情報セキュリティ	小林吉純	IC科3年、IS科3年 IM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、(15　　)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15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「Q06－777」の場合、学籍番号欄の3～8桁目は「406777」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. 以下の不正プログラムに対応する名称を用語欄から選び、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)強制的に広告を表示するプログラム
(2)キーボードからの入力情報を収集するプログラム
(3)プログラムに寄生し、攻撃を行うと共に、他のプログラムに感染し、増殖するプログラム
(4)利用者に気付かれずに、又は承認を得ずに、個人情報を収集し、転送するプログラム
(5)単独のプログラムとして存在し、攻撃を行うと共に、コンピュータからコンピュータに感染し、増殖するプログラム
(6)有用なプログラムに見せかけて、コンピュータに侵入し、攻撃を行うプログラムであり、自己増殖は行わない。
(7)外部からの指示に応じた動作を行うプログラムであり、それに感染したコンピュータは外部から操られ、不正行為を行う。

0. セキュリティホール　1. トロイの木馬　2. キーコレクター　3. キーロガー　4. ワクチン　5. ワーム　6. ウィルス　7. ボット　8. アドウェア　9. スパイウェア

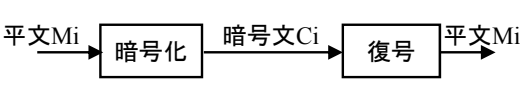
2. 以下の記述は、ウィルス感染の原因について述べたものである。記述が正しい場合には2を、間違っている場合には3をマークせよ。

(8)ウィルスはネットワーク経由で感染するので、ネットワークに接続されていないコンピュータは安全である。
(9)Webページを閲覧するだけでは、ファイルはダウンロードされないので、ウィルス感染の危険はない。
(10)添付ファイルにはウィルスが潜んでいる恐れがあるので、むやみに添付ファイルを開かない。
(11)添付ファイルのないメールであれば、ウィルスには感染しない。
(12)メールサーバでウィルスチェックを行っていれば、少なくともメールを介したウィルス感染はない。
(13)ウィルスに感染するのはセキュリティホールがあるからで、セキュリティホールをすべてふさげばウィルス感染は防げる。
(14)ウィルスはプログラムに感染するので、画像などのデータであれば、安心してダウンロードできる。

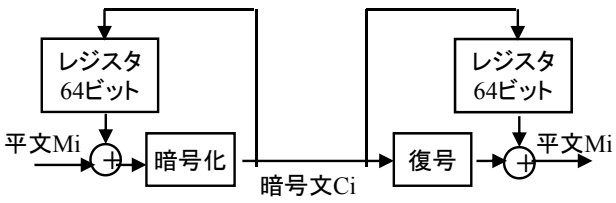
〔到達目標 b〕

3. 下図は共通暗号方式の適用モードを示したものである。それぞれの図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。

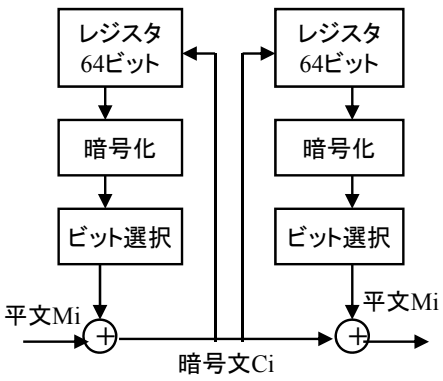
(15)



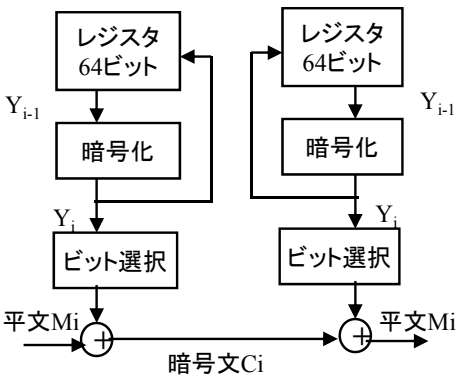
(16)



(17)



(18)



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=3、q=19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(19)であり、一の位の数字は(20)である。従って、公開鍵 e、n のうち、e=5 とすると、条件(k,e)=1を満たすので、e の値は5で問題ない。この時、n の値の十の位の数字は(21)で、一の位の数字は(22)となる。
②また、秘密鍵 d をed≡1 mod 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(23)で、一の位の数字は(24)となる。
③更に、平文 M=46 とした場合の暗号文は、十の位の数字は(25)で、一の位の数字は(26)となる。

〔到達目標 c〕

5. 以下はパスワードやバイオメトリクスによる認証に比べ、PKIによる認証が優れている点を述べたものである。以下の( )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。

・個人の(27)を預かる必要がなく、特定システムに依存しない(28)を有する。
・他人の(29)を預かる必要がないので、他の認証サーバとは異なり、不正侵入等により、他人の(30)を盗まれる危険がない。
・(31)を送信する必要がなく、(32)での認証に効果的である。
・パスワードのように(33)に頼ることがなく、(34)の危険が格段に少ない。
・パスワードに比べると、(35)の解読が極めて困難である。
・バイオメトリクス認証に比べ、特別な(36)が不要で、導入に抵抗がない。

0. 共通鍵 1. 公開鍵 2. 秘密情報 3. 公開情報 4. 透過性 5. 広域性 6. ネットワーク 7. 記憶 8. 装置 9. なりすまし

マークシート2枚目

6. クライアントからサーバに個人情報を安全に送信する場合の以下の手順に関して、( )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①～④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クライアントは(1)から(2)鍵を取り出す。
②サーバからクライアントに(3)の(4)鍵が格納された(5)を送信。
③サーバは暗号化された(6)鍵を(7)の(8)鍵で復号し、(9)鍵を取り出し、暗号化された個人情報を(10)鍵で復号する。
④クライアントは(11)鍵を作成し、個人情報を(12)鍵で暗号化すると共に、(13)鍵を(14)の(15)鍵で暗号化し、これらをサーバへ送信。

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. 以下はチャレンジ・レスポンス方式により、なりすましが防げる理由である。下記の記述の( )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。

・ネットワーク上に(16)をそのまま送信するのではなく、その(17)を送信する。従って、盗聴しても(18)は盗まれない。
・(19)を盗聴しても、(20)から元の(21)は(22)不可である。
・(23)は毎回変わるため、(24)を盗聴しても、その(25)は不可である。

0. ハッシュ値 1. 認証 2. 秘密情報 3. 公開情報 4. 導出 5. 送信 6. 変換値 7. 再使用 8. 平文 9. 暗号文

8. メッセージ認証の手順の( )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。

①送受信者間で(26)を共有する。
②送信側はメッセージと(27)を連結した結果のハッシュ値を取り、それを(28)とする。
③送信側はメッセージと(29)を受信側に送信する。
④受信側では受信したメッセージと(30)を連結した結果のハッシュ値を取り、それと受信した(31)を比較する。
⑤比較結果が一致していれば、受信した(32)が正しく、その作成者は(33)の(34)と判断する。

0. 平文 1. メッセージ 2. 秘密情報 3. レスポンス 4. MAC 5. 暗号文 6. 送信者 7. 共有者 8. ハッシュ値 9. ディジタル署名