情報セキュリティ 試験問題 (2022 年度)

(注意 1) 計算問題は，途中の計算式や考え方の筋道等を必ず併記すること．
(注意 2) なるべく解答の順序が前後しないようにせよ (前後する場合は注意書きを書くこと).

問題 1

以下の問いに答えなさい.

(i)

$$\begin{cases} x \equiv 7 \pmod{13}, \\ x \equiv 1 \pmod{11}, \\ x \equiv 5 \pmod{7} \end{cases}$$

を満足する最小の正整数x を求めなさい.

(ii) 3^{125} を 10 進数で計算したとき，下位 2 桁の値を求めなさい.

(iii) 合成数 n を法とする剰余類環 R の元 a が乗法に関する逆元を持たないのはどのような場合か．理由も答えること.

問題 2

2 つの素数 $p = 19$，$q = 29$ を用いて RSA 暗号を構成するとき，以下の各問いに答えなさい.

(i) 公開鍵のうち，法 n の値を求めなさい.

(ii) 暗号化指数 $e = 11$ に対応する復号化指数 d を求めなさい.

(iii) 平文 M に対する暗号文 C は $C = M^e \pmod{n}$ で与えられる．暗号化指数 $e = 11$ であるとき，高速指数演算法を用いて暗号化を行うと，法 n における 2 乗演算と法 n における通常の乗算がそれぞれ何回ずつ必要か答えなさい.

問題 3

バイオメトリクス認証に関する以下の各問いに答えなさい.

(i) 本人認証の方法には，バイオメトリクス認証の他に，所有物による方法と知識による方法がある．バイオメトリクス認証をこれらの方法と比較したとき，長所と短所をそれぞれ説明しなさい.

(ii) バイオメトリクス認証に用いる特徴が持つべき性質を 3 つ挙げ，説明しなさい.

(iii) バイオメトリクス認証方式における認証精度は，一般に，FRR(False Reject Rate) と，FAR(False Accept Rate) によって評価される．バイオメトリクス認証を，FAR < FRR の領域で利用する場合は，どのような応用が考えられるか．その理由とともに述べなさい.

問題 4

ネットワークセキュリティに関する以下の文章の（【1】）〜（【15】）に適切な語句を記入しなさい.

- パスワード認証を行う場合，考えられる攻撃として，通信チャンネルを流れるパスワードを盗聴される（【1】）攻撃や，サーバーに保管されているパスワード情報を解析する（【2】）攻撃が考えられる．この他にも，利用者が異なるサービスで同じパスワードを使いまわしていると,（【3】）攻撃の被害を受けやすくなる.
- 公開鍵暗号系を利用する認証方式では，あらかじめサーバーに利用者の（【4】）鍵を保管しておく．サーバーに保管されている（【5】）鍵が流出しても利用者の（【6】）鍵を導出することは計算量的に困難である.

- アルファベット小文字のみで長さ 15 文字のパスワードのエントロピーは（【7】）ビット，アルファベット大文字と小文字を使う長さ 10 文字のパスワードのエントロピーは（【8】）ビットなので，この両者のうち（【9】）の方が総当たり攻撃に強い．($\log_2(26) = 4.7$ とせよ）
- データアクセス制御には，オブジェクトの所有者が利用者の属性ごとに権限を設定する（【10】）制御，システムが強制的にアクセス権限を決める（【11】）制御，オブジェクトへのアクセス権限が利用者の属するロールに基づいて決まる（【12】）制御がある．
- インターネットで利用されるセキュアプロトコルである IPsec は，OSI のネットワーク階層における（【13】）層で動作するプロトコルである．また（【14】）層で使われるセキュアプロトコルとして TLS が知られている．
- ウェブで個人情報等の重要な情報を送信する時は，HTTP ではなく，（【15】）を利用することが望ましい．