〔Ⅰ〕 次の文章を読み，下の問に答えなさい。

この20年ほどの間の(a)情報通信技術の発達・普及はめざましい。1990年代後半からインターネットが急速に普及し，日本では2000年頃から携帯電話によるインターネットの利用が著しく増加した。総務省の統計によれば2010年に日本ではインターネットを利用したことがある人の割合が人口100人あたり78.0人に達している。世界的な動向を国際電気通信連合の統計でみると，同じ年，インターネットの利用者は人口100人あたり29.7人に達している。最も驚くべき普及を遂げているのが携帯電話で，途上国を含めても携帯電話の契約数は，人口100人あたり78.0件に達している。

だが，情報通信技術のあまりに急速な普及に，社会の取り組みや，人々の意識がついてゆけず，次々に新しい問題点が生じている。(b)電子メールは商品やサービスに関する情報を一度に沢山の人に知らせるには非常に便利な道具である。しかし，反面，受け手の側からすると関心のないメールが大量に届くことにつながり，送り手には適切な運用が求められている。

ウェブサービスにより，わたしたちは，世界中に散らばる情報資源をクリックひとつで簡単に入手できるようになり，これがインターネットの普及の原動力となった。しかし，簡単にコンテンツが入手できるがゆえに，かえって安易に他人の著作物を違法にコピーするなどの(c)知的財産権の侵害が問題になっている。また，突然ウェブサービスが利用不能に陥ったり，(d)個人情報が大量に流出するなど，社会に大きな不安を与える事件が起きている。こうした事件は，ウェブサーバーに大量のアクセスを集中させて障害を引き起こすDDoS攻撃による場合もある。インターネットは，わたしたちの生活のあらゆる場面に浸透しているサービスであるから，安心して利用するために(e)情報セキュリティの強化が求められている。

(問 1) 下線部(a)に関連して，情報通信技術の普及動向に関する記述として**最も不適切なもの**を，下記の①～④の中から１つ選び，その番号を解答欄にマークしなさい。

① 日本ではインターネット利用者の割合がかなり高いので，その伸びは鈍る傾向にある。

② 日本では，インターネットを利用する際，パソコンだけで利用する人が少なくなり，携帯電話などの情報端末を使う人が多くなってきている。

③ 携帯電話の高機能化，低価格パソコンやタブレット端末の登場のおかげで，インターネットの利用という点について，先進国と途上国の差はほぼ解消されている。

④ 国によっては，検索サイトで違法な情報が検索・表示されることを問題視し，政府が違法な情報が閲覧されないように規制を行なっている場合がある。

(問 2) 下線部(b)に関連して，電子メールの利用に関する記述として**最も不適切なもの**を，下記の①～④の中から１つ選び，その番号を解答欄にマークしなさい。

① 金融機関などを装ってメールを送り，偽のページに誘導し不正に個人情報を入手する手口をフィッシング詐欺と呼ぶ。

② 広告などを電子メールで多くの人に送る際に，適正な方法で行なわれるように規制する法律は日本では未だ整備されていない。

③ 迷惑メールは国内だけの対策では十分とはいえないため，発信元に関する情報の交換など，国際的に連携した取り組みが始まっている。

④ 日本語で書かれた迷惑メールであっても，海外から発信されている場合がある。

(問 3) 下線部(c)に関連して，知的財産の保護に関する記述として**最も不適切なもの**を，下記の①～④の中から１つ選び，その番号を解答欄にマークしなさい。

① 商標権によって保護されるのは，他と識別するのに用いられるロゴマークなどである。

② 特許権は一定期間経過後に消滅し，保護対象が広く社会で用いられるように定められている。

③ 著作権法は，著作者の利益を著しく害する複製のことを「私的使用のための複製」と呼び禁じている。

④ 近年，ブランド名などが外国で先に登録されてしまい，その国への企業進出の障害となる事例が起きている。

(問 4) 下線部(d)に関連して，個人情報をめぐる問題に関する記述として**最も不適切なもの**を，下記の①～④の中から１つ選び，その番号を解答欄にマークしなさい。

① 個人情報保護法は，個人情報が流出する被害を未然に防ぐため，営利目的の活動に個人情報を利用することを禁じている。

② 個人情報を収集する場合には，あらかじめ明確な目的を示し，対象となる個人の同意を得て行なわなければならないのが原則である。

③ 個人情報は電子化されたデータばかりでなく，紙に記載された情報も含めて適切に管理される必要がある。

④ 個人情報に関する取り組みが適切かどうかを評価し認証する機関があり，企業やサービスの信頼性を判断する手がかりにすることができる。

(問 5) 下線部(e)に関連して，情報セキュリティに関する記述として**最も不適切なもの**を，下記の①～④の中から１つ選び，その番号を解答欄にマークしなさい。

