情報セキュリティ 中間試験

2022 年 11 月 18 日　　担当：萩原，高野

氏名	
学籍番号	
学年とクラス	b2123456
出席番号	

【注意事項】

- 電卓使用可（スマホ等，通信機能を持つ機器は使用不可），資料持ち込み不可．
- 正整数 $x \geq n$ に対し，x を n で割った余りは

$$x \bmod n = x - \lfloor x/n \rfloor \times n$$

を用いて計算してもよい．但し，$\lfloor x/n \rfloor$ は小数部切り捨ての除算である．
- 冪剰余は 2 進数展開した指数部の非ゼロ桁に対応する重みの積の剰余をオーバーフローに注意しながら計算してもよい．
例) 重みを $A_j \stackrel{\text{def}}{=} 3^{2^j} \bmod 10$ とする．$19 = (10011)_2$ つまり $19 = 2^4 + 2^1 + 2^0$ であるから，$3^{19} \bmod 10 = A_4 \cdot A_1 \cdot A_0 \bmod 10$.

I) 設問に回答せよ．

(1) 次のインシデント ① ② ③ によって損なわれる情報セキュリティの 3 要素を，選択肢 **ア** 機密性，**イ** 完全性，**ウ** 可用性 からそれぞれ選べ．

① DDoS 攻撃によって，Web サイトがダウンした．

② キーボードの打ち間違いによって，不正確なデータが入力された．

③ PC がマルウェアに感染したことによって，個人情報が漏えいした．

①	②	③

(2) シーザー暗号による暗号文　GWCEZWE　に対応するローマ字表記の平文を解読せよ．

(3) 暗号方式に関する記述のうち，適切なものはどれか．

ア RSA は共通鍵暗号方式，AES は公開鍵暗号方式の一種である．

イ 共通鍵暗号方式では，暗号化及び復号に同一の鍵を使用する．

ウ 公開鍵暗号方式を通信内容の秘匿に使用する場合は，暗号化に使用する鍵を秘密にして，復号に使用する鍵を公開する．

エ ディジタル署名に公開鍵暗号方式が使用されることはなく，共通鍵暗号方式が使用される．

(4) 2 要素認証に該当する組みはどれか．

ア クライアント証明書，ハードウェアトークン

イ 静脈認証，指紋認証

ウ パスワード認証，静脈認証

エ パスワード認証，秘密の質問の答え

(5) アプリケーションソフトウェア (App) にディジタル署名を施す目的はどれか．

ア App の改ざんを利用者が検知できるようにする．

イ App の使用を特定の利用者に制限する．

ウ App の著作権が作成者にあることを証明する．

エ App の利用者による修正や改変を不可能にする．