

情報セキュリティ基礎 演習問題

光成滋生

last update: 2026/1/7

HMAC-SHA3が使われない理由

適切な語句を入れよ。

- HMAC-SHA3が使われない理由を述べる。
SHA-2などの(A)は(B)を受けが、SHA-3は(C)であり(B)を受けない。
HMACはハッシュを(D)回することで(B)を防いでいるが、SHA-3では不要であるため。

答え

- (A) Merkle–Damgård構造
- (B) 伸長攻撃
- (C) スポンジ構造
- (D) 2

位数計算による素因数分解

適切な語句を入れよ。

- 素因数分解を位数計算に帰着する。
 $n = 2021027$ とする。
 $g = 2$ としたとき $g^r \equiv 1 \pmod{n}$ となる最小の r (位数) は(A)である。
- $a = g^{(r/2)} - 1 \pmod{n}$, $b = a + 2 \pmod{n}$
とする。
- このとき $g^r - 1 \equiv ab \pmod{n}$ であり、 a と n の最大公約数は(B)であり、 b と n の最大公約数は(C)である。
よって $n = pq$ ($p < q$) としたとき、 $p = (D)$, $q = (E)$ である。

答え

- (A) 72072, (B) 2003, (C) 1009, (D) 1009, (E) 2003

前問の計算方法

Pythonによるプログラム例

```
def gcd(a, b):  
    while b:  
        a, b = b, a % b  
    return a  
  
def find_order(g, n):  
    v = 1  
    for r in range(1, n):  
        v = (v * g) % n  
        if v == 1:  
            return r  
    raise Exception('not found')
```

```
n=2021027  
g=2  
r=find_order(g, n) # 72072  
a=pow(g, r//2, n)-1 # 943413  
b=a+2 # 943415  
gcd(a, n) # 2003  
gcd(b, n) # 1009
```

TLS 1.3

適切な語句を入れよ。

- TLS 1.3で公開鍵暗号化方式(Public Key Encryption)が使われなくなった理由を述べよ。
- (A)が漏洩したときに、盗聴されていた(B)が過去にさかのぼって(C)される危険性があるから。すなわち(D)を保つため。

答え

- (A) 秘密鍵
- (B) 暗号文
- (C) 復号
- (D) 前方秘匿性

ECDSA攻撃1

適切な語句を入れよ。

- ECDSAの署名は次のアルゴリズムで表される。
Hをハッシュ関数、Pを楕円曲線の位数 r の点、秘密鍵 s を固定する。
メッセージ m に対して $h=H(m)$ 。 k をランダムにとり、 t を kP の x 座標、 $\sigma=(t, u)=(t, (h+st)/k \bmod r)$ とする。
- 今、ある署名プログラムの k の選択が、ある初期時刻からの秒数の値を利用していたとする。ある時刻における m_1 の署名が $\sigma_1=(t_1, u_1)$ 、 a 秒後における m_2 の署名が $\sigma_2=(t_2, u_2)$ であった。このとき、署名鍵 s を求めよ。
- 解法: σ_1 、 σ_2 の生成時に使った k を k_1, k_2 , $h_1=H(m_1)$, $h_2=H(m_2)$ とすると $k_2 = (A)$ である。
- \mathbb{F}_r の中で (B) となる。よって k_1 と s に関する連立方程式 Q ができる。

$$\begin{cases} u_1 k_1 - t_1 s = h_1 \\ u_2 k_1 - t_2 s = h_2 - u_2 a \end{cases}$$

ECDSA攻撃1

続き

- 行列Aを

$$A = \begin{pmatrix} u_1 & -t_1 \\ u_2 & -t_2 \end{pmatrix}$$

とすると $\det A = (C)$ である。Aの逆行列を求めてQを解くと $s = (D)$ となる。

答え

- (A) $k_1 + a$
- (B) $u_1 = (h_1 + s t_1) / k_1, u_2 = (h_2 + s t_2) / k_2$
- (C) $u_1 * (-t_2) + t_1 * u_2$
- (D) $(1/\det A) * (-u_2 h_1 + u_1 * (h_2 - u_2 a))$

