1 次の説明文の空欄［ア］～［コ］に入る適切な言葉を解答群から選び，それぞれの選択肢の番号を解答欄にマークしなさい。

(1) ネットワークサービスで使われる場所を表すものを［ア］という。

(2) ネットワーク上でサービスを提供する側のことを［イ］といい，サービスを提供される側のことを［ウ］という。

(3) 会社や家の中など限られた範囲を結んだネットワークのことを［エ］という。

(4) ［エ］とインターネットを中継する通信機器のことを［オ］という。

(5) ［オ］にはノートPCやスマートフォンなどで電波を利用して［エ］に参加する機能が搭載されていることがありこの通信のことを［カ］という。

(6) ［イ］はその原理上，ネットワークからの通信を待ち受けているためインターネット上に［イ］を用意すると攻撃される可能性がある。特に［キ］攻撃と呼ばれる大量に通信を行う攻撃の対象になりやすい。

(7) ［イ］を用意すること無く［ウ］を用意するだけで使えるネットワークサービスのことを雲に例えて［ク］サービスという。

(8) ［ク］サービスは利用するためにアカウントが必要となるが，パスワードに加えてワンタイムパスワードを発行するセキュリティトークンを利用した認証も併用する［ケ］への対応も進んでいる。

(9) ［ケ］を利用していても偽サイトに誘導されて認証に必要な情報を入力してしまうとアカウントを乗っ取られてしまうためEメールやSNSで送られてきた［コ］は安全だと確認できるものだけ開くようにすることが大切である。

解答群

⓪ クラウド	① サーバ	② リンク	③ ルータ
④ クライアント	⑤ 二段階認証	⑥ IPアドレス	⑦ Wi-Fi
⑧ LAN	⑨ DoS		

2　次の各問い（問１～問３）に答えなさい。

問１　２進法表現について述べた次の文章を読み，空欄に入る数字をそれぞれの解答欄にマークしなさい。［ア］～［シ］

５ビットで０と正の整数を表現する場合について考える。表現できる最大値は［アイ］$_{10}$である。次に，負の数も含めた表現を考える。２の補数表現を用いると，５ビットでは，－［ウエ］$_{10}$から［オカ］$_{10}$までの整数が表現できる。また，-6_{10}は２の補数表現を用いると［キクケコサ］$_{2}$となる。さらに，01100_2と11000_2の和を計算すると，10進法表現で［シ］$_{10}$となる。ただし，桁をあふれた数値は無視をすることとする。

問２　SNSでの人のつながりや鉄道路線のようなつながりの関係性を表現する方法として離散グラフがある。図１のように離散グラフは頂点（ノード）と辺（エッジ）によって構成される。例えば図１の場合，ノードａとノードｂ，ノードｂとノードｃ，ノードｃとノードｄ，ノードｃとノードｅ，ノードｄとノードｅがそれぞれエッジによってつながっている。このような離散グラフをコンピュータ上で表現するには，コンピュータで扱うことができるデータ形式で表現する必要がある。一つの例として２次元配列を用いて表現することができる。このような２次元配列は隣接行列という。図１の離散グラフの隣接行列が図２であるとき，図２中の空欄に最も適切な数字を選び，その番号をマークしなさい。［ス］～［タ］

ヒント：隣接行列の横方向を行，縦方向を列と呼ぶ。図２の隣接行列のａ行に着目してみよう。
図１の離散グラフでは，ノードａとノードａをつなぐエッジは存在しないため，ａ行ａ列の値は「０」である。
図１の離散グラフでは，ノードａとノードｂをつなぐエッジは存在するため，ａ行ｂ列の値は「１」である。
図１の離散グラフでは，ノードａとノードｄをつなぐエッジは存在しないため，ａ行ｄ列の値は「０」である。

