では L の山に 0=$(0000000000)_2$ から 511=$(0111111111)_2$ までの数字が、R の山には 512=$(1000000000)_2$ から 1023=$(1111111111)_2$ までの数字が割り振られます。つまり L の山は、二進数で数えた最高位の数字が 0 である数字の集合、R の山は最高位が 1 である数字の集合になります。

同じようにして LL は最高位の二桁が 00、LRLRR は 01011、…のように決まっていき、最終的に集合の要素が二進数で表した 10 桁の数字一つになり、例えば 50=$(0000011010)_2$ は LLLLLRRLRL の山に、100=$(0001100100)_2$ は LLLRRLLRLL の山に置かれていることになります。以上のことに**気づければ**、それなりにスムーズに解けるのではないでしょうか。気づかなくても手を動かしている内に規則に気づくはずです。

与えられた数字がどの山に入っているかは、数字を二進数表示できれば判別することができます。500=$(0111110100)_2$ なので LRRRRRLRLL の山に入ります。左から小さい順に数字が並ぶのは、常に左の山に右の山より小さい数字が含まれるよう頑張って分けてきたからに決まっていますね。

（4）は情報ではなくて高校の数列の問題です。これは一般式から求まりますね。初めは二進数表示して n 桁で表せる数字の全体が一つに集まっていて、それらを全てめくらないといけないので 2^n 回めくります。次に最高位の数字が 0 の数字が 2^{n-1} 個、最高位が 1 の数字が 2^{n-1} 個集まっていて、そのどちらの山も 2^{n-1} 回めくらないといけないので合計で $2 \times 2^{n-1} = 2^n$ 回めくります。あとはどこでも同じようになって、一般に k 回目の作業では$2^{k-1} \times 2^{n-k+1} = 2^n$ 回めくることになります。全部で n 桁なので、答えは $p(n) = n \cdot 2^n$ となります。（ア）と（イ）は各自求めてください。