RSA feltörése

Az RSA algoritmus gyenge pontja a kulcsgenerálás: N-et fel kell bontani prímtényezőire, ami csak próbálgatással lehetséges. Az algoritmus addig lesz uralkodó, ameddig ez valakinek nem sikerül valamilyen heurisztikus módszerrel.

Nem is hinnénk el, ha például $N=77$ esetén mennyi p és q? Ha kitaláltuk akkor gondoljuk arra mi is volt az algoritmus??? Hogyan találtuk ki?

A 2048 bites számok prímtényezőkre bontásáért az RSA Labs 200000$-t fizetett korábban. Eltávolították a díjat, mert újabb kutatások szerint, ha az p és q prímek speciális viszonyban vannak egymással, akkor a módszer törhető.

Az RSA Labs százezer dolláros pénznyereményt ajánlott annak, aki elküldi az alábbi (N) egész szám prímtényezőit, azaz jelen esetben azt a két prímet, amely szorzata N:

```
N = p * q = 25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357
```

Érezzük, hogy ez nem könnyű feladat: 617 számjegyet látunk és sajnos nem páros az utolsó számjegye sem.