ECDSA攻撃2

記号はそちらを参照すること。

- ある時刻における $m1="Don't use AI."$ の署名が
 $\sigma1=(t1, u1)=$
(0x6d5db36d6b5c5e18cedcbd7165dcd5219d1b98646334c810103e714696185d4,
0xda87a6f4db00a9a69e726b782aa1098d028bd2476d427987d290a35fb9d142e8)
- 60秒後に生成された $m2="Solve it yourself."$ の署名が
 $\sigma2=(t2, u2)=(0x8fbc1bed0b1ffa5068b75144503fceb6047bca7fca10cc2629a6ea6e998c99db,$
0x1b31394d4b10d86770a01c92b9038fa6d2a916957ae134241f35aaab1a79cd6c)
であった。このとき、署名鍵 s を求めよ。
- ただし、楕円曲線とハッシュ関数はsecp256k1とSHA256を利用し、
 $r=0xfffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141$
 $h1=H(m1)=0x94cf850eb237e579a6336dcab8aeafccea7a7b3ef15cd283c691c3fb2dff4c4e$
 $h2=H(m2)=0x97c982f7320f4ff1402636575c354c452e729f4999381c9116b65c8c99e8f385$
とする。

ECDSA攻撃2

```
r=0xfffffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
a=60
h1=0x94cf850eb237e579a6336dcab8aeafccea7a7b3ef15cd283c691c3fb2dff4c4e
h2=0x97c982f7320f4ff1402636575c354c452e729f4999381c9116b65c8c99e8f385
t1=0x6d5db36d6b5c5e18cedcbd7165dcdf5219d1b98646334c810103e714696185d4
u1=0xda87a6f4db00a9a69e726b782aa1098d028bd2476d427987d290a35fb9d142e8
t2=0x8fbc1bed0b1ffa5068b75144503fceb6047bca7fca10cc2629a6ea6e998c99db
u2=0x1b31394d4b10d86770a01c92b9038fa6d2a916957ae134241f35aaab1a79cd6c
```

- Pythonで上記を入力し、 $\text{detA} = u1 * (-t2) + t1 * u2$ を計算すると、 $\text{detA}=(A)$ である。
 $1/\text{detA}=\text{invA}=\text{pow}(\text{detA}, -1, r)$ は $\text{invA}=(B)$ 、
 $s = (\text{invA} * (-u2 * h1 + u1 * (h2 - u2 * a)))\%r$ は $s=(C)$ となる。回答は全て10進数で入力せよ。

答え

- (A) 28846587240671913786089642235089787991894823479620465402632155360576814886916
- (B) 30934875024514956202678923428789566989154769627495250571062325542482402060672
- (C) 111601559888206902938973665514922793002413295977247509890789347730332982800612

Regev暗号

適切な語句を入れよ。

- 小さい（安全ではない）パラメータでRegev暗号の動作を確認する。
 $q=257, n=m=2$ とする。 x^T を x の転置とする。
秘密鍵を $s=(102\ 106)^T$, 行列を
 $A=\begin{pmatrix} 71 & 188 \\ 20 & 102 \end{pmatrix}$
ノイズを $e=(-1\ 0)^T$ とする。このとき公開鍵 $b = A s + e$ である。
- $M=1$ の暗号化は $r=(0\ 1)^T$ を乱数として $u = A^T r = (B)$
 $v = b^T r + (q//2)M = (C)$ として $\text{Enc}(M) = c = (u, v)$ である。
- 復号は $\text{Dec}(c) = v - s^T u = (D)$ この値は $q//2=(E)$ に近いので $\text{Dec}(c)=(F)$ となる。

答え

- (A) $(184\ 2)^T$, (B) $(20\ 102)^T$, (C) 130, (D) 128, (E) 128, (F) 1