情報セキュリティ	小林吉純	IJ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、(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「A05－777」の場合、学籍番号欄の3～8桁目は「105777」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。

マークシート1枚目

〔到達目標 a〕

1. 以下のフィッシングメールに関する記述を正しい順序に並び替えたい。マークシートのカラム1から5に、1から始まる正しい順序番号に対応する数字をマークせよ。
(1)クレジットカード番号などの個人情報の入力を要求するWebページが表示される。
(2)クレジットカード会社などの信頼できる企業からのメールと見せかけた偽のメールがある個人に送信される。
(3)個人情報は偽のWebサイトから搾取する人物宛にメールで送信される。
(4)メールには本当の企業のWebサイトと誤解させるに足るURLがリンク先として記述されており、メール受信者は本物のURLと信じ、クリックする。
(5)メール受信者は本当の企業のWebページと信じ、個人情報を入力する。

2. 以下の攻撃の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。
(6)侵入後の再侵入を容易にするための仕掛け
(7)大量のパケットを送信する等の手段により、システムを機能停止に追い込む攻撃
(8)特定の相手に的を絞った攻撃
(9)Webアクセス時などに最初は小さなウィルスがダウンロードされ、その後次々と新たなウィルスをダウンロードさせる攻撃
(10)HTMLやJavaScriptの機能を悪用し、パソコンの動作を不安定にさせる攻撃

0. ターゲット型攻撃　1. スピア型攻撃　2. トロイの木馬　3. バックドア　4. マシンクラッシャー　5. ブラウザクラッシャー
6. リトライ攻撃　7. モジュラー攻撃　8. DoS攻撃　9. DoC攻撃

3. 以下の迷惑メール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。
(11)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
(12)有用なメール、重要なメールに見せかけ、転送を促すメール
(13)圧縮率が非常に高い添付ファイル付きメールであり、受信者側での解凍によりハードディスクの容量を圧迫し、パソコンの動作を不安定にするメール

0. 警告メール　1. メール爆弾　2. フィッシングメール　3. チェーンメール　4. 催促メール　5. POPメール　6. HTMLメール
7. アドメール　8. スパムメール　9. スパイメール

〔到達目標 b〕

4. 以下は共通鍵暗号方式、公開鍵暗号方式の特徴である。共通鍵暗号方式の特徴であれば1 、公開鍵暗号方式の特徴であれば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。
(14) 認証に使用できる。
(15) 鍵の長さが比較的短い。
(16) 処理時間が比較的短い。
(17) 大量データの暗号化に適す。
(18) 秘密に保持する鍵の数が少ない。
(19) 鍵を秘密に配送しておく必要がある。
(20) 解読の困難さは鍵の長さに比例する。
(21) 一般に暗号アルゴリズムは非公開である。
(22) 専用ハードウェアの開発が比較的容易である。
(23) 暗号文の受信者は送信者の範囲を特定できる。
(24) 機能するためには、鍵と本人との対応を証明する機関が必要である。

裏面にも問題あり

5. 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=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(25)であり、一の位の数字は(26)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(27)で、一の位の数字は(28)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(29)で、一の位の数字は(30)となる。
(3) 更に、平文 M=42 とした場合の暗号文は、十の位の数字は(31)で、一の位の数字は(32)となる。

〔到達目標 c〕

6. 以下はパスワードによる認証に比べ、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(33)を預かる必要がなく、特定システムに依存しない(34)を有する。
・他の認証サーバとは異なり、不正侵入等により、他人の(35)を盗まれる危険がない。
・(36)を送信する必要がなく、(37)での認証に効果的である。
・パスワードのように(38)に頼る必要がない。
・パスワードに比べると、(39)の解読が極めて困難である。
・ディジタル署名は盗まれても、(40)の危険がない。

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

7. サーバは自身の秘密鍵、公開鍵を所有しており、クライアントはサーバの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を示したい。以下の文を手順に従って並べた場合の順序番号(1から始める)を各カラム毎にマークせよ。但し、以下の文には不要な文もあるので、不要な文に対しては、0 をマークせよ。

(41)サーバで、共通鍵を生成。
(42)クライアントで、共通鍵を生成。
(43)サーバで、共通鍵でクライアントの秘密鍵を暗号化し、クライアントへ送信。
(44)クライアントで、共通鍵で受信データを復号し、クライアントの秘密鍵を取り出す。
(45)サーバで、サーバの秘密鍵で受信データを復号し、共通鍵を取り出す。
(46)クライアントで、サーバの公開鍵証明書内の公開鍵で受信データを復号し、共通鍵を取り出す。
(47)サーバで、自身の秘密鍵で共通鍵を暗号化し、その結果をクライアントへ送信。
(48)クライアントで、公開鍵証明書内の公開鍵で共通鍵を暗号化し、その結果をサーバへ送信。

マークシート2枚目

〔到達目標 d〕

8. チャレンジ・レスポンス方式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。なお、同一番号の( )内には同一の用語が入るものとする。

①前提条件として、認証側と被認証側で(1)を共有しておく。
②認証側が(2)と呼ばれる(3)を生成し、被認証側へ送信する。
③被認証側が(2)と(1)に基づき、ある演算を行い、その演算結果を(4)として認証側に送信する。
④認証側でも(2)と(1)に基づき、同一の演算を行い、その結果と送信されてきた(4)を比較する。
⑤比較結果が(5)であれば、相手の認証はOKと判断する。

0. 一致 1. 不一致 2. 秘密情報 3. 公開情報 4. チャレンジ 5. レスポンス 6. 変数 7. 乱数 8. 認証 9. ハッシュ値

9. 以下は、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(認証を含む)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。

(6)送信文書の改ざん検出を行える。
(7)文書作成者の特定が可能である。
(8)秘密情報を共有しないと認証が行えない。
(9)ハッシュ値に対する暗号化が必要である。
(10)高速な認証情報作成、認証が可能である。
(11)認証はチャレンジレスポンス方式を利用する。
(12)認証方式に関して、事前に合意を取る必要がない。
(13)認証時には被認証側の公開鍵証明書が必要である。
(14)ネットワークに秘密情報を流すことなく、認証が行える。
(15)認証側で秘密情報と被認証側の対応管理が必要である。
(16)秘密情報を共有する特定の二者間でしか、認証できない。
(17)判断根拠となる認証情報をどちらが生成したかを単独では判定できない。