情報学基礎 第４回課題

（6 月 14 日配布；6 月 28 日 23:50 締め切り）

1. データがネットワーク内を流れる様子について以下の問いに答えなさい。ここで k、 M、 G は大きな数を表すときの補助単位であり、k=10^3、M=10^6、G=10^9 である。

   （ア）1k バイトのフレームを通信速度 1kbps のネットワークで伝送するのに必要な時間を計算しなさい。ここで bps（bits per second の略）とはネットワークの伝送速度の単位であり、1 秒間あたりに伝送できるビット数を表している。

   （イ）アプリケーションが 1k バイトのデータ（ペイロード）を送るとき、インターネット・プロトコルの各階層で作成されるパケット（PDU）のサイズ（長さ; バイト数）を計算しなさい。教科書の図 5.4 を参考にすること。解答では、階層の名前とその階層におけるパケットのサイズを答えなさい。データは分割されず 1 つのフレームで送られると仮定し、各階層で付与されるヘッダのサイズは以下の通りとする。トランスポート層 20 バイト、ネットワーク層 20 バイト、データリンク層 14 バイト。

   （ウ）2G バイトのデータを通信速度 100Mbps のネットワークで伝送したい。データは 1k バイト毎にパケットに分割され、**（イ）**と同じ条件でフレーム化され、全フレームが合間無く伝送されるとすると、何秒で送信が完了するか計算しなさい。

   （エ）このパケット群を、教科書の図 5-13(a)に示すストップ・アンド・ウェイトで確実に送信することを考える。パケットを送ってから確認応答が戻るまでに 20ms かかるとき、何秒で全データの伝送が完了するか計算しなさい。ここで、伝送の完了時刻は、最後の確認応答を受信した時刻である。また、送信中に一度もパケットが失われなかったものとする。

   （オ）このパケット群を、教科書の図 5-13(b)に示すスライディングウィンドウで送ると何秒で伝送が完了するか計算しなさい。ウィンドウサイズを 20 に固定し、データを送ってから確認応答が戻るまでに 20ms かかり、パケット送信間隔が一定になるように調整しているものとする。また、一度もパケットが失われなかったものとする。

   （カ）単位時間あたりの受信データ量をスループットと呼ぶ（単位は bps）。**（エ）**、**（オ）**のスループットを計算しなさい。

2. 自分の学籍番号の一の位の数に 8 を加算した値を k とするシーザー暗号について､次の問いに答えなさい。なお、問（イ）と（ウ）は表形式で解答すること。

（ア）使用する k の値を書きなさい。

（イ）教科書の図 6.7 にならい、（ア）で解答した k に対応するシーザー暗号の表を作成しなさい。

（ウ）表 1 の平文と暗号文の変換を完成させなさい。

(1) 自分の氏名の英語表記について，平文と対応する暗号文を示しなさい。

(2) （ア）で解答した k に対応する暗号文を表 2 から選び，それに対する平文を示しなさい。

表 1 平文と暗号文の変換

	平文	暗号文
(1)	*自分の氏名の英文表記*	
(2)		*表 2 中で、（ア）で解答した k に対応する暗号文*

表 2 暗号表

k	暗号文	k	暗号文
08	mcktqltm	13	sbhevrew
09	jalqrvnm	14	rsgqofhs
10	zkcmkvlv	15	qtgcdjaa
11	pfwpcwpz	16	wqbeyiul
12	rqdymfbp	17	crgcrtvj

3. 情報システムには様々な脅威がある。外部の悪者がある会社のサーバにアクセスして、パスワードを探り出し、保存されていた秘密の顧客情報を外部にコピーした。同時に、サーバにあった会計情報の一部を勝手に書き換えた。この者の行為は、教科書 p.77 に示す主な脅威のどれに該当するかを答えなさい。行為のどの部分がどの脅威に該当するのかが分かるように解答すること。複数の脅威を解答してもよい。

提出方法：

- Word、 latex など好みのワープロソフトを使って、上記の問題の解答を作成し、pdf に変換すること。なお、提出ファイルは一つです。問題ごとにファイルを作成しないこと。
- レポートの 1 ページ目の先頭に、学籍番号と氏名を記述すること。
- Keio.jp 上の授業支援システムの課題「第 4 回課題」に作成した pdf を提出すること。