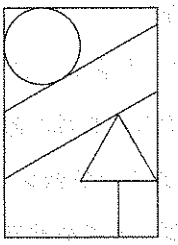
① ネットワークを介してアクセスする情報システムを利用する際に必要となるIDやパスワードを他人に貸し与えても，自分自身が不正アクセス行為を行なうのでなければ，罰せられることはない。

② 政府機関や民間企業の情報システムがDDoS攻撃の標的にされ，閲覧が不能になるなどの障害が発生する事件が起きている。

③ 自分のパソコンが知らない間にDDoS攻撃や迷惑メールの送信に利用されないようにするには，セキュリティソフトを利用することが重要である。

④ 悪意あるプログラムに感染する危険があるため，電子メールの添付ファイルは，警戒し注意深く扱う必要がある。

〔Ⅱ〕 下の枠内の図の描き方を文字だけで説明したい。説明文の空欄A～Cに入る適切な文を解答欄に記述しなさい。



【説明文】

まず円を，枠の上辺と左辺に接し，直径が枠の左辺の長さの約$\frac{1}{3}$となるように描く。

次に直線を，［ A ］ように引く。さらに，この直線の下に，これと平行な別の直線を，枠の左辺の長さの約$\frac{1}{4}$の間隔を空けて引く。

次に正三角形を，一辺の長さが枠の上辺の半分で，［ B ］ように描く。

最後に，［ C ］を引く。

〔Ⅲ〕 下の図1および2は二分決定グラフと呼ばれるもので，図1の終端点(ア)は $\overline{X}Y\overline{Z}$ という式の値が1であることを表し，(イ)は XZ という式の値が0であることを表している。なお，XZ の値が0のとき，XYZ および $X\overline{Y}Z$ の値も0となる。

(問 1) 図2の終端点(1)が表す式を，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。

① $\overline{X}\,\overline{Y}\,\overline{Z}$　② $\overline{X}\,\overline{Y}Z$　③ $\overline{X}Y\overline{Z}$

④ $X\overline{Y}Z$　⑤ $XY\overline{Z}$　⑥ XYZ

(問 2) 図2において，値がつねに0となる式を，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。

① $\overline{X}\,\overline{Y}$　② $\overline{X}Y$　③ $X\overline{Y}$

④ XY　⑤ $\overline{X}Z$　⑥ $X\overline{Z}$

(問 3) 図2において，値が1となる式を，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。

① $\overline{X}\,\overline{Y}\,\overline{Z}$　② $\overline{X}\,\overline{Y}Z$　③ $\overline{X}Y\overline{Z}$

④ $X\overline{Y}\,\overline{Z}$　⑤ $X\overline{Y}Z$　⑥ XYZ

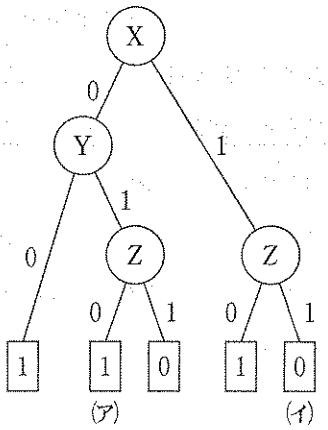


図1

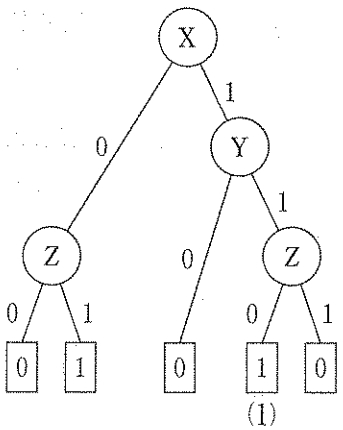


図2

（このページは計算用紙として使用してよい。問題は次ページに続く。）

〔Ⅳ〕 次の文章を読み，下の問に答えなさい。

今日世界中に広がったインターネットは，情報通信サービスの新たな可能性をひらいている。インターネットの通信データは多様な経路をたどって相手側に届けられるので，発信された通信文が盗み見られたり，発信者が他人によってなりすまされたりする危険性がある。そこで利用されるのが暗号技術である。

盗み見を防止する最も素朴な暗号方式に「シーザー暗号」がある。シーザー暗号では，「通信文のアルファベットをx文字すすめる」という規則で暗号化して相手に送り，受け手は「暗号文のアルファベットをx文字もどす」という規則で元の通信文へと復号する。たとえば，$x=3$のとき，通信文の「You」は，暗号文で「Brx」となる。暗号文を盗み見ても一見したところ意味がわからないが，3文字もどせば通信文が復号される。