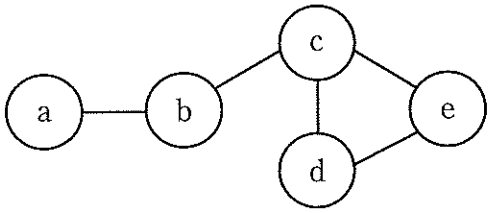


図１　離散グラフ

	a	b	c	d	e
a	0	1	ソ	0	0
b	1	0	1	0	タ
c	0	ス	0	1	1
d	0	セ	1	0	1
e	0	0	1	1	0

図２　隣接行列

3　次の暗号化に関する各問い（**問1**～**問4**）に答えなさい。

問1　次の説明文の空欄［ア］，［イ］に入る最も適切な言葉を選択肢から選び，それぞれ番号をマークしなさい。

情報を送信するときに送り手と受け手以外の第三者にわからないような形にすることを暗号化と言い，暗号化した文を［ア］，暗号化する前の文を［イ］という。

また［ア］から［イ］に戻すことを復号化と言い，暗号化と復号化で用いる手順やデータなどのことを鍵という。インターネット上では途中で情報を場合によっては盗み見ることができるため第三者に見られたくない情報は［ア］としてやりとりされることが望ましい。

選択肢

①　平文　　②　暗号文　　③　情報文　　④　鍵文

問2　次の説明文の空欄［ ウ ］～［ カ ］に入る最も適切な言葉を選択肢から選び，それぞれ番号をマークしなさい。

情報の送り手と受け手で両方が同じ鍵をもって情報を暗号文としてやりとりする方法を［ ウ ］方式という。この方式は同じ鍵を第三者から隠した状態でやりとりしなければならないためインターネットなどの途中で情報を盗み見ることができる手段で，鍵を送ることはできない。

暗号化と復号化でペアとなる別々の鍵を用意して片方の鍵を公開してもう片方の鍵は公開しないで情報を暗号文としてやりとりする方法を［ エ ］方式という。ペアとなる鍵のうち公開した鍵を公開鍵，公開しない鍵を秘密鍵という。この方式は片方の鍵で暗号化した暗号文はもう片方の鍵でしか復号化できない性質をもっている。そのため公開鍵を使って暗号化すると秘密鍵を使わなければ復号化できず，秘密鍵で暗号化すると公開鍵を使わなければ復号化できない。

［ エ ］暗号には秘密鍵で暗号化すると公開鍵を使わなければ復号化できないという性質がある。この性質を使うことで送り手のみが持つ秘密鍵を使って暗号化した暗号文を公開鍵で復号化して確認することで送り手本人であるかどうか確認できる署名として利用するのが，［ オ ］である。このとき最初から偽って公開鍵を作ってしまえばなりすますことができるため信頼できる機関が公開鍵などの情報を電子証明書として管理することでなりすましを防いで本人証明をする技術を［ カ ］という。

［ エ ］方式は一方向性関数というものを利用している。一方向性関数とは計算自体は比較的簡単だか計算結果から計算前を逆算することが非常に困難である関数のことである。現在のコンピュータでは素因数分解が困難であることを利用しているものが代表的である。

選択肢

① 公開鍵暗号	② AES	③ DES	④ 共通鍵暗号
⑤ 手書き署名	⑥ ディジタル署名	⑦ 電子認証	⑧ 対面認証

問3　公開鍵暗号の一つである RSA 暗号に関する次の文章を読み適切な公開鍵と秘密鍵の組み合わせを選択肢の中から選び，その番号をマークしなさい。[キ]

異なる2つの素数 a, b を任意にとる。
$c = ab$ とする。
$(a-1)(b-1)$ を d とすると d との最大公約数が1となる自然数 e を任意にとる。
ef を d で割ったあまりが1となる自然数 f を任意にとる。
このとき c と e が公開鍵で，a と b と f が秘密鍵である。

平文 g を e 乗して c で割った余り h が暗号文である。
h を f 乗して c で割ると平文 g が得られる。

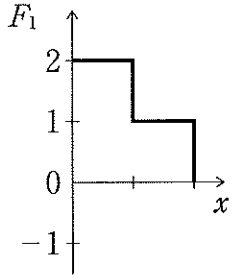
① 公開鍵 $c = 77,\ e = 37$　　秘密鍵 $a = 7,\ b = 11,\ f = 13$
② 公開鍵 $c = 50,\ e = 49$　　秘密鍵 $a = 5,\ b = 10,\ f = 14$
③ 公開鍵 $c = 24,\ e = 51$　　秘密鍵 $a = 4,\ b = 6,\ f = 20$
④ 公開鍵 $c = 28,\ e = 29$　　秘密鍵 $a = 4,\ b = 7,\ f = 18$

問4　次の電子証明書に関する文章を読み，その中から**適切でない文章**を選び，その番号をマークしなさい。[ク]

