Aszimmetrikus titkosítás

RSA algoritmus

Mi kell hozzá?

- Két fél
- Két privát/publikus kulcspár
- Üzenet

Privát/publikus kulcspár

- Privát kulcs:
  - **N** modulus
  - **d** privát kitevő
  - Ezt nem osztjuk meg másokkal
- Publikus kulcs:
  - **N** modulus
  - **e** nyilvános kitevő
  - Ezt osztjuk meg másokkal

RSA algoritmus

Ron Rivest, Adi **S**hamir és Len **A**dleman

1. Vegyünk két tetszőleges prímszámot:
   a. **p** = 2
   b. **q** = 7
2. Legyen **N** = **p** * **q**
   a. **N** = 2 * 7 = 14
3. Legyen **φ(N)** = **N** relatív prímjeinek a száma (**φ** - az Euler függvény)
   a. **φ(N)** = (**p** - 1) * (**q** - 1) = (2 - 1) * (7 - 1) = 6 (mivel **p** és **q** prímszámok)

RSA algoritmus folyt.

1. Legyen **e** az a szám amely kielégíti az alábbi feltételeket:
    a. $1 < e < \varphi(N)$
    b. **e** relatív prím **φ(N)** - el (φ(N) = 6)
    c. Lehetséges **e** értékek
        i. 2 -> kizárva, hiszen LNKO (2, 6) = 2
        ii. 3 -> kizárva, hiszen LNKO (3, 6) = 3
        iii. 4 -> kizárva, hiszen LNKO (4, 6) = 2
        iv. 5 -> Teljesíti a feltételeket
2. Az **e** kitevő és az **N** modulus fogja alkotni a publikus kulcsot

RSA algoritmus folyt.

1. Legyen **d** az a szám amely kielégíti az alábbi feltételt:
   a. **d** * **e** (mod **φ(N)**) ≡ 1
   b. Lehetséges **d** értékek
      i. 1: 1 * 5 (mod 6) ≡ 5 (mod 6) ≡ 5 (mod 6), nem jó
      ii. 2: 2 * 5 (mod 6) ≡ 10 (mod 6) ≡ 4 (mod 6), nem jó
      iii. 3: 3 * 5 (mod 6) ≡ 15 (mod 6) ≡ 3 (mod 6), nem jó
      iv. 4: 4 * 5 (mod 6) ≡ 20 (mod 6) ≡ 2 (mod 6), nem jó
      v. 5: 5 * 5 (mod 6) ≡ 25 (mod 6) ≡ 1 (mod 6), ez már jó lehet
      vi. …
      vii. 11: 11 * 5 (mod 6) ≡ 55 (mod 6) ≡ 1 (mod 6), ez már jó lehet, válasszuk ezt
2. Az **d** kitevő és az **N** modulus fogja alkotni a privát kulcsot

Üzenet

- Legyen a kódolandó szöveg: “FBI”
- Mivel ezek karakterek, az egyszerűség kedvéért az üzenet tartalma legyen a karakterek angol ábécében elfoglalt helye
    - F -> 6
    - B -> 2
    - I -> 9
- Tehát az üzenet amit küldeni akarunk: “6 2 9”

Kódolás

- A kulcs (**e**) és modulus (**N**) párt a publikus kulcsból kapjuk
- Kódolt üzenet: Számítsuk ki az üzenet minden karakterére (**m**) a következő értéket
  - **c** = **m** ^ **e** (mod **N**)
- **Példa**
  - kulcs: 5
  - modulus: 14
  - Üzenet: “6 2 9” (“FBI”)
    - 6 ^ 5 (mod 14) ≡ 7776 (mod 14) ≡ 6 (mod 14) -> 6 (“F”)
    - 2 ^ 5 (mod 14) ≡ 32 (mod 14) ≡ 4 (mod 14) -> 4 (“D”)
    - 9 ^ 5 (mod 1 4) ≡ 59049 (mod 14) ≡ 11 (mod 14) -> 11 (“K”)
  - A kapott titkosított üzenet: “6 4 11” (“FDK”)

Dekódolás

- A kulcs (**d**) és modulus (**N**) párt a privát kulcsból kapjuk
- Kódolt üzenet: Számítsuk ki a titkosított üzenet minden karakterére (**c**) a következő értéket
  - **m** = **c** ^ **d** (mod **N**)
- **Példa:**
  - kulcs: 11
  - modulus: 14
  - Titkosított üzenet: “6 4 11” (“FDK”)
    - 6 ^ 11 (mod 14) ≡ 362797056 (mod 14) ≡ 6 (mod 14) -> 6 (“F”)
    - 4 ^ 11 (mod 14) ≡ 4194304 (mod 14) ≡ 2 (mod 14) -> 2 (“B”)
    - 11 ^ 11 (mod 1 4) ≡ 285311670611 (mod 14) ≡9 (mod 14) -> 9 (“I”)
  - A kapott üzenet: “6 2 9” (“FBI”)