

選考問題

【質問1】共通

あなたがミニキャンプに応募された動機について教えてください。また、この講義で学んだことを何に役立てたいかを教えてください。

【質問2】

あなたが興味をもっているセキュリティ技術とその理由について教えてください。

【質問3】

あなたが興味を持った脆弱性（攻撃手法でも可）とその理由を教えてください。

【質問4】

これからCMSシステムを公開しようと検討しています。どのようにセキュリティ対策をしたら良いでしょうか？あなたの考えを教えてください。

選考問題

【質問5】

RSA暗号で使われる数学の基礎固めの出題です。

- a. 「剰余」について調べ、17の法3における剰余（17を3で割った余り）を求めよ。
- b. 「モジュラ逆数」について調べ、 $4^{-1} \pmod{7}$ （4の法7におけるモジュラ逆数）を求めよ。解は無限に存在するが、その1つを答えれば良い。

【質問6】

AさんがBさんだけに秘密のメッセージを送るために使うために、どの種の鍵を使うのが最も適切か答えよ。ただし、各鍵が改ざんされていないことは別途証明できているものとする。

- a. 選択肢1: Aさんが作成した公開鍵
- b. 選択肢2: Aさんが作成した秘密鍵
- c. 選択肢3: Bさんが作成した公開鍵
- d. 選択肢4: Bさんが作成した秘密鍵

選考問題

【質問7】

講義で使うPythonプログラミング環境を整えてもらうための出題です。下記リンク先のPythonのプログラムを実行し、出力結果を答えよ。

<https://gist.github.com/laysakura/c841d6f6a1beb6e12643eeb054b3af2d>