シーザー暗号におけるxのように，暗号文の送り手と受け手で了解が必要な情報を「鍵」と呼ぶ。シーザー暗号のように，送り手と受け手で共通鍵（たとえば$x=3$）を取り決め，他人には明かさない暗号方式を「共通鍵暗号方式」と呼ぶ。(a)シーザー暗号は容易に解読できてしまうが，解読が難しい共通鍵暗号にはDES暗号などが知られ，使用されている。

しかし，共通鍵暗号方式には難点がある。遠くに住む人どうしがネットワークを介して共通鍵暗号方式で通信しようとすると，最初に共通鍵を取り決める必要があり，その通信自体が盗み見られて共通鍵が知られてしまう可能性がある。そこで注目されるのが「公開鍵暗号方式」である。この暗号方式では，共通鍵のかわりに(b)個人ごとに固有の公開鍵と秘密鍵のペアを作成して使用する。

インターネットで通信される情報は0と1の数字の列で表記される(c)ディジタル信号であるから，その数字列をLビットごとに区切れば，それぞれを（L桁の2進数の）数値として扱うことができる。それに「×7÷5」などの計算をほどこせば別な数値に暗号化でき，それを逆に「×5÷7」などと計算すると元の通信文に復号できる。つまり関数「×7÷5」で通信文に鍵をかけ，逆関数「×5÷7」で鍵をあけると考える。

関数「×7÷5」の逆関数はすぐにわかってしまうので公開鍵暗号には使用でき

ないが，関数$f(x)$がわかってもその逆関数$f^{-1}(x)$は求められないような，特別な関数とその逆関数のペアが生成できることが発見された。この発見によって次の手順で暗号通信ができる。

通信の受け手であるAさんは，適当な乱数をもとにして関数$f_A(x)$と逆関数$f_A{}^{-1}(x)$の組を生成し，関数$f_A(x)$を自分の「公開鍵」として，送り手を含めた一般多数に公開しておく。一方の逆関数$f_A{}^{-1}(x)$は，「秘密鍵」として誰にも知らせずに保管しておく。Aさんへの送り手は通信文をAさんの公開鍵$f_A(x)$で暗号化して送ると，受け手のAさんは秘密鍵$f_A{}^{-1}(x)$で復号できる。(d)第三者が公開鍵を知ったうえで暗号文を盗み見ても解読はできない。

なりすましを防止する方法も公開鍵暗号方式を利用することで可能となる。通信の送り手であるBさんもあらかじめ，公開鍵である関数$f_B(x)$と秘密鍵である逆関数$f_B{}^{-1}(x)$とを生成し，公開鍵を公開しておく。送り手のBさんは，通信文から所定の規則(以下「ハッシュ関数」と呼ぶ)で要約文を作り，その要約文を秘密鍵である逆関数$f_B{}^{-1}(x)$で暗号化した(e)暗号要約文を作る。通信文とその暗号要約文を受け取った受け手は，公開鍵である関数$f_B(x)$で要約文を復号すると同時に，受け取った通信文からハッシュ関数で要約文を生成し，前の復号した要約文と同一かどうか照合する。同一であれば，Bさんは秘密鍵$f_B{}^{-1}(x)$の所有者であることが保証される。

しかしそれでも，関数$f_B(x)$を公開するときから，誰かがBさんになりすましている可能性が残される。それを防ぐために，各人の公開鍵を管理し，正当な公開鍵であることを保証する(f)認証機関が設立されている。

以上の盗み見対策となりすまし防止を同時に施した通信も可能である。そうした通信によって，Pさんからの暗号文と暗号要約文を受け取ったQさんは，Pさんの［ア］を認証機関から入手して準備を整える。暗号文をQさんの［イ］によって復号すれば，まず，盗み見のおそれがない状態で通信文を読むことができる。次に，その通信文からハッシュ関数で要約文を作り，暗号要約文をPさんの［ウ］によって復号したものと照合することで，発信人は確かにPさんであると信頼できる。

こうした公開鍵暗号の技術を活用すれば，ゆくゆくは(g)インターネット上で選挙

を行なうことも可能である。すなわち，①インターネット上で有権者を特定し，②すべての有権者が1票だけ投票可能であり，③投票数を不正が入りこむ余地なく集計し，④有権者が誰に投票したかを秘密にするシステムを構築できる。実現されれば，ネットワークを通した市民運動や政治運動も促進され，(h)選挙制度のあり方も再考されるだろう。

(問 1) (a)シーザー暗号は容易に解読できてしまうというのは，たとえば英文であるとeの出現頻度が極端に多いので，暗号文中に出現する頻度が多い文字が元の通信文のeに対応するなどと推測でき，鍵が解読できてしまうからである。その方法で次の暗号文を解読し，復号した英文を所定欄に記しなさい。(空白とピリオドはそのままでよい。)

Cvasqc kc.

