情報セキュリティ 試験問題 (2021 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)

$$\begin{cases} x \equiv 1 \pmod{13}, \\ x \equiv 7 \pmod{19} \end{cases}$$

を満足する最小の正整数x を求めなさい．

(ii) $5^{142} \pmod{504}$ を求めなさい (0〜504 の範囲で答えること)．

(iii) 素数 p に対して，$x \neq 0 \pmod{p}$ であるとき，$a \neq b \pmod{p}$ ならば，$ax \neq bx \pmod{p}$ であることを示しなさい．

問題 2

2 つの素数 $p = 17$，$q = 23$ 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) 暗号化指数 $e = 3$ に対応する復号化指数 d を求めなさい．

(ii) 暗号化指数 $e = 3$ であるとき，ある平文 M に対する暗号文 C の値が $C = M^e \pmod{n} = 98$ であった．(ただし，$n = pq$ である) このとき，平文 $3M$ に対する暗号文 C' の値を求めなさい．

問題 3

以下は，零知識対話型証明の一つである Fiat-Shamir 法の手順を説明したものである．なお，p，q は互いに異なる大きな素数であり，$n = pq$ である（p，q は秘密である）．証明者 P は秘密情報 s を持っており，$v = s^2 \pmod{n}$ であることを s に関する情報を漏らさずに検証者 V に証明するものとする．なお，k は正の整数である．

このとき，以下の問いに答えなさい．

ステップ *1:* カウンタ $i = 0$ とする．

ステップ *2:* P は乱数 r を生成し，$x = r^2 \pmod{n}$ を V に送る．

ステップ *3:* V は $e = 0$ または $e = 1$ をランダムに選び，P に送る．

ステップ *4:* P は $y = s^e r \pmod{n}$ を求め，V に送る．

ステップ *5:* V は $y^2 = v^e x \pmod{n}$ が成立することを確認する．成立しなければ，P は秘密 s を持っていないと判断して終了する．成立していれば，i を 1 増やし，$i < k$ ならばステップ 2 に戻る．$i = k$ ならば，P は秘密 s を持っていると判断して終了する．

(i) このアルゴリズムが，P が秘密 s を持っているとして終了したとき，検証者 V はどの程度の確率でこの結果が正しいと判定できるか．

(ii) 証明者 P が秘密 s を持っておらず，ステップ 3 で検証者 V が $e = 0$ を送ってくると予想できるとき，証明者 P はどうすれば検証者 V を騙せるか，答えなさい．

(iii) 証明者 P が秘密 s を持っておらず，ステップ 3 で検証者 V が $e = 1$ を送ってくると予想できるとき，証明者 P はどうすれば検証者 V を騙せるか，答えなさい．

問題 4

以下の語句のうち，3 つを選び，詳しく説明しなさい．説明は，各語句の右側の () 内の語句を全て使用して行うこと．

(i) 情報セキュリティの 3 要素 (CIA, 認証, 法律)

(ii) 公開鍵暗号の安全性 (識別不可能性，選択暗号文攻撃，RSA-OAEP)

(iii) 個人認証 (知識, 永続性, 行動的特徴)

(iv) TLS(ネットワーク層, 公開鍵証明書, UDP)

(v) ランサムウェア (マルウェア，バックアップ，ビットコイン)

(vi) 量子コンピュータ (RSA 暗号, ショアのアルゴリズム, 耐量子計算機暗号 (PQC))