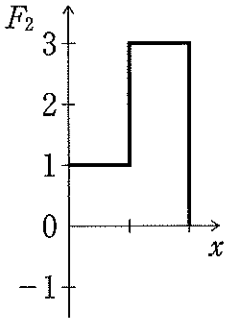
① マイナンバーカードなどの電子証明を行える IC カードは内部に秘密鍵を持っていて，それによって電子証明を行っている。
② 電子証明書などに使われている RSA 暗号は逆算が困難で第三者が絶対解読できないため有効期限を設けていない。
③ インターネットで https:// から始まるサイトは電子証明書を利用しているためフィッシングサイトかどうか確認しやすい。
④ インターネットで https:// から始まるサイトは電子証明書を利用してサイトと利用者の間のやりとりを暗号化している。

4 下記の文章を読み，次の各問い（**問1～問5**）に答えなさい。

(1) ある一定の区間毎に一つの値しか持たないディジタルな関数について考える。2つの区間を持ち，1つ目の区間で2の値を，2つ目の区間で1の値を持つ関数 $F_1 = (2, 1)$，1つ目の区間で1の値を，2つ目の区間で3の値を持つ関数 $F_2 = (1, 3)$ を図に表すと以下のようになる。

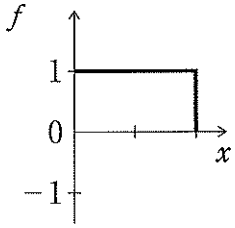


$$F_1 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

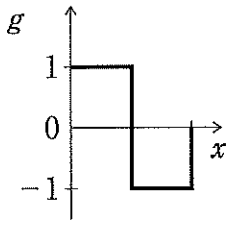


$$F_2 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

この関数を，別の関数 f と関数 g の組み合わせで表現することを考える。関数 f と関数 g を以下に示す。



$$f = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$



$$g = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

問1 空欄 ア ～ エ に入る最も適切な項目を選択肢の中から選び，その番号をマークしなさい。

関数 F_1 と F_2 はそれぞれ以下の式で表すことができる。

$F_1 = af + bg$

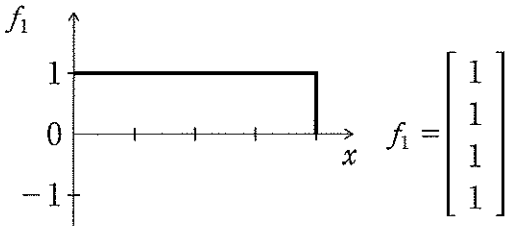
$F_2 = cf + dg$

このとき $a =$ ア，$b =$ イ，$c =$ ウ，$d =$ エ である。

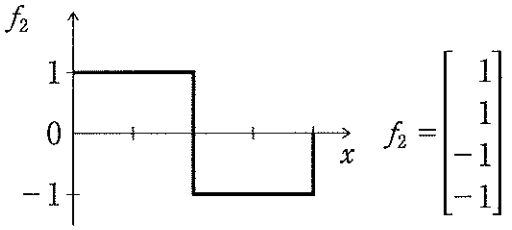
① −2.0　② −1.5　③ −1.0　④ −0.5　⑤ 0.0

⑥ 0.5　⑦ 1.0　⑧ 1.5　⑨ 2.0

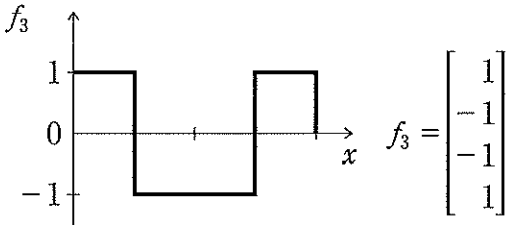
(2)　4つの区間を持つディジタルな関数について考える。関数f_1～f_4を以下に示す。



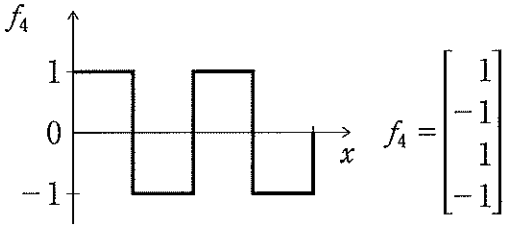
$$f_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$



$$f_2 = \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$$



$$f_3 = \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}$$



$$f_4 = \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

関数f_iとf_jをそれぞれ$f_i = (k_{i1},\ k_{i2},\ k_{i3},\ k_{i4})$，$f_j = (k_{j1},\ k_{j2},\ k_{j3},\ k_{j4})$ とするとき，関数f_iとf_jの積の積分$\int f_i \cdot f_j\, dx$の定義は以下の通りとなる。

$$\int f_i \cdot f_j\, dx = \sum_{l=1}^{4} k_{il}\, k_{jl} = k_{i1}\, k_{j1} + k_{i2}\, k_{j2} + k_{i3}\, k_{j3} + k_{i4}\, k_{j4}$$

