

情報セキュリティ基礎 演習問題

光成滋生

last update: 2025/10/23

収束の定義

問題

- 実数 x に関する実数値関数 $f(x)$ が $x \rightarrow \infty$ で a に収束することを本来の収束の定義の ε と N の順序を入れ換えて
 $D': \exists N > 0 \text{ s.t. } \forall \varepsilon > 0, \forall x > N, |f(x) - a| < \varepsilon$
と定義すると収束の意味をなさないのはなぜか。

答え

- D' は「 $x > N$ 」ならどんなに「小さい $\varepsilon > 0$ 」であっても「 $|f(x) - a| < \varepsilon$ 」を要求する。
「 $f(x) \neq a$ となる $x > N$ 」が存在すると、これは成り立たないので
「 $x > N$ ならば $f(x) = a$ 」でなければならない。
これは x が大きいところで $f(x)$ が「定数関数」になっていることを要求し
扱いたい収束の概念とは異なる。

電話番号のハッシュ値

問題

- あるWebサービスが、ユーザの携帯電話の番号のSHA-1値をデータベースに保存していたが、ある日そのデータベースが漏洩した。
そのニュースを見たAは「SHA-1は安全じゃないからSHA-2を使うべきだった」と主張した。
- この主張の誤りの理由を述べよ。

答え

- 携帯番号のパターンは先頭は070, 080, 090で始まるもののみを考え全体で11桁の数値とすると最大「 $3 * 10^8$ 」通りである。
それらのパターン一つずつの「ハッシュ値」を求めてデータベースの値と一致するものを探索すれば元の携帯番号を復元できる。
仮に1秒間に1000万回探索できるなら $3 * 10^8 / 10000000 = 30$ 秒で全数探索できる。
ハッシュ関数をそのまま使う限り、安全な「SHA-2」で保存してもこの状況はほぼ変わらないから。

脆弱なHMAC

問題

- H をSHA-2としてMACを256bitの秘密鍵 s , メッセージ m に対して $MAC(s, m) = H(s||m)$ と作った。このMACはsEUF-CMA安全でないことを示す。

答え

- メッセージ m に対して $t = MAC(s, m)$ を取得したとする
 $pad(|x|)$ を x の長さにしか依存しないpaddingデータとする。
SHA-2はMerkle-Damgård構造なので別のメッセージ m' に対して
 $t' = H(s||m||pad(|s| + |m|)||m')$ を計算できる。
つまり、「 $m||pad(|s| + |m|)||m'$ 」に対するvalid MAC値な t' を構成できた。

2次拡大体

問題

- $K = (\mathbb{F}_2)^2$ の元 $x = (a, b), y = (c, d)$ に対して x と y の乗算を $xy = (ac, bd)$ と定義する。
このとき K は体にならないことを示せ。

答え

- $(1, 0) \times (0, 1) = (0, 0)$ となり $(1, 0)$ の逆元が存在しないから。

解説

- 一般に $ab = 0$ となる 0 でない元 $a, b \in K$ が存在すると体にはならない。
なぜなら a の逆元 a^{-1} が存在するなら、 $a^{-1}ab = b = 0$ となり矛盾するから。

8次拡大体

問題

- $K = \mathbb{F}_2[x]/(f(x))$ の多項式を $f(x) = x^8 + x + 1$ とすると拡大体とはならない。

答え

- $x^8 + x + 1$ を $x^2 + x + 1$ で割ると商が $x^6 + x^5 + x^3 + x^2 + 1$ で余りが 0 である。
つまり $x^8 + x + 1 = (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1)$ なので
 $x^8 + x + 1$ は既約ではなく $x^2 + x + 1$ の逆元が存在しないから。

多項式の除算の例

筆算でする

- 多項式の除算: 煩雑さを避けるため $x^8 + x + 1$ を $8 + 1 + 0$ などと表記する

$$\begin{array}{r} 6+5+3+2+1 \\ \hline 2+1+0 \) \ 8+1+0 \\ 8+7+6 \\ \hline 7+6+1+0 \\ 7+6+5 \\ \hline 5+1+0 \\ 5+4+3 \\ \hline 4+3+1+0 \\ 4+3+2 \\ \hline 2+1+0 \\ 2+1+0 \\ \hline 0 \end{array}$$