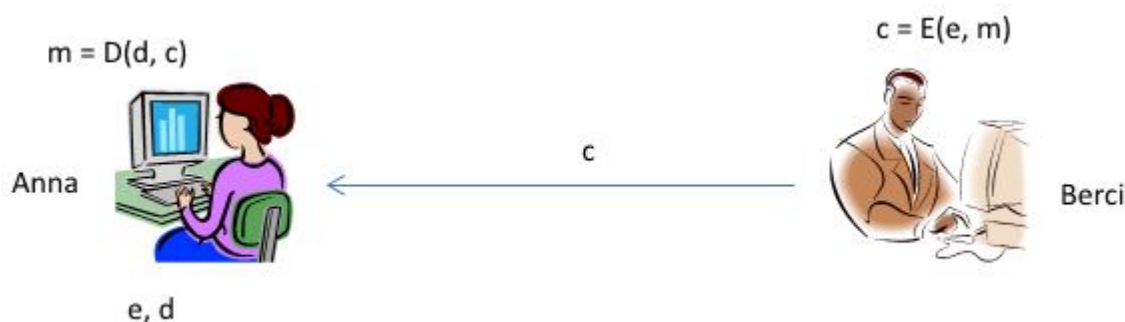


## Nyilvános kulcsú rendszerek



A kommunikáció alapmodellje:

1. Anna készít egy **e, d** kulcspárt.
2. **d**-t titokban tartja, **e**-t nyilvánosságra hozza.
3. Ha Berci üzeni 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 üzeni 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, Shamir, Adleman (1977), az algoritmus a hatványozáson és a moduló (maradékos osztás) műveleten alapul. Ha következő egyenlet teljesül:

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

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

$$T^e \bmod N = C \quad C^d \bmod N = T$$

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

### Alaptétel

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

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

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

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

Az  $\phi(N)$  jelölje azt, hogy  $N$ -nek hány relatív prímje van. pl:  $\phi(9) = 6$  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:  $\phi(11) = 10$ , 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:  $\phi(N) + 1 = N$  összefüggés. Tehát:

$$T^{\phi(N)} \pmod{N} = 1,$$

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

$$T^{K \cdot \phi(N)} \pmod{N} = 1.$$

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:

$$T^{K \cdot \phi(N) + 1} \pmod{N} = T.$$

ha  $K$ -t úgy választjuk meg, hogy a  $(K \cdot \phi(N) + 1)$  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.

## RSA kulcsgenerálás

A kulcsgenerálás a következőképpen történik:

1. keresünk két nagy prímszámot:  $X$  és  $Y$
2. ezek szorzata lesz:  $(N = X \cdot Y)$
3. mindkét számnak ismerjük, hogy hány relatív prímje van:  $(\phi(X) = X - 1, \phi(Y) = Y - 1)$  és ez alapján  $\phi(N)$  könnyen számolható:  $\phi(N) = (X-1) \cdot (Y-1)$
4. felbontjuk  $(K \cdot \phi(N) + 1)$  összefüggést két egész szám szorzatára.  $(K \cdot \phi(N) + 1 = e \cdot d)$  felbontást a gyakorlatban a következő képlettel számoljuk:  $\text{lnc}(e, \phi(N)) = 1$  egyenletből az  $e$ -t, majd a  $d$ -t a  $(1 < d < \phi(N))$  feltétel figyelembe vételével az  $(e \cdot d \pmod{\phi(N)} = 1)$  egyenlet megoldásával nyerjük.
5. nyilvános kulcs  $(e, N)$ , titkos kulcs  $(d, N)$

## Példa a kulcsgenerálásra

Anna választ 2 prímszámot, például legyenek:  $(p=67)$  és  $(q=11)$  a két választott prím.

1.)  $(N = p \cdot q = 67 \cdot 11 = 737)$

2.) A relatív prímek száma:  $(\phi(N) = (p-1) \cdot (q-1) = 66 \cdot 10 = 660)$

3.) Válasszunk egy  $(e)$  számot amelyre igaz:  $(1 < e < \phi(N))$  és  $(\text{lnc}(e, \phi(N)) = 1)$   $(\phi(N) = 660)$ -hoz a legkisebb ilyen kitevő  $(e = 7)$

From:  
<https://edu.iit.uni-miskolc.hu/> - Institute of Information Science - University of Miskolc

Permanent link:  
[https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai\\_architekturak:informacio\\_titkositas\\_es\\_hitelesites:nyilvanos\\_kulcsu\\_rendszerek?rev=1731520425](https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai_architekturak:informacio_titkositas_es_hitelesites:nyilvanos_kulcsu_rendszerek?rev=1731520425)

Last update: 2024/11/13 17:53