ここで関数f_1～f_4は$i \neq j$であるとき，$\int f_i \cdot f_j\, dx = 0$となる。この関係を，関数$f_i$と$f_j$は直交していると呼ぶ。関数$f_1$～$f_4$はそれぞれが互いに直交している。

問2　空欄［オ］～［ク］に入る最も適切な項目を選択肢の中から選び，その番号をマークしなさい。

具体例として，$\int f_2 \cdot f_3\, dx$について計算すると

$$\int f_2 \cdot f_3\, dx = k_{21}\, k_{31} + k_{22}\, k_{32} + k_{23}\, k_{33} + k_{24}\, k_{34} = 0$$

となる。このとき$k_{21}\, k_{31} =$［オ］，$k_{22}\, k_{32} =$［カ］，$k_{23}\, k_{33} =$［キ］，$k_{24}\, k_{34} =$［ク］である。

① −2.0	② −1.5	③ −1.0	④ −0.5	⑤ 0.0
⑥ 0.5	⑦ 1.0	⑧ 1.5	⑨ 2.0	

問3　次の文章の空欄［ケ］に入る数字をマークしなさい。

関数f_1～f_4について，$\int f_i \cdot f_j \, dx$は$i=j$であるとき，$\int f_i \cdot f_j \, dx =$［ケ］となる。

4つの区間を持つディジタルな関数F_nは，どのようなものであっても，関数f_1～f_4を用いて以下のように表現できる。

$$F_n = a_1 f_1 + a_2 f_2 + a_3 f_3 + a_4 f_4$$

そしてこのとき，a_iは，以下に示す式で求めることができる。

$$a_i = \frac{1}{\boxed{\text{ケ}}} \int F_n \cdot f_i \, dx$$

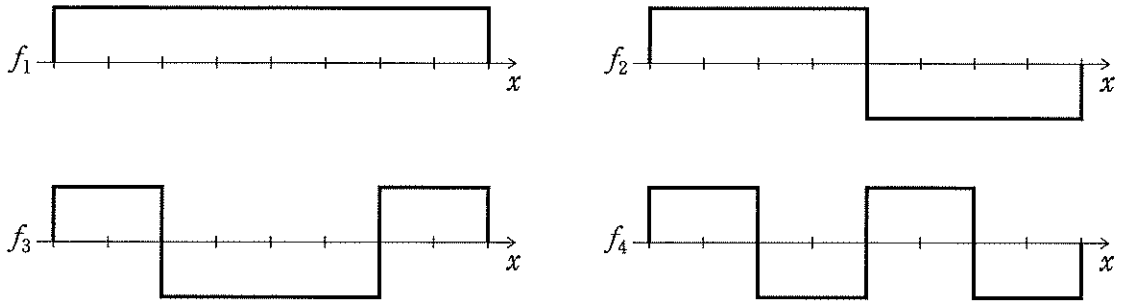
問4　次の文章の空欄［コ］，［サ］に入る数字をマークしなさい。

$F_3 = (-1, 3, 7, -1)$であるとき，F_3は以下の式で表現できる。

$$F_3 = b_1 f_1 + b_2 f_2 + b_3 f_3 + b_4 f_4$$

このとき$b_1 =$［コ］，$b_2 = -1$，$b_3 = -3$，$b_4 =$［サ］である。

(3)　8つの区間を持つディジタル関数について考える。4つの区間の場合と同様に，互いに直交する関数を用意することで，任意の関数を展開することができる。4つの区間のときに用いた関数f_1～f_4は，区間の刻みを2倍に細かくすることで以下のように表現できる。



8つの区間を持つ任意の関数を展開するには，関数f_1～f_4に加えて，f_5～f_8が必要である。関数f_1～f_8は互いに直交している必要がある。

問5　空欄［シ］に入る最も適切なグラフを選択肢の中から選び，その番号をマークしなさい。