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、(8)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「Q08－123」の場合、学籍番号欄の3～8桁目は「408123」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、マークシートの裏面には何枚目であるかの番号(①、②)を大きく記述し、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、不正行為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)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
(2)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
(3)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
(4)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。
(5)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。
(6)第3者のWebサーバを経由して、危険なプログラムを送り込む攻撃
(7)広告メールなどのように、毎日何通も送られてくる不要なメール
(8)本当の企業から送信したように見せかけたメールにより、偽のWebサイトへ誘導し、個人情報を搾取するメール

0. セキュリティホール　1. トロイの木馬　2. フィッシングメール　3. スパムメール　4. チェーンメール　5. ワーム　6. ウィルス　7. ボット
8. クロスサイトスクリプティング　9. スパイウェア

2. セキュリティについての以下の文に関して、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。

(9)通常通りコンピュータが使えるときはウィルス感染を疑う必要はない。
(10)メールの本文を閲覧しただけで感染するウイルスがある。
(11)見栄えのよいメールの作成にはHTML形式が相応しいので、メールはHTML形式で送信した方がよい。
(12)ウィルス対策ソフトを導入し、ウィルス定義ファイルを最新化しておけば、ウィルス感染の危険はない。
(13)インターネットに接続しただけで侵入してくるウイルスがある。
(14)ウイルスはコンピュータに障害を与えたり、ファイルを破壊したりするが、情報漏洩につながることはない。
(15)ウィルスはネットワークから侵入するので、ネットワークに接続しなければ、ウィルスに感染することはない。

〔到達目標 b〕

3. 以下は、同期式ストリーム暗号と自己同期式ストリーム暗号の特徴である。同期式ストリーム暗号の特徴であれば1 、自己同期式ストリーム暗号の特徴であれば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。

(16)暗号モードCBCによって実現できる。
(17)暗号モードOFBによって実現できる。
(18)暗号モードCFBによって実現できる。
(19)鍵は直前の暗号文に従って生成される。
(20)鍵生成用の初期値は送受信側で異なってもよい。
(21)性能が要求される通信の下位レイヤで使用されることが多い。
(22)鍵は回数で管理されており、同じ回数であれば、同じ鍵が生成される。
(23)送信される暗号文の喪失後、最初に到着した暗号文の復号は異常となる。
(24)送信される暗号文の喪失後、2番目に到着した暗号文の復号は正常である。
(25)暗号化、復号は、それぞれ平文、暗号文と鍵の排他的論理和により行われる。
(26)送信される暗号文が喪失した場合、鍵の回数にずれが生じ、ずれが永久に持続する。

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=5、q=17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(27)であり、一の位の数字は(28)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(29)で、一の位の数字は(30)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(31)で、一の位の数字は(32)となる。
(3) 更に、平文M=74とした場合の暗号文は、十の位の数字は(33)で、一の位の数字は(34)となる。

〔到達目標c〕

5. 秘密鍵の漏洩がないとして、文書とディジタル署名の受信者が署名検証を行い、署名が正しかった場合に分かることを以下に列挙した。以下の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。

(35)文書が正しく到着した。即ち、送信途中で文書の改ざんがなかった。
(36)署名が正しく到着した。即ち、送信途中で署名の改ざんがなかった。
(37)署名作成に使用した秘密鍵は文書所有者の秘密鍵であった。
(38)署名作成に使用した秘密鍵は文書送信者の秘密鍵であった。
(39)署名作成者は署名に使用した秘密鍵の所有者であった。
(40)署名送信者は署名に使用した秘密鍵の所有者であった。

マークシート2枚目

5. クライアントで公開鍵、秘密鍵の鍵ペアを生成し、登録要求書内に公開鍵を格納し、それをサーバへ送信することにより、公開鍵の登録要求を行うものとする。サーバは届出のあった公開鍵に対応する秘密鍵をクライアントが所有していることを確かめたい。クライアントの秘密鍵をサーバへ渡すことなく、これを確かめる方法に関して、( )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①～⑤は手順通りの記述ではないので、注意すること。

①クライアントは登録要求書とディジタル署名をサーバへ送信する。
②照合結果が(1)いれば、署名が正しいと分かるので、登録要求書内の(2)鍵に対応する(3)鍵をクライアントが所有していると判断できる。
③サーバは取り出した(4)鍵でディジタル署名を復号し、(5)を取り出す。そして、これを登録要求書の(6)と照合する。
④サーバは登録要求書とディジタル署名を受信し、登録要求書から(7)の(8)鍵を取り出す。
⑤クライアントはクライアントの公開鍵が格納された登録要求書の(9)を(10)の(11)鍵で暗号化し、ディジタル署名を作成する。

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. 一致して 8. 違って 9. 公開鍵証明書

〔到達目標d〕

7. 以下は、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とディジタル署名による認証方法の特徴である。共通鍵暗号やハッシュによる認証方法の特徴であれば1、ディジタル署名による認証方法の特徴であれば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。

(12)他人の秘密情報漏洩の危険が全くない。
(13)ハッシュ値に対する暗号化が必要である。
(14)秘密情報を共有しないと認証が行えない。
(15)高速な認証情報作成、認証が可能である。
(16)チャレンジ受信前に認証情報を作成できる。
(17)認証方式に関して、事前に合意を取る必要がない。
(18)認証時には被認証側の公開鍵証明書が必要である。
(19)ネットワークに秘密情報を流すことなく、認証が行える。
(20)認証側で秘密情報と被認証側の対応管理が必要である。
(21)秘密情報を共有する特定の二者間でしか、認証できない。
(22)認証情報が漏洩しても、その再利用による「なりすまし」はできない。

8. パスワードに関する下記の記述の( )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。

・人の(23)に頼る方式であり、覚えやすいパスワードにすると、(24)されやすくなる。
・(25)されにくくするため、(26)文字列、特殊文字を含む文字列、長い文字列にすると覚えにくくなる。
・安全性向上のためには、パスワードの頻繁な(27)が必要だが、それが面倒である。
・パスワードをコンピュータに(28)などの不注意な利用者を完全には排除できない。

0. 暗号 1. 貼り付ける 2. 貼り付けない 3. 更新 4. 秘匿 5. 推測 6. 観測 7. 記憶 8. 意味のない 9. 意味のある