注意	試験日	1月18日	所属	部	情報科学部			科目等履修生	学生番号		組
1. 右の欄を正確に記入すること。 2. 所属を○で囲むこと。 3. 前記「1. 2」を守らない答案は採点されないことがあり得る。	座席番号	B－9		学科	IJ	IS	IM		フリガナ 氏名		
				年次	1	2	3	4			

授業科目名　情報セキュリティ　担当者名　小林吉純　対象学生　IJ科3年、IS科3年、IM科3年　参照・使用許可物等　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、(10)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10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。学籍番号欄には学生番号を記入すること。学生番号の中で学科を表す左端の1桁(英数字)を16進数と考えて、3桁の10進数に変換し(即ち、8は008、Aは010、Bは011、Cは012)、学生番号を8桁の番号に変換して記入すること。例えば、「B04－777」は「01104777」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、問題用紙は持ち帰り、フォローアップ授業時に持参すること。

〔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無料のソフトウェアやデータを(1)した場合、ウィルスなどが潜んでいる恐れがある。
②HTMLテキストの(2)部分にウィルスが潜んでいると、(3)サイトにアクセスし、ブラウザで表示しただけで、ウィルスに感染する。
③メールを受信した場合、(4)にウィルスが潜んでいる恐れがある。(4)がWordやExcelのテキストであっても、(5)ウィルスが潜んでいる恐れがある。
④HTMLメールの場合、メールを開くと、(6)などが(3)サイトから取り込まれるが、その時にウィルスがダウンロードされる恐れがある。
⑤通信ソフトウェアに(7)があると、コンピュータを(8)に接続しただけで、ウィルスが侵入する場合がある。

0. 添付ファイル ~~1.~~ 画像データ ~~2.~~ セキュリティホール ~~3.~~ ダウンロード 4. 作成 ~~5.~~ スクリプト ~~6.~~ マクロ 7. メール ~~8.~~ Web ~~9.~~ ネットワーク

2. 以下はウィルス対策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ソフトウェアの(9)をなくすため、ソフトウェアの最新化に努める。
②ウィルス対策ソフトを導入し、(10)ファイルの最新化に努める。
③無闇にプログラムやデータを(11)ない。
④(12)を無条件に信用せず、怪しいファイルは開かない。
⑤アプリケーションの(13)を適切に設定する。
⑥万一に備え、データの(14)に心がける。

0. スパイウェア ~~1.~~ アイコン ~~2.~~ セキュリティホール ~~3.~~ ダウンロード 4. アップロード ~~5.~~ ウィルス定義 6. マクロ ~~7.~~ バックアップ 8. 影響 ~~9.~~ セキュリティレベル

〔到達目標 b〕

3. 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=23とする。
(a) この時、k=LCM(p-1,q-1)とおくと、kの値の十の位の数字は(15)であり、一の位の数字は(16)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(17)で、一の位の数字は(18)となる。
(b) 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(19)で、一の位の数字は(20)となる。
(c) 更に、平文 M=60 とした場合の暗号文は、十の位の数字は(21)で、一の位の数字は(22)となる。

裏面にも問題あり

〔到達目標 c〕

4. PKI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。

PKIとは、(23)暗号方式をベースに(24)暗号方式を組み合わせ、通信相手や文書作成者の(25)、文書の(26)チェック、暗号化による文書の(27)保証などの情報セキュリティに関する機能を提供する情報基盤のことである。(28)の役割は公開鍵とその所有者との対応関係を証明する(29)を発行することであり、この対応関係の保証がなければ、PKIが成立しなくなる。

0. 共通鍵 1. 公開鍵 2. 認証 3. 公証 4. CA 5. AC 6. 秘匿性 7. 完全性 8. 公開鍵証明書 9. 所有者証明書

〔到達目標 d〕

5. 以下はクライアントとサーバ間で秘密情報を共有した後、メッセージ認証を行うまでの手順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。但し、クライアント、サーバとも、自身の公開鍵、秘密鍵、及び相手の公開鍵を所有しているものとする。

①サーバは秘密情報を作成した後、(30)の(31)で秘密情報を暗号化し、クライアントへ送信する。
②クライアントは(32)の(33)で、受信した暗号化秘密情報を復号し、秘密情報を取り出す。
③クライアントはメッセージと(34)を連結し、そのハッシュ値を取り、その結果である(35)とメッセージをサーバへ送信する。
④サーバは受信メッセージと(36)を連結し、そのハッシュ値を(37)とする。これと受信した(38)を比較し、一致していれば、メッセージが(39)で、(40)を共有しているクライアントからの送信と判断する。

0. 共通鍵 1. 公開鍵 2. 秘密鍵 3. クライアント 4. サーバ 5. 完全 6. 不完全 7. MAC 8. デジタル署名 9. 秘密情報

〔到達目標 e〕

6. 以下はディジタル署名、メッセージ認証の特徴である。ディジタル署名の特徴であれば1 、メッセージ認証の特徴であれば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。

(41) 処理に、より時間が掛かる。
(42) メッセージの改ざんを検出できる。
(43) 不特定の人の間での認証ができる。
(44) 送受信者間での認証に使用できる。
(45) メッセージを送信しなくても認証できる。
(46) ハッシュ値に対する暗号化が必要である。
(47) 蓄積メッセージの作成者確認に使用できる。
(48) 送受信者間での秘密情報の共有が前提となる。
(49)認証方式に関して、事前に合意を取る必要がない。
(50)ネットワークに秘密情報を流すことなく、認証が行える。