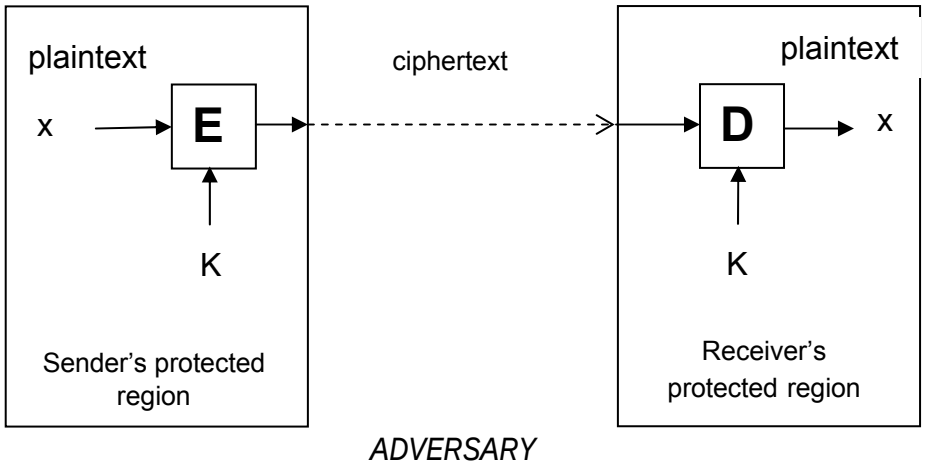
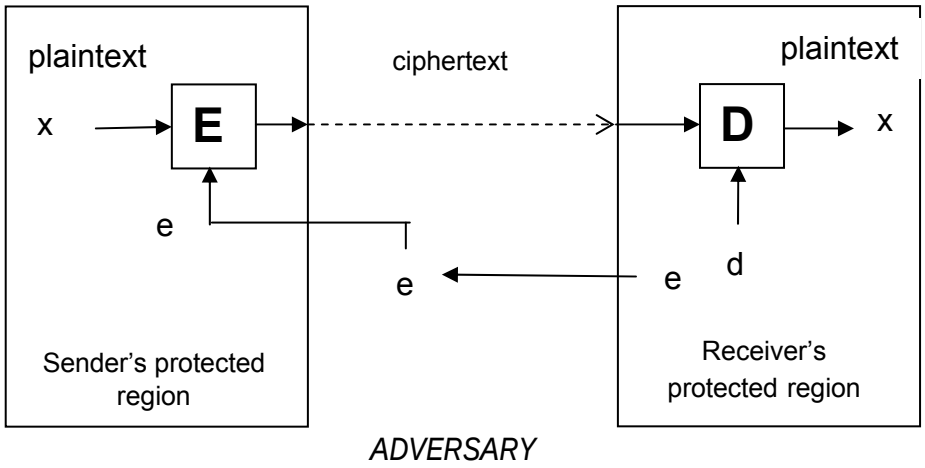
Data Security: Public key

- Nyilvános kulcsú rejtjelezés
- RSA rejtjelező
- El-Gamal rejtjelező

Data Security: Encryption



Szimmetrikus kulcsú rejtjelezés



Publikus kulcsú rejtjelezés

Data Security: Public key

RSA (Tk.3.1-3.fejezetek)

1. Véletlenszerűen választunk két "nagy" prímszámot: p1, p2

2. m= p1p2 $\phi(m) = (p_1 - 1)(p_2 - 1)$

e, $1 \le e < \phi(m)$ $(\phi(m), e) = 1$

3. $d = e^{-1} \pmod{\phi(m)}$

4. $k^p = (m, e)$ $k^s = (d, p_1, p_2)$

Kódolás: $y = x^e \pmod{m}$ $1 \le x < m$

Dekódolás: $x = y^d \pmod{m}$ $1 \le y < m$

Data Security: Public key

RSA

Diszkrét matematika előismeretek

Maradékos osztás tétele: *Tetszőleges a és b, a > 0, b > 0 egészekre egyértelműen létezik q és r egész, hogy* $a = b\,q + r$ *, ahol* $0 \leq r < b$, $q \geq 0$.

