高度 OS2013⑧保護とセキュリティ（２）

学生番号 _____ 氏名 _____

問１

暗号方式に関する以下の説明で誤っているものはどれか（複数回答）.

A. 通信文を暗号化しておくことで，第３者が盗み見しても，メッセージの内容が漏れることがない.

B. 暗号化と復号化に同じ鍵を用いる共通鍵暗号は，かぎの管理が簡単である.

C. 公開鍵暗号は，全ての鍵を公開して良いので，管理が簡単である.

D. 共通鍵暗号は，秘密鍵で暗号化し，秘密鍵で復号化する.

E. 公開鍵暗号では，秘密鍵で暗号化し，公開鍵で復号化することで通信内容を秘密にすることができる .

F. 公開鍵暗号では，秘密鍵で暗号化し，公開鍵で複号化することでメッセージが改ざんされていないことを示すことができる.

問２

内容を秘密にするために公開かぎ暗号方式で通信する場合，送信者の暗号化と受信者復号化の手順は以下のどれか. 但し,「○○の公開かぎ（秘密かぎ）」とは,「○○が作成した公開かぎ（秘密かぎ）」という意味である.

A. 送信者は自分の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する.

B. 送信者は自分の秘密かぎで暗号化し，受信者は送信者の公開かぎで復号する.

C. 送信者は受信者の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する.

D. 送信者は受信者の秘密かぎで暗号化し，受信者は自分の公開かぎで復号する.

問３

ある商店は，公開鍵暗号方式を利用して，顧客からの注文メッセージを受信することにより，注文内容が漏れないようにしている．商店，顧客それぞれが利用する鍵の組合せはどれか.

A. 商店：秘密鍵，顧客：秘密鍵　　B. 商店：秘密鍵，顧客：公開鍵

C. 商店：公開鍵，顧客：公開鍵　　D. 商店：公開鍵，顧客：秘密鍵

問４

公開かぎ暗号に基づくディジタル署名により，電子メールの送信者が本人であることを保障する場合のかぎとして，以下の組み合わせのどれを用いればよいか.

A. 受信者の公開かぎと受信者の秘密かぎ　B. 受信者の公開かぎと送信者の秘密かぎ

C. 送信者の公開かぎと受信者の秘密かぎ　D. 送信者の公開かぎと送信者の秘密かぎ

問５

ユーザ X は通販サイト Y から商品を購入する際，以下の手順を用いる.

(1) X は自分の秘密鍵で暗号化した署名を注文メールに付加して送信

(2) Y は X の公開鍵で復号化して受信メールの署名を確認

この手順で確認できることはどれか.

A. Y に届いたメールは，X 本人からの注文である.

B. Y は，X に商品を売ることの許可が得られる.

C. X から Y に送られた注文の内容は，第三者に漏れない.

D. X から送信された注文は，Y に届く.

（裏面にも設問あり）

問６

スライド【添付ファイル】の手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか.

A. 送信者による電子メールの送達確認.

B. 送信者のなりすましの検出.

C. 電子メール本文の改ざん有無の検出.

D. 電子メール本文の内容漏えいの防止.

スライド（添付ファイル：問６～１０）

問6の手順

(a)送信者は電子メールの本文のハッシュ値を計算する.
(b)送信者は，電子メールの本文と上記のハッシュ値を送信する.
(c)受信者は，電子メール本文から自分で求めたハッシュ値と受け取った
ハッシュ値を比較する.

問7～10のプログラム

セマフォの定義

```
P(S):
  Sの値を1減らす
    S≧0→nop;
    S＜0→発行元ﾌﾟﾛｾｽを待機中状態に;
  戻る;

  V(S):
  Sの値を1増やす
    S＞0→nop;
    S≦0→待機中ﾌﾟﾛｾｽ1つをレディ状態に;
  戻る;
```

```
生産者プロセス:
（以下を繰り返す）
(1)ﾃﾞｨｽｸreadし，nextpに入力
(2)P(b2);
(3)buffer[in]=nextp;
(4)in=(in+1) % n;
(5)V(b1);

消費者プロセス:
（以下を繰り返す）
(6)P(b1);
(7)nextc = buffer[out];
(8)out=(out+1) % n;
(9)V(b2);
(10)nextcのﾃﾞｰﾀをﾌﾟﾘﾝﾀにwrite
```

問７

スライドに示すように，セマフォを用いてバッファの排他制御を行う２つのプロセスがある．尚，変数 in，out はﾊﾞｯﾌｧのﾎﾟｲﾝﾀであり初期値は in=0，out=0．また，n はﾊﾞｯﾌｧ数を表し，初期状態ではﾊﾞｯﾌｧは空きとする．

ｎ＝3 の場合，セマフォ変数 b1，b2 の初期値は幾つにすれば良いか.

解答欄　［b1＝　　，b2＝　　］

問８

前問の排他制御プログラムにおいて, 生産者, 消費者は何回かの処理を行い，(1), (10)の read, write ｼｽﾃﾑｺｰﾙを発行したことにより待機状態となっている. また, セマフォ変数の値は, b1=2, b2=1 である．この後，(A)生産者，(B)生産者，(C)消費者，(D)生産者の順で実行中状態となった．その途中経過を考える．

先ず，(A)で生産者が処理を行い待機状態となる直前のセマフォ変数 b1，b2 の値は幾つか.

解答欄　［b1＝　　，b2＝　　］

問９

前問に続いて，(B)で生産者が処理を行い待機状態となる直前のセマフォ変数 b1，b2 の値は幾つか.

解答欄　［b1＝　　，b2＝　　］

問１０

前問に続いて，（C）で消費者が処理を行い，待機状態となる直前のセマフォ変数 b1，b2 の値は幾つか.

解答欄　［b1＝　　，b2＝　　］