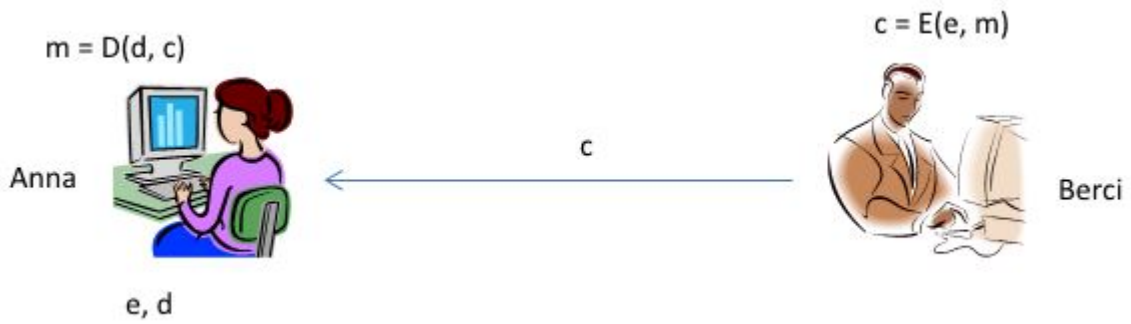
# Nyilvános kulcsú rendszerek




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.

## 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: \( f(X) = X - 1,\,\, f(Y) = Y - 1 \) és ez alapján \( f(N) \) könnyen számolható: \( f(N) = (X-1) \cdot (Y-1) \)
4. felbontjuk \( K \cdot f(N) + 1 \) összefüggést két egész szám szorzatára. \( K \cdot f(N) + 1 = e \cdot d \) felbontást a gyakorlatban a következő képlettel számoljuk: $$ \text{lnko} (e, f(N)) = 1 $$ egyenletből az e-t, majd a d-t a \( 1<d<f(N) \) feltétel figyelembe vételével az \( e \cdot d \mod{f(N)} =1 \) egyenlet megoldásával nyerjük.
5. nyilvános kulcs **(e,N)**, titkos kulcs **d**

## 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: \( φ(N) = (p-1) \cdot (q-1) = 66 \cdot 10 = 660 \)

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

4.) Anna nyilvános kulcsa tehát ezek alapján: \( (N,e) = (737,7) \)

A következő 5. lépés többféleképpen is megoldható:

5a.) $K \cdot \varphi(N) + 1$ felbontható két szám szorzatára (miből a $e=7$ az egyik): tehát keressük azt a legkisebb $K$-t amelyre igaz: $K \cdot 660 + 1 \mod{7} = 0$. A legkisebb ilyen a $K=3$. Ebből következik, hogy $(3*660+1) / 7 = 283$.

5b.) $e \cdot d \mod {f(N)} = 1$, egyenletből $d$ kifejezhető. $d = 283$

6.) A titkos kulcs $(N,d) = (737,283)$ lesz.

7.) Az ABC 26 karaktert tartalmaz tehát $I = log_{26} N = log_{26} 737 = 2$. Tehát a blokkhossz most 2-byte lesz.

8.) A kódolandó üzenetet 2 bájtonként tördeljük, és 26-os számrendszerbe átalakítjuk. Pl. Ha a kódolandó üzenet ‘A’ és ‘B’, akkor $1*26^1+2*26^0=26+2=28$.

9.) $28^7 \mod{737} = 316$. ez felírva 26-os számrendszerbe: $12*26^1+4*26^0$ –> A kódolt szöveg: $LD$ lett.

10.) Visszafejtés: $LD$ átalakítva számmá: 316

11.) $316^{283} \mod{737} = 28$ → Betűkre átalakítva: $AB$