Euklideszi l.n.k.o. algoritmus

l.n.k.o. algoritmus következménye: Tetszőleges *b* és *c* egészekre, amelyek közül legalább egyik nem nulla, léteznek *s* és *t* egészek, hogy $(b, c) = s\,b + t\,c$

Inverz modulo m: *A b szám modulo m inverze akkor és csak akkor létezik, ha (b, m) = 1. Ha létezik inverz, akkor az egyértelmű az m-nél kisebb pozitív egészek között.*

Fermat tétel: *Ha a c egész nem osztható a p primmel, akkor* $c^{p-1} = 1 \pmod{p}$

Fermat-tétel általánosítása: *Ha p1 és p2 különböző primek, és az c egészre teljesül, hogy* $(c, p_1p_2) = 1$, *akkor* $c^{(p1-1)(p2-1)} = 1 \pmod{p_1p_2}$.

Kínai maradékok tétele: Ha az az $m_1, m_2, \ldots m_r$ pozitív egészek páronként relatív prímek, és $a_1, a_2, \ldots, a_r$ tetszőleges egész számok, akkor az $x = a_i \pmod{m_i}$, $i = 1, \ldots r$, rendszernek van közös megoldása. Bármely két megoldás azonos modulo $m_1, m_2, \ldots, m_r$.

Data Security: Public key

RSA

Játék RSA algoritmus:

p1=7, p2=11

m=77, $\varphi(m)=6*10=60=2*3*5$

e=7

$$d = 7^{-1} \bmod 60$$

Euklideszi algoritmus alkalmazása:

60=8*7+4 1*60-8*7=4

7=1*4+3 7=60-8*7+3

4=1*3+1 -60+9*7=3

3=3*1+0 60-8*7=-60+9*3+1

2*60-17*7=1 ---> (-17)*7=1 (mod 60) ---> d= $7^{-1} = -17 = 43 \ (60)$

Data Security: Public key

RSA

"Ismételt négyzetre emelés és szorzás" algoritmus

Miért előnyös az e=3 vagy általában $e=2^t+1$ alakú választás?

$e=2^t+1$: 1 db (moduláris) szorzás és t db négyzetre emelés,
összes szorzási műveletek száma: t+1

Pl.
e=3: 1 szorzás és 1 négyzetre emelés,

$e=2^{16}+1$: 1 szorzás és 16 négyzetre emelés.

Data Security: Public key

RSA

Primszámkeresés

Mekkora annak P valószínűsége, hogy egy véletlenszerűen választott m bit hosszú n egész ($2^{m-1} < n < 2^m$) prímszám?

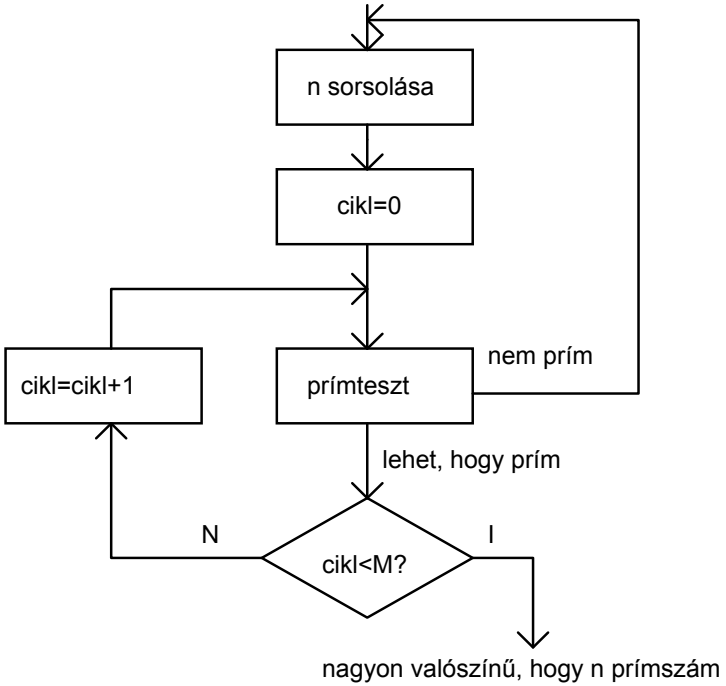
Csebisev számelméleti tétele: $\Pi(n)$ az n pozitív egésznél kisebb primek számának nagyságrendje:

$$\prod(n) \cong \frac{n}{\ln n}$$

$$P = \frac{\prod(2^m) - \prod(2^{m-1})}{2^m - 2^{m-1}} \cong \frac{2^{m-1}\dfrac{1}{(m-1)\cdot \ln 2}}{2^{m-1}} \cong \frac{1}{(m-1)\ln(2)}$$

