Diszkrét Modellek Alkalmazásai

BEADANDÓ

50 pontos feladat

Rabin-féle Titkosítási és Aláírási Séma

Dokumentáció

Készítette:

Horánszki Patrik Donát

CJJ14N

Bevezetés

Ez a dokumentáció bemutatja a **Rabin-féle** titkosítási és aláírási séma működését, implementációját, valamint a módszerek matematikai hátterét. A Rabin-séma a négyzetgyök moduláris számításán alapuló aszimmetrikus kriptográfiai algoritmus, amelynek biztonsága az egész számok faktorizálásának nehézségén alapul.

Titkosítási Séma

Matematikai Háttere

A **Rabin-séma** a következő matematikai tulajdonságokon alapul:

1. Ha $\mathbf{n=p\times q}$, ahol **p, q** nagy prímek és $\mathbf{p\equiv q\equiv 3 \bmod 4}$, akkor bármely $\mathbf{c\in Z_n}$-hez pontosan négy négyzetgyök létezik **mod n**.
2. A négyzetgyökök kiszámítására a kínai maradéktételt (CRT) használjuk.

Algoritmus

1. **Kulcsgenerálás**:
   - Választunk két nagy prím számot **p** és **q**, ahol $\mathbf{p\equiv q\equiv 3 \bmod 4}$.
   - Kiszámoljuk: $\mathbf{n=p\times q}$.
   - A publikus kulcs **n**, a privát kulcs pedig **p, q.**
2. **Titkosítás**:
   - Az üzenet legyen **m**, ahol $\mathbf{0\le m<n}$.
   - Számítsuk ki a titkosított szöveget: $\mathbf{c = m^2 \bmod n}$
3. **Dekódolás**:
   - Számítsuk ki a **c**-hez tartozó 4 négyzetgyököt: *m1, m2, m3, m4*
   - Válasszuk ki a megfelelő üzenetet a négy négyzetgyök közül.

Implementáció

Az alábbi kód SageMath-ban valósítja meg a titkosítási sémát:

Kulcsgenerálás

```
def generate_key():
    p = next_prime(2^256 + randint(1, 2^256))
    q = next_prime(2^256 + randint(1, 2^256))
    while p % 4 != 3 or q % 4 != 3:
        p = next_prime(2^256 + randint(1, 2^256))
        q = next_prime(2^256 + randint(1, 2^256))
    n = p * q
    return p, q, n
```

Titkosítás

```
def encrypt(m, n):
    return (m^2) % n
```

Dekódolás

```
def decrypt(c,p,q):
    n = p * q
    # maradékok
    r1 = power_mod(c, (p+1) // 4, p)
    s1 = power_mod(c, (q+1) // 4, q)
    # kínai maradéktétel
    m1 = crt([r1,s1], [p,q])
    m2 = crt([r1,-s1], [p,q])
    m3 = crt([-r1,s1], [p,q])
    m4 = crt([-r1,-s1], [p,q])
    return m1, m2, m3, m4
```

Aláírási Séma

Matematikai Háttere

Az aláírási séma célja annak biztosítása, hogy az aláírás hitelesítse az üzenetet. A Rabin-aláírás **hash-függvényt** alkalmaz az üzenet rögzítésére, mielőtt az aláírást kiszámítanánk.

Algoritmus

1. **Kulcsgenerálás**:
   - Ugyanaz, mint a titkosítási séma esetében.
2. **Aláírás Generálása**:
   - Számítsuk ki az üzenet **hash** értékét: **h = H(m)**.
   - Számítsuk ki a hash négyzetgyökét mod p és q:
     $\mathbf{s = h^{(p+1)/4} \bmod p, \quad t = h^{(q+1)/4} \bmod q}$
   - Használjuk a **Kínai-maradéktételt** az aláírás előállítására.
3. **Aláírás Ellenőrzése**:
   - Ellenőrizzük, hogy az aláírás négyzete *mod n* megegyezik-e a hash-sel.

Implementáció

Az alábbi kód SageMath-ban valósítja meg az aláírási sémát:

Dekódolás

```
def sign(m, p, q):
    h = Integer(hash(m))
    # maradékok
    s = power_mod(h, (p+1) // 4, p)
    t = power_mod(h, (q+1) // 4, q)
    # kínai maradéktétel
    return crt([s,t], [p,q])
```

Aláírás ellenőrzése

```
def verify(signature, m, n):
    h = Integer(hash(m))
    return (signature^2) % n == h
```

Példa

1. **Kulcsgenerálás**:
```
p, q, n = generate_key()
print(f"p = {p}, q = {q}, n = {n}")
```
2. **Titkosítás és dekódolás**:
```
message = 7
print(f"Titkosítandó üzenet: {message}")
c = encrypt(message, n)
print(f"Titkosított üzenet: c = {c}")

m1, m2, m3, m4 = decrypt(c,p,q)
print(f"Lehetséges megoldások: {m1}, {m2}, {m3}, {m4}")
```
3. **Aláírás és ellenőrzés**:
```
signature = sign(message, p, q)
print(f"Aláírás: {signature}")

is_valid = verify(signature, message, n)
print(f"Aláírás érvényessége: {is_valid}")
```
4. **Lehetséges eredmény:**

```
p = 201312570100787700867945543706387488673361107400542726299479979464573533699031, q =
146381289883102974045497440862845889434260412151079478742677868553057383143063, n =
29468393681035892937144592601760035018525636224473825400860557572830187760565644451452348477900332772363653926963048776989781878793780806696677947457471953
Titkosítandó üzenet: 7
Titkosított üzenet: c = 49
Lehetséges megoldások: 7,
15896526072304228322228148923089993380411866042727079737392047767442265717223201548747660405355730085889537935642286407236051077883230515362124534194578487
,
13571867608731664614916443678670041638113770181746745663468509805387922043342442902704688072544602686474115991320762369753730800910550291334553413262893466
,
29468393681035892937144592601760035018525636224473825400860557572830187760565644451452348477900332772363653926963048776989781878793780806696677947457471946
Aláírás:
12894901096936819613152669056589544779339895534957929301605669836621034823666247519639104045428517843246048793432559778743846030497273490586719210222106371
Aláírás érvényessége: True
```