(問 2) (b)個人ごとに固有の公開鍵と秘密鍵のペアを作成して使用する公開鍵暗号方式では，個人ごとに2つの鍵を生成するので，共通鍵暗号方式より多くの異なる鍵が必要だと思われるが，そうではない。たとえば1000人のうちのどの2人もたがいに秘密の(他の998人にはわからない)通信を行なう場合，公開鍵暗号方式では個人ごとに2つの，計2000の異なる鍵で通信が可能であるが，共通鍵暗号方式で必要な鍵の数はそれより多い。その数はいくつになるか計算して所定の解答欄に数字で記しなさい。

(問 3) 次のうち(c)ディジタル信号とは**言えないもの**を，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。

① GIF 形式の画像ファイル

② JPEG 形式の画像ファイル

③ WMA 形式の音声ファイル

④ CD に記録された音声信号

⑤ DVD に記録された映像信号

⑥ VHS テープに記録された映像信号

(問 4) (d)第三者が公開鍵を知ったうえで暗号文を盗み見ても解読はできないとあるが，秘密鍵がわからなくとも公開鍵がわかっているので，あらゆる通信文についてその公開鍵によって暗号文をつくり，盗み見た暗号文と照合し一致したら，原理的には元の通信文が解読できる。しかし，区切りビット数 L が 150 のとき，調べるべきあらゆる通信文は 2 の 150 乗通りある。これを1秒間に1億通りを調べられるコンピュータを1億台同時に動作させたとすると，どのくらいに相当する時間がかかるか。最も適切な語句を，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。なお，1年間は約 3000 万秒である。

① 人間の寿命　② 文明の歴史　③ 人類の歴史

④ 生命の歴史　⑤ 地球の歴史　⑥ 宇宙の歴史以上

(問 5) この(e)暗号要約文は通常どのように呼ばれるか。最も適切な語句を，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。

① 拡張子　② 文字コード　③ ディジタル署名

④ オープンソース　⑤ 相対参照　⑥ インデント

(問 6) 次のうち(f)認証機関と同様の役割をする機関はどれか。最も適切なものを，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。

① 街を見まわる警察

② 小切手を決済する銀行

③ ポイントを発行する商店

④ 印鑑証明を発行する市役所

⑤ 収入印紙を販売する郵便局

⑥ ブランド品を買い取る質屋

(問 7) 問題文中の空欄ア，イ，ウに当てはまる語句の組を，下記の①～⑥の中から1つ選び，その番号を解答欄にマークしなさい。

① ア：公開鍵，イ：公開鍵，ウ：秘密鍵

② ア：公開鍵，イ：秘密鍵，ウ：公開鍵

③ ア：秘密鍵，イ：公開鍵，ウ：公開鍵

④ ア：秘密鍵，イ：秘密鍵，ウ：公開鍵

⑤ ア：秘密鍵，イ：公開鍵，ウ：秘密鍵

⑥ ア：公開鍵，イ：秘密鍵，ウ：秘密鍵

(問 8) 次の(A), (B), (C)の設問のうちから**1つを選び**，その解答を解答欄に 80 文字以内で記述しなさい(句読点なども各 1 文字と数える)。また，**解答用紙の「選択した設問」の記号に○をつけること。**

(A) インターネット上で選挙を行なうことも可能であるとはいえ，そうした選挙のやり方に反対する意見もある。「ディジタルデバイド」という用語を使いながら，反対意見の一例を作文しなさい。 (g)

(B) 選挙制度のあり方も再考されるだろうとあるが，いろいろな新しい選挙制度を考えることができる。「SNS」という用語を使いながら，制度提案の一例を作文しなさい。 (h)

(C) なりすまし防止の手順においてハッシュ関数で要約文を作ってから暗号化する理由は，公開鍵暗号方式の暗号化に時間がかかるからである。そうでなければ，要約文を作らずに通信文そのものを暗号化すればよく，ハッシュ関数は不要である。一般に公開鍵暗号方式の暗号化は共通鍵暗号方式の暗号化にくらべて時間がかかる。一方，盗み見防止の手順では要約文を作れず，長い通信文をすべて暗号化しなければならないので，公開鍵暗号方式での暗号化にともなう時間の遅れは問題になっている。そのため，特定の相手と非常に多くの情報をやりとりする場合は，依然として共通鍵暗号方式が好まれる。しかし，本文に述べたように，共通鍵暗号方式を採用するには最初の共通鍵の通信が盗み見られる問題が残る。この問題の解決方法を答えなさい。

（下のマス目は，問８の下書き用に使用してよい）