Data Security: Public key

RSA



Fermat-teszt: Egy n összetett szám álprím egy b bázisra nézve, ha

$b^{n-1} = 1 \pmod{n}$

ahol $b \in Z_n$, $Z_n = \{z : 1 < z < n \text{ és } (z, n) = 1\}$.

Miller-Rabin teszt: Véletlenszerűen választunk egy *b* bázist

n prímgyanús , ha $b \in R_n$,

n összetett, ha $b \in R_n$

ahol R_n azon $b \in Z_n$ számok halmaza, amelyekre vagy

$b^u = 1 \pmod{n}$, $n - 1 = 2^v u$, *u* páratlan

vagy létezik olyan $0 \leq j < v$, melyre

$$b^{2^j u} = -1 (\mathrm{mod}\, n)$$

Data Security: Public key

RSA

$b^{n-1} = 1 \pmod{n}$

Fermat álprím-e 33 a b=2 bázisra nézve?

Nem: $2^{32}=4\cdot(2^5)^6=4\cdot(32)^6=4\cdot(-1)^6=4\neq 1 \bmod 33$

Fermat álprím-e p-1 a b=p-2 bázisra nézve, ahol p prim, p>3?

Nem. $(p-2)^{p-2} = (-1)^{p-2} = -1 \ (\neq 1) \pmod{p-1}$, (p-2 páratlan).

Data Security: Public key

RSA

Fermat-faktorizáció: $n = ab$, $a,b > 0$.

Legyen $t = (a + b) / 2$, $s = (a - b) / 2 \rightarrow a = t+s$, $b = t-s$.

$\rightarrow$ $n = t^2 - s^2 = (t+s)(t-s)$

Ötlet: ha a-b különbség "kicsi", akkor s is "kicsi " $\rightarrow$ $t \approx n^{1/2}$.

Találgatás t-re : $t_1 = \text{int}(n^{1/2})+1$, $t_2 = \text{int}(n^{1/2})+2$, ...

Ellenőrzés: t_i^2-n négyzetszám?

Ha igen, akkor $t_i^2 - n = s^2 \rightarrow t$, $s \rightarrow a$, b.

Példa: n=14803 ; int(n$^{1/2}$)+1=122 $\rightarrow$ 122^2-n=81=9^2,
a=122+9=131, b=122-9=113.

Data Security: Public key

RSA

Kicsi kódoló kulcsok problémája

$$y_1 = x^e \pmod{m_1}$$
$$y_2 = x^e \pmod{m_2}$$
$$\dots$$
$$y_r = x^e \pmod{m_r} \qquad r \geq e$$

Ha $m_1, m_2, \dots, m_r$

modulusok páronként relatív prímek, a kínai maradékok tétele alkalmazható

$\rightarrow$ hatékonyan kiszámíthatjuk $z=x^e$ hatványt,

$$x < \min\{m_i\} \quad \rightarrow \quad 0 < x^e < m_1 m_2 \cdots m_r$$

z egész szám e-edik gyökét kiszámítva x nyílt szöveget megkapjuk!

(Tk.3.1-20. feladatok)

Data Security: Public key

ElGamal

El-Gamal rejtjelező

G: multiplikativ csoport g generátor elemmel

Kulcspár: pk=X, sk=x,
ahol $X=g^x$, x véletlen elem S={1,2,…,|G|} halmazból

Rejtjelezés:
$m \in S$
$E_{pk}(m)=(Y,b)$,
ahol $Y=g^y$, y véletlen elem S halmazból
$b=Km$, $K=X^y$

Dekódolás:
(Y,b) rejtett szöveg
$D_{sk}(Y,b)=m$, $K=Y^x$,m=b/K,