2024前期中間（2章まで）

2025年5月28日　14:30

1. 情報セキュリティの三要素名を挙げ、webサーバを運用する場合に各要素を強化する対策例をそれぞれ挙げよ。ただし、例えば「OSをアップデートする」「気を付けて管理する」といった、どの要素にも通じるような例や抽象的な例は不可とする。（6点）
   （　　性）　対策例：（　　）
   （　　性）　対策例：（　　）
   （　　性）　対策例：（　　）

2. CSIRTとはどのようなものか概説せよ。また、読みを答えよ。（3点）
   説明：
   読み：

3. 典型的なインシデントレスポンスの順に沿って以下の各項目に番号を付けよ。（4点）
   （　）封じ込め・根絶　　（　）インシデント後の対応　　（　）準備・予防対策
   （　）検知と分析　　（　）システム復旧

4. リスク対策の低減・保有・回避・移転のうち、「移転」とはどのような対応を取ることか概説せよ。また、一般的に移転策は「リスク発生時の損害の度合い」「発生確率」の大きさがどのような場合に適用されるものか答えよ。（4点）

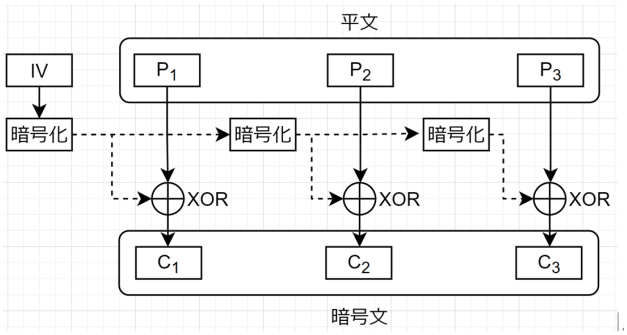
   リスク発生時の損害の度合い：　小さい　　大きい
   発生確率：　　低い　　高い
   説明：

5. ゼロデイ攻撃とはどのような攻撃手法か概説せよ。（3点）

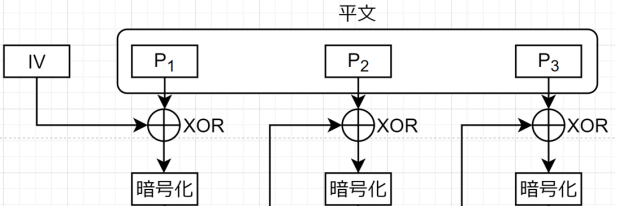
6. バーナム暗号の持つ問題点を1つ挙げよ。（3点）

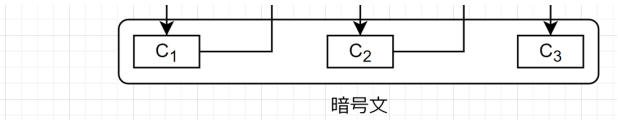
7. 暗号に関する各文について内容が適切であればT、そうでなければFを付けよ。（各1点）
   （　）シーザー暗号の仕組みは現代暗号でも一部取り入れられている。
   （　）3DESはストリーム暗号である。
   （　）AESはブロック暗号の一種であり、SPN構造を用いる。
   （　）RC4はAEADアルゴリズムの一つであり、無線LANのWEPで利用されている。
   （　）PKCS#5では、入力文字列長がブロック長の倍数であるときもパディングを行う。
   （　）鍵0xD9で平文0x39をバーナム暗号化すると0xe0になる。
   （　）AからBへ公開鍵暗号を使って通信する場合、Aの秘密鍵で平文を暗号化する。
   （　）AからBへデジタル署名を送る場合、Aの公開鍵で平文を暗号化する。
   （　）ユーザAが公開鍵暗号でB、C、Dと互いに秘密の通信を行う場合、Aは3個の秘密を保持する必要がある。
   （　）ハイブリッド暗号では、共通鍵暗号を使って相手に安全に秘密鍵を渡す。
   （　）RSAはECCと比べて等価安全性の点で優れている。
   （　）RSA暗号で暗号化鍵（n=7、e=5）、復号鍵（n=7、d=不明）のとき、平文P=2を暗号化すると3になる。
   （　）CTRモードは並列に暗号化を行える。

8. 各図に示すブロック暗号化の構成に対応する運用モード名を答えよ。（各3点）
   図1：（　　）
   図2：（　　）
   図3：（　　）

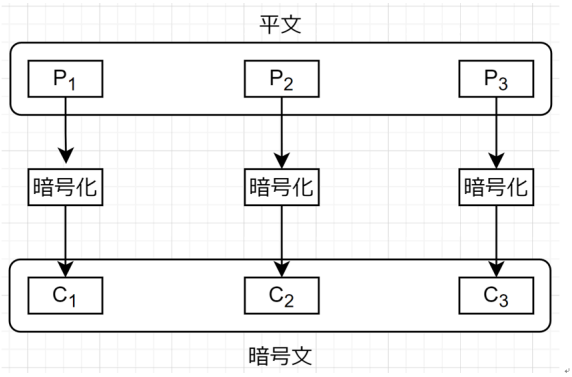


（図 1）





（図 2）



（図 3）

9. ユーザAとBがDiffie-Hellman鍵共有アルゴリズムで共有鍵Kを導出する際の手順を完成させよ。（各2点）
    1. A、Bは素数pとgを決め、その値を2人で共有する。
    2. A、Bはそれぞれ秘密鍵Ka、Kbを乱数で生成する。
    3. Aは（　　）
    4. Bは（　　）
    5. （　　）
    6. Aは次式でKを求める。
       （式：　　）＿＿＿＿＿＿
    7. Bは次式でKを求める。
       （式：　　）＿＿＿＿＿＿

10. セキュアハッシュに関する以下の各文について、内容が妥当であればT、そうでなければFを付けよ。（各1点）

    （　　）住所録データSからハッシュ値H_1を求め、1年前にSから求めたハッシュ値H_0と比べると$H_1 = H_0 + 1$の関係になった。このことからSは改ざんされていないと判断した。

    （　　）ハッシュアルゴリズムを検証したところ、衝突困難性の性質を持つことが分かった。そのためこのアルゴリズムは使うべきでないと判断した。

    （　　）256byteあるデータAからハッシュ値を求めたところ、128byteで出力された。このことから、Aに64byte分のデータBを結合し、再び同じアルゴリズムでハッシュ値を求めた場合、160byteになると考えられる。

    （　　）ハッシュアルゴリズムを検証したところ、逆関数の存在を確認できた。そのためこのアルゴリズムは使うべきでないと判断した。

    （　　）md5sumとsha256sumのコマンドがあったので、前者を優先して使った。