3 次の暗号化に関する各問い（問１～問４）に答えなさい。

学習指導要領（4）- 知・技 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

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

学習指導要領（4）- 知・技 - ア
学習指導要領（4）- 思・判・表 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

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 $a = 4,\ b = 7,\ f = 18$

学習指導要領（4）- 知・技 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

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。