情報セキュリティ	小林吉純	IC科3年、IS科3年 IM科3年、IN科3年	なし

★解答注意事項

問題文の(　)に入る最も適当な1つの数値、または問題文の後に続く選択項目欄の番号を表す数字(0～9)を決め、マークシートの対応する番号のカラムの中の1つの数字を塗りつぶす(マークする)こと。なお、問題文の(　)には、マークシートのカラム番号が記入されている。例えば、(12　)に対しては、そこに記入すべき数字を選択項目欄の0～9より選び、マークシートの12番カラムの0～9の1つをマークすることにより、解答を行う。更に、数値の記入が求められている場合、不要な(　)欄には0が入るものとする。また、選択項目番号を答える場合、同じ問題中の複数の(　)に同一の選択項目番号を解答してもよい。

★マークシート記入時の注意事項

マークは黒の鉛筆ではっきり行うこと。もしマークシートが汚れた場合は、手を上げて転記を申請すること。名前欄には自分の氏名を記入すること。学籍番号欄の1桁目にはマークシート枚数番号を記入すること。2桁目には何も記入しないこと。学籍番号欄の3桁目には学生番号の1桁目の英数字(A、B、C、Q、N、8、9)を以下のような対応する数字(1、2、3、4、5、8、9)に変換し、記述のこと。

A:1、B:2、C:3、Q:4、N:5、8:8、9:9

学籍番号欄の4～8桁目には、学生番号の下5桁の数字を記入のこと。例えば、学生番号「Q07－123」の場合、学籍番号欄の3～8桁目は「407123」となる。学籍番号欄の下部の対応数字もマークすること。**塗りつぶしが不完全だと採点不能となり、結果が0点となる**恐れがあるので、注意すること!!　なお、提出はマークシートのみとし、問題用紙は持ち帰ること。

マークシート1枚目

〔到達目標 a〕

1. 以下はウィルスの感染経路に関する記述である。(　)内に当てはまる用語を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

①プログラムやデータの(1)時に、それらに紛れてウィルスが侵入する場合がある。
②HTMLテキストの(2)部分に、ブラウザなどの(3)を突くウィルスが潜んでいると、Webページを表示しただけで、ウィルスに感染する。
③メールの(4)によりウィルスが侵入する場合がある。(5)自体がウィルスである場合や(6)がWordやExcelのテキストであっても、(7)ウィルスが潜んでいる場合がある。
④HTMLメールの(8)部分にウィルスが潜んでいると、メールを開いただけで、ウィルスに感染する。
⑤通信サービスを提供するソフトウェアに(9)があると、(10)に接続しただけで、ウィルスが侵入する場合がある。
⑥(11)で、暗号通信などの設定を怠ると不正な接続が行われ、ウィルスが侵入する場合がある。

0. メール　1. 添付ファイル　2. アップロード　3. ダウンロード　4. スクリプト　5. ワーム　6. マクロ　7. セキュリティホール
8. 無線LAN　9. ネットワーク

2. 次の文章は、ウィルス対策について述べたものである。記述が正しい場合には2を、間違っている場合には3をマークせよ。
(12)ワクチンソフトを使用していればウィルスには感染しない。
(13)ウィルスはデータファイルには感染しないので、データのバックアップは必要がない。
(14)メールサーバでメールのウィルスチェックを行っていれば、メールを介したウィルス感染は起こらない。
(15)ウィルス感染後、最も安全で確実な復旧方法は、ワクチンソフトを使用してシステムを修復する方法である。
(16)ウィルスに感染したと思われるときは、すぐにネットワークへの接続を遮断し、システム管理者の指示を仰ぐ。

〔到達目標 b〕

3. 以下は共通暗号方式の適用モードの特徴を記述したものである。それぞれに対応する適用モード名を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

(17)同期式ストリーム暗号として使用できる。
(18)自己同期式ストリーム暗号として使用できる。
(19)鍵が同一の場合、同じ平文ブロックは同じ暗号文ブロックとなるため、解読されやすい。
(20)ストリーム暗号には使用できず、平文ブロックの暗号化に1つ前の暗号文ブロックを使用するため、暗号化は順番に行う必要がある。

