情報セキュリティ 試験問題 (2020 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)

$$\begin{cases} x \equiv 2 \pmod 5, \\ x \equiv 3 \pmod 7, \\ x \equiv 10 \pmod{11} \end{cases}$$

を満足する 最小の正整数x を求めなさい.

(ii) $11^{194} (\mathrm{mod} 360)$ を求めなさい (0〜360 の範囲 で答えること).

問題 2

以下の問いに答えなさい.

(i) 素数 $p = 131$ であるとき，$g = 2$ は法 p における原始元 (生成元) である．このとき，$y = g^{24} (\mathrm{mod} p)$ を求めなさい ($1 \leq y < p$ の範囲 で答えること).

(ii) 素数 $p = 131$, $g = 2$, $s = 3$, $y = g^s (\mathrm{mod} p)$ であるとき，平文 $M (0 < M < p)$ を

$$(C_1, C_2) = (g^r (\mathrm{mod} p), M \cdot y^r (\mathrm{mod} p))$$

により暗号化 (r は，乱数 $(0 < r < p - 1)$ である) し，暗号文 $(C_1, C_2) = (11, 117)$ を得た．この暗号文を 復号するための式 を示し，平文 M の値を求めなさい.

問題 3

ユーザ Alice がサーバにログインするとき，以下のような認証方式を考えた．なお，Alice の公開鍵は P_A，秘密鍵は S_A とする.

ステップ *1:* Alice はサーバに，ユーザ名 ID_A を送り，引き続いて，ユーザ名に対する署名 $Sign(ID_A)$ を送る.

ステップ *2:* サーバは，署名 $Sign(ID_A)$ を検証し，正しければログインを許可する．正しくなければ許可しない.

(i) Alice が署名 $Sign(ID_A)$ を作成する際に用いる鍵は P_A と S_A のいずれの鍵か，答えなさい.

(ii) この認証方式は，リプレイ攻撃に対して脆弱である．なぜか，その理由を答えなさい.

(iii) 前問 (ii) に関して，どのように改良すればリプレイ攻撃に耐性を持つか，修正したプロトコルを示しなさい.

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 (暗号, 情報資産, DDoS 攻撃)

(ii) PKI (公開鍵暗号，X.509，認証局，CRL)

(iii) RSA 暗号 (公開鍵暗号，素因数分解，オイラー関数)

(iv) バイオメトリクス認証 (普遍性，マルチモーダルバイオメトリクス，ROC)

(v) SSL/TLS(IPsec，プロキシ，トランスポート層)

(vi) マルウェア (ウイルス，ボット，ランサムウェア)