情報セキュリティ基礎 演習問題

光成滋生

last update: 2025/10/16

秘密鍵の転送

問題

- 64TiBのHDDデータを東京から大阪に転送したい。10Gbpsの専用線で送ると何時間かかる? ただし伝送効率を95%とする。小数点2桁目を四捨五入して小数点1桁目までを答えよ。

答え

- 64TiB / (10Gbps * 0.95) = 64 * 1024 * 1024 * 1024 * 1024 / (10 * 1e9 / 8 * 0.95)/3600 = 16.46 = 16.5時間

解説

- bpsはbit per secondの略で1秒あたりのビット数を表す
- K, M, Gは10進接頭辞でそれぞれ $10^3, 10^6, 10^9$ を表す
- SDDやメモリ容量は通常2進接頭辞が使われる Ki, Mi, Gi, Ti はそれぞれ $2^{10}, 2^{20}, 2^{30}, 2^{40}$ を表す
- 100kmを越える10Gbpsの専用線はとても高い（検索してみよ）
  - 1回だけの転送なら新幹線などを使って人力でHDDを運ぶ方が速くずっと安い

秘密鍵の2回利用

問題

- 年齢を1バイトの整数値としてOTPによる暗号化を考える。
  子供の年齢の暗号文が16進数で0x1eだったとき,
  同じ秘密鍵を利用した大人の暗号文が0x5eだった。
  大人の年齢は10進数で何歳以上?

答え

- 子供の年齢を x, 大人の年齢を y, 秘密鍵を s とすると $x \oplus s = 0x1e$, $y \oplus s = 0x5e$
  よって $x \oplus y = 0x1e \oplus 0x5e = 0x40 = 64$
  子供の年齢は $0 \leqq x < 18$ なので $y \geqq 64$

CBCモードの並列化

問題

- CBCモードの復号は並列化可能である。その理由を延べよ。

答え

- 初期化ベクトル IV を C_0, 暗号文のブロックを $C_1, C_2, ...$ とすると各ブロックの復号は $Dec(K, C_i) \oplus C_{i-1}$ となる。
  $Dec(K, C_i)$ は個別に計算可能であり、その結果の C_{i-1} との排他的論理和も個別に計算できる。よって並列化可能。

頑強性

問題

1. ChaCha20はIND-CCA2安全ではない理由を簡潔に延べよ。
2. CBCモードはIND-CCA2安全ではない理由を簡潔に延べよ。

解説と答え

- 1024bitの平文を暗号化した暗号文を考える。
  ChaCha20はストリーム暗号なので暗号文のビット反転が平文のビット反転に対応する。
  CBCモードはブロック暗号なので暗号文のビット反転は平文に複雑に影響する。
  ただ先頭ブロックのみ IV のビット反転が平文のビット反転に対応する。

1. ChaCha20の暗号文のi (1~1024) 番目のビットを反転させる。
   その暗号文を復号すると対応する平文のi番目のビットが反転している。

2. CBCモードのIVのi (1~128) 番目のビットを反転させる。
   その暗号文を復号すると対応する平文のi番目のビットが反転している。