0. CCB　1. CBC　2. CFB　3. EBC　4. ECB　5. EFB　6. OBC　7. OCB　8. OFB　9. OBF

裏面にも問題あり

4. RSA暗号に関する以下の記述の( )内に当てはまる数値に対応するマークシートの数字をマークせよ。
相異なる2つの素数を p=7、q=11とする。
(1) この時、k=LCM(p-1,q-1)とおくと、kの値の十の位の数字は(21)であり、一の位の数字は(22)である。従って、公開鍵 e、n のうち、e=7 とすると、条件(k,e)=1を満たすので、e の値は7で問題ない。この時、n の値の十の位の数字は(23)で、一の位の数字は(24)となる。
(2) また、秘密鍵 d を$ed \equiv 1 \bmod k$ に基づき、ユークリッドの互助法を適用し、計算すると、十の位の数字は(25)で、一の位の数字は(26)となる。
(3) 更に、平文 M=49 とした場合の暗号文は、十の位の数字は(27)で、一の位の数字は(28)となる。

〔到達目標 c〕

5. 以下はディジタル署名、手書き署名の特徴である。ディジタル署名の特徴であれば1 、手書き署名の特徴であれば2 、どちらの特徴にも当てはまる場合は3 、どちらの特徴にも当てはまらない場合は4、それぞれに対応するマークシートの数字をマークせよ。

(29)誰でも署名検証を行える。
(30)文書と署名は不可分である。
(31)厳密な署名検証が可能である。
(32)署名のまねをされる危険が高い。
(33)文書作成者の確認には使えない。
(34)署名検証は一般に人の眼に頼っており、正確さに欠ける。
(35)本人の本当の署名を保管している人しか署名の検証ができない。
(36)文書内の1文字が変更されても、署名検証時に文書の改ざんを容易に検出できる。
(37)署名文書内の文章の削除、変更は容易に検出できるが、文章追加の検出は容易ではない。

マークシート2枚目

6. サーバは自身の秘密鍵、公開鍵及び公開鍵証明書を所有している。サーバでクライアント用の秘密鍵、公開鍵を作成したとして、この秘密鍵を安全にクライアントへ送信する場合の手順に関して、( )内に当てはまる用語を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。但し、以下の①～⑥は手順通りの記述ではないので、手順通りに並べ替えたものとして解答すること。

①サーバで、(1)の(2)鍵で受信データを復号し、(3)鍵を取り出す。
②サーバで、(4)鍵で(5)の(6)鍵を暗号化し、クライアントへ送信。
③サーバからクライアントに(7)の(8)鍵が格納された(9)を送信。
④(10)で、(11)鍵を生成。
⑤クライアントで、(12)鍵で受信データを復号し、(13)の(14)鍵を取り出す。
⑥クライアントで、(15)内の(16)鍵で(17)鍵を暗号化し、その結果をサーバへ送信。

0. 共通 1. 公開 2. 秘密 3. クライアント 4. サーバ 5. ハッシュ値 6. MAC 7. 共通鍵証明書 8. 公開鍵証明書 9. 秘密鍵証明書

〔到達目標 d〕

7. チャレンジレスポンスに基づく、共通鍵暗号やハッシュによる認証方法(前者)とディジタル署名による認証方法(後者)には、以下の特徴がある。これらに関して、( )内に当てはまる用語を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

①(18)の場合、認証側で秘密情報と被認証側の対応管理が必要である。
②前者の場合は、(19)を共有する特定の(20)間でしか、認証できない。
③(21)の場合、他人の(22)を保持していないため、盗難や漏えいの危険がない。
④(23)は(24)に比べ、処理時間が短いため、高速な認証情報作成、(25)が可能である。
⑤(26)の場合、相手が同一の(27)を保持していることを確認することにより、(28)する。
⑥前者の場合、(29)を共有しないと認証が行えず、(30)を如何に共有するかが問題となる。

0. 認証 1. 前者 2. 後者 3. 二者 4. 三者 5. 改ざん 6. 蓄積 7. 送信 8. 秘密情報 9. 認証情報

8. メッセージ認証の仕組みに関する以下の記述の( )内に当てはまる用語を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

送受信者間で(31)を共有しておき、送信側はメッセージと(32を連結した結果の(33)を取り、それを(34)とする。そして、送信側はメッセージと(35)を受信側に送信する。受信側では受信したメッセージと(36)を連結した結果の(37)を取り、それと受信した(38)を比較する。これにより、メッセージの(39)と送信側の(40)を行える。

0. メッセージ 1. 認証 2. 秘密情報 3. SHA 4. MAC 5. 送信 6. 受信 7. 完全性チェック 8. ハッシュ値 9. ディジタル署名