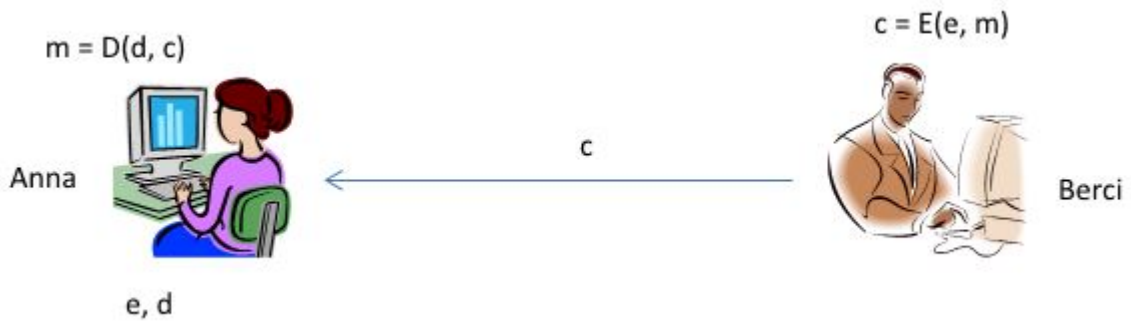
Nyilvános kulcsú rendszerek



A kommunikáció alapmodellje:

1. Anna készít egy **e,d** kulcspárt.
2. **d**-t titokban tartja, **e**-t nyilvánosságra hozza.
3. Ha Berci üzenni akar Annának, akkor Anna (**e**) nyilvános kulcsát használja.
4. **c=E(e , m)** alapján **c**-t csak Anna tudja visszafejteni, **m = D(d,c)** alkalmazásával.
5. Ha más is üzenni kíván Annának, akkor használhatja az ő nyilvános (**e**) kulcsát.

A rendszer biztonságos a visszafejtés szempontjából, de Anna soha sem lehet biztos, hogy Berci küldte az üzenetet, hiszen a nyilvános (e) kulcsot bárki használhatja.

RSA algoritmus

Rivest, Shanir, Adleman (1977), az algoritmus a hatványozáson és a moduló (maradékos osztás) műveleten alapul. Ha következő egyenlet teljesül:

$$ T ^ {ed} \mod{N} = T $$

Akkor az egyenletet szét lehet választani két részre, ahol az első egyenlet kódol, a második dekódol:

$$ T ^{e} \mod{N} = C $$ $$ C ^{d} \mod{N} = T $$

Sajnos ez az összefüggés, nem fog működni tetszőleges e, d, N számhármasokra. Próbáljuk meghatározni milyen feltételek szükségesek?

Alaptétel

Akármennyire hihetetlen, de a következő összefüggést még az ókori görögök is ismerték:

\(T^{N-1} \mod {N} = 1 \) egyenlet egész számokra abban az esetben teljesül, ha \(N > T \) és \(N \) prímszám.

megjegyzés: prímek azok a pozitív egész számok, amelyeknek nincsen (1-nél különböző) egész osztójuk, pl. 1, 2, 3, 5, 7, 11, 13, 19, stb...

Az alapötlet szerint az egyenlet ekvivalens átalakításokkal a fenti alakra hozható a következőképpen:

Az \(f(N)\) jelölje azt, hogy \(N\)-nek hány relatív prímje van. pl: \(f(9) = 6 \) mivel 9 relatív prímjei sorban a (1,2,4,5,7,8), a 6 nem az, mert a 3 többszöröse.

Érdekes megfigyelni, hogy prímszámok esetén nem kell számolnunk, pl: \(f(11) = 10 \), mivel (1,2,3,4,5,6,7,8,9,10) nem lesz olyan nála kisebb szám ami osztója, mivel 11 prím szám!

Ezért felírható az általános: \(f(N) + 1 = N \) összefüggés. Tehát:

$$ T ^{f(N)} \mod{N} = 1, $$

mivel \(N - 1 = f(N) \) összefüggés behelyettesíthető. Ha a hatványozás kitevőjét beszorozzuk egy konstanssal, akkor a moduló művelet nem változik, a maradék akkor is ugyanannyi lesz:

$$ T ^{K\cdot f(N)} \mod{N} = 1. $$

Ez a lépés biztosítja, hogy végtelen kulcs lehet, mivel “bármilyen” K-t alkalmazhatunk (K tetszőleges egész szám). Most pedig szorozzuk be T-vel mindkét oldalt:

$$ T ^{K\cdot f(N) + 1} \mod{N} = T. $$

ha K-t úgy választjuk meg, hogy a \(K \cdot f(N) + 1\) felbontható legyen két egész szám szorzatára, akkor megkapjuk e, d kulcsokat. Hogy ne kelljen próbálgatni, ezért egy egzakt módszer is létezik, amit majd később részletezünk.