

## Factorisation d'un nombre de 768 bits

Écrit par Administrator

Jeudi, 07 Janvier 2010 19:39 - Mis à jour Samedi, 09 Janvier 2010 15:49

---

Un groupe de chercheurs (voir la liste à la fin de l'article) vient de donner la factorisation du challenge RSA 768. Voici un extrait de leur courrier:

*"We are pleased to announce the factorization of RSA768, the following 768-bit, 232-digit number from RSA's challenge list:*

```
1 2 3 0 1 8 6 6 8 4 5 3 0 1 1 7 7 5 5 1 3 0 4 9 4 9 5 8 3 8 4 9 6 2 7 2 0 7 7 2 8 5 3 5 6 9 5 9 5 3 3
4 7 9 2 1 9 7 3 2                                     2 4
5 2 1 5 1 7 2 6 4 0 0 5 0 7 2 6 3 6
5 7 5 1 8 7 4 5 2 0 2 1 9 9 7 8 6 4 6 9
3 8 9 9 5 6 4 7 4 9 4 2 7 7 4 0 6 3 8 4
5 9 2 5 1 9 2 5 5 7 3 2 6 3 0 3 4 5 3 7
3 1 5 4 8 2 6 8 5 0 7 9 1 7 0 2 6 1 2 2
1 4 2 9 1 3 4 6 1 6 7 0 4 2 9 2 1 4 3 1
1 6 0 2 2 2 1 2 4 0 4 7 9 2 7 4 7 3 7
7 9 4 0 8 0 6 6 5 3 5 1 4 1 9 5 9 7 4
5 9 8 5 6 9 0 2 1 4 3 4 1 3.
```

*The factorization, found using the Number Field Sieve (NFS), is:*

```
3 3 4 7 8 0 7 1 6 9 8 9 5 6 8 9 8 7 8 6 0 4 4 1 6 9 8 4 8 2 1 2 6 9 0 8 1 7 7 0 4 7 9 4 9 8 3 7 1 3
7 6 8 5 6 8 9 1 2 4 3 1 3 8 8 9 8 2 8 8 3 7 9 3 8 7 8 0 0 2 2 8 7 6 1 4 7 1 1 6 5 2 5 3 1 7 4 3 0 8 7
7 3 7 8 1 4 4 6 7 9 9 9 4 8 9
```

\*

```
3 6 7 4 6 0 4 3 6 6 6 7 9 9 5 9 0 4 2 8 2 4 4 6 3 3 7 9 9 6 2 7 9 5 2 6 3 2 2 7 9 1 5 8 1 6 4 3 4 3
0 8 7 6 4 2 6 7 6 0 3 2 2 8 3 8 1 5 7 3 9 6 6 6 5 1 1 2 7 9 2 3 3 3 7 3 4 1 7 1 4 3 3 9 6 8 1 0 2 7 0
```

## Factorisation d'un nombre de 768 bits

Écrit par Administrator

Jeudi, 07 Janvier 2010 19:39 - Mis à jour Samedi, 09 Janvier 2010 15:49

---

0 9 2 7 9 8 7 3 6 3 0 8 9 1 7

*Both factors have 384 bits and 116 digits. Referring to the smallest one as  $p$  and its cofactor as  $q$ , we have the following prime factorizations:*

$$p-1 = 2^8 \cdot 11^2 \cdot 13 \cdot 7193 \cdot 160378082551 \cdot 7721565388263419219 \cdot 111103163449484882484711393053 \cdot p_{47}$$

$$p+1 = 2 \cdot 3 \cdot 5 \cdot 31932122749553372262005491861630345183416467 \cdot p_{71}$$

$$q-1 = 2^2 \cdot 359 \cdot p_{113}$$

$$q+1 = 2 \cdot 3 \cdot 23 \cdot 41 \cdot 47 \cdot 239875144072757917901 \cdot p_{90}$$

*where  $p_k$  denotes a  $k$ -digit prime number.*

*A paper describing the details of this factorization effort can be found on*

<http://eprint.iacr.org/2010/006.pdf>

*and on*

<http://lcal.epfl.ch/> ".

## Factorisation d'un nombre de 768 bits

Écrit par Administrator

Jeudi, 07 Janvier 2010 19:39 - Mis à jour Samedi, 09 Janvier 2010 15:49

---

Le groupe des chercheurs ayant mené à bien ce projet est :

Thorsten Kleinjung (1),  
Kazumaro Aoki (2), Jens Franke (3), Arjen K. Lenstra (1), Emmanuel Thomé (4),  
Joppe W. Bos (1), Pierrick Gaudry (4), Alexander Kruppa (4),  
Peter L. Montgomery (5,6), Dag Arne Osvik (1), Herman te Riele (6),  
Andrey Timofeev (6), and Paul Zimmermann (4)

1: EPFL; 2: NTT; 3: Bonn University; 4: INRIA; 5: MS Research; 6: CWI

Je ne sais pas si la carte bancaire française a évolué récemment, mais il y a peu de temps, la partie de la carte bancaire qui assure la vérification de la carte lorsque que le lecteur n'est pas connecté à la banque reposait sur une signature RSA avec ombre de module 768 bits. Si c'était encore le cas, cette fonctionnalité serait de nouveau potentiellement cassée.