⑧保護とセキュリティ(2)

高度OS2015年度

問1　暗号方式

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.

B. 共通鍵暗号は, 通信相手毎に異なる鍵を使用する必要があり, 管理が難しい.
C. 公開鍵暗号では, 秘密鍵は公開してはならない.
E. 通信内容を秘密にするには, 公開鍵で暗号化し, 秘密鍵で復号化する.

問2　セキュリティ(暗号)

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. (基本情報　平成15年度秋期改)
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.

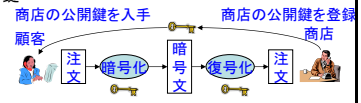
次スライドの説明を参照

問3　公開鍵暗号方式

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. (基本情報　平成18年度・春期改)

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

顧客が注文内容を暗号化して商店に送信
商店は, 暗号文を復号化し, 注文内容を知る



顧客は, 商店の公開鍵(商店が作成・登録)
商店は, 自分の秘密鍵(商店が作成)を用いる

問4　ディジタル署名

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. (基本情報　平成16年度春期改)

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

ディジタル署名では, メッセージの作成者(送信者)のみが, 自分が作成した秘密鍵で署名
受信者は, メッセージの作成者(送信者)の公開鍵を入手し, 署名を復号化する.
従って, 送信者の公開鍵(送信者が作成し, 公開した鍵)と送信者の秘密鍵を用いる

問5　セキュリティ(ディジタル署名)

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. (基本情報　平成19年度・秋期)

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.

ディジタル署名の主な目的は, 以下の2つ
①ﾒｯｾｰｼﾞが改ざんされていない
②署名したのは本人であることを保障
A:注文に署名すれば, ②本人が作成した注文であることが保障される. 注文内容が改ざんされていないことも同時に保障
C:復号化の鍵は公開されているので, このままでは第3者も注文内容が見れてしまう.
B, D:送達確認や売買の許可は, 暗号化とは無関係である.

問6　セキュリティ（ディジタル署名）

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．（基本情報　平成24年度・春期　問40改）

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.

送信者からメールの本文から求めたハッシュ値が，受信者が受け取ったメールの本文から求めたハッシュ値と異なっていた場合，送信時のメールの本文と受信時のメールの本文が異なっていることになり，「メールが改ざんされている」ことになる.

スライド（問6の添付ファイル）

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状態に;
  戻る;

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

生産者プロセス:
（以下を繰り返す）
(1)read(disk, nextp);
(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)write(printer, nextc)

問7　セマフォ

スライド[問6の添付ファイル]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．nはバッファ（buffer[　]）の数を表し，n=3，また，変数in，outはバッファのポインタであり初期値はin=0，out=0とする.
セマフォ変数b1，b2の初期値は幾つにすれば良いか．[b1，b2の順に半角のコンマ「,」で区切り，整数値を半角数字で解答欄に記入（例　3,4）]

答　0,3　（b1=0，b2=3）

セマフォの初期値は，使用可能な資源の数
生産者プロセスが動く（バッファにデータを入力）とb2が1減少し，b1が1増加
消費者プロセスが動く（バッファの内容を出力）とb1が1減少し，b2が1増加

b1が使用中バッファ数，
b2が空きバッファ数を示す.

初期状態では，バッファは空きでありn=3なのでb1＝0，b2＝3.

問8の始めに至るまでの処理例

実行ｻｲｸﾙ	事象の発生と命令の実行	生産者	消費者	b1	b2
	［生産者，消費者生成］	レディ	レディ	0	3
(a)生産者	生産者にCPU割り当て	実行中	レディ	0	3
	(1) read(disk, nextp)=I/O要求	待機	レディ	0	3
(b)消費者	CPU割当て	待機	実行中	0	3
	(6)P(b1)=事象待合せ	待機	待機	-1	3
(c)生産者	read完了．CPU割当て	実行中	待機	-1	3
	(2)P(b2), (3), (4)	実行中	待機	-1	2
	(5)V(b1)=[消費者]事象発生	実行中	レディ	**0**	**2**
	(1)read(disc, nextp)=I/O要求	待機	レディ	0	2
(d)消費者	CPU割当て．	待機	実行中	0	2
	(7), (8), (9)V(b2)	待機	実行中	0	3
	(10)write(printer, nextc)=I/O要求	待機	待機	0	3
(e)生産者	read完了．CPU割当て	実行中	待機	0	3
	(2)P(b2), (3), (4)	実行中	待機	0	2
	(5)V(b1)=[消費者]事象発生	実行中	待機	1	2
	(1)read(disc, nextp)=I/O要求	待機	待機	1	2
(f)生産者	read完了．CPU割当て	実行中	待機	1	2
	(2)P(b2), (3), (4)	実行中	待機	1	1
	(5)V(b1)=[消費者]事象発生	実行中	待機	2	1
	(1)read(disc, nextp)=I/O要求	待機	待機	2	1

問8　セマフォ

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，生産者が(A)を実行し，待機状態となる時のセマフォ変数b1，b2の値は幾つか．[b1，b2の順に半角のコンマ「,」で区切り，整数値を半角数字で解答欄に記入（例　3,4）]

答　3,0（b1=3，b2=0）

問8の初めの状態は，以下のような定常状態．生産者：(1)のreadｼｽﾃﾑｺｰﾙ発行により，readが済むまで待機状態．
消費者：(10)のwriteｼｽﾃﾑｺｰﾙ発行により，writeが済むまで待機状態．
空きバッファ数b1=2，入力済みバッファ数b2=0．readまたはwriteの終了により，各プロセスは，レディ状態になり，CPU割当てにより，実行中となる.

生産者の1回の実行サイクルで空きﾊﾞｯﾌｧが1減り，入力済みﾊﾞｯﾌｧが1増える実行サイクル（A）の中で，(2)P(b2)，(5)V(b1)を実行し，b1=3，b2=0となる．さらに，(1)の実行で待機状態となる.

（次スライド参照）

問8～10の解説

実行ｻｲｸﾙ	発生事象および命令の実行	生産者	消費者	b1	b2	
	［問8の初めの状態］	待機	待機	2	1	
(A)生産者	read完了，CPU割り当て	実行中	待機	2	1	
	(2)P(b2)，その後(3)(4)	実行中	待機	2	0	
	(5)V(b1)	実行中	待機	3	0	
	(1) read(disk, nextp)=I/O要求	待機	待機	3	0	問8
(B)生産者	read完了，CPU割り当て	実行中	待機	3	0	
	(2)P(b2)=事象待合せ	待機	待機	3	**-1**	問9
(C)消費者	write完了，CPU割り当て	待機	実行中	3	-1	
	(6)P(b1)，その後(7)(8)	待機	実行中	2	-1	
	(9)V(b2))=[生産者]事象発生	レディ	実行中	2	**0**	
	(10) write(printer, nextc)=I/O要求，	レディ	待機	2	0	問10
(D)生産者	CPU割り当て，その後(3)(4)	実行中	待機	2	0	
(B)の残り	(5)V(b1)	実行中	待機	3	0	
	(1) read(disk, nextp)=I/O要求	待機	待機	3	0	

問9　セマフォ

前問に続いて，生産者が(B)を実行し，待機状態となる時のセマフォ変数b1，b2の値は幾つか．【b1，b2の順に半角のコンマ「,」で区切り，整数値を半角数字で解答欄に記入．(例　3,-4)】

答　3,-1（b1=3，b2=-1）

前問の実行サイクル（A）により，b1=3，b2=0（空きﾊﾞｯﾌｧが無い）．そのため，実行サイクル（B）では生産者によるバッファ入力処理を止める必要がある．
（B）最初で，生産者が(6)P(b2)を発行すると，b2=-1（b2<0)となり，OSは生産者を待機状態にする．従って，この時の値であるb1=3，b2=-1が答えである．

（前スライド参照）

注：b2<0の状態でそのまま生産者を実行させると入力済みバッファに上書きしてしまう．そのため，消費者が実行して入力済みバッファが空きバッファに変わるまで生産者を待たせる．

問10　セマフォ

前問に続いて，消費者が(C)を実行し，待機状態となる時のセマフォ変数b1，b2の値は幾つか．【b1，b2の順に半角のコンマ「,」で区切り，整数値を半角数字で解答欄に記入．(例　3,-4)】

答　2,0（b1=2，b2=0）

前問の実行により，b1=3，b2=-1となっている．
生産者は，消費者がV命令を実行するまで，ずっと待機状態である．いつかは，消費者のwriteが終了し，実行サイクル（C）が始まる．
まず，(6)P(b1)により，b1=2となる．また，(7)(8)に続いて(9)V(b2)により，b2=0となる．この時点で空きバッファが1個できており，生産者の実行が可能となった．そこで，OSは待機状態の生産者をレディ状態にし，消費者に戻る．次に，消費者は(10)の実行により，待機状態となる．従って，この時の値であるb1=2，b2=0が解答である．

（D）この後，CPUが割り当てられると生産者は，(2)のP命令から戻り，(3)以降の処理を行う．即ち，（D）は，実行サイクル（B）の残りの処理である．

（前々スライド参照）