MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Partial Key Exposure with RSA – Part 1

Authors: H. Koy, B. Esslinger

January 2012

Partial Key Exposure for RSA with small public keys

With RSA keys, the private key d must remain private. If the public key e is very small, this is not completely possible. This exercise demonstrates how simple it is to compute a portion of the secret key d.

The public RSA key is given with the values:

N = 11748548000338754589 63418513294678146058405488725863843375871404053126501231188039037392429359891331770972611779623223580027156770296714854670114368829712639631427476148558403850135873110695364675608065410578217307353652601503494635208001251653315107517135401568563445428649384660529005472383693253461320790 99

and e = 3.

For the private key d it is: e*d = 1 mod phi(N), where phi(N) is the Euler number from N, and phi(N) here is unknown.

Task:
Find the integer value d' that approximates d for at least 510 bits.
Please send us the complete d' in binary format.
Your solution will be accepted if the first 510 bits are correct.

Hints

- The factor N is the product of the two 512 bit prime numbers p and q.
- The Euler number phi(N) can be approximated with N.
- Given d*e = 1 mod phi(N) $\Leftrightarrow$There is a whole number s with d*e = 1 + s*phi(N).
  Consider which value s can have when e = 3.
- When phi(N) has been approximated, how well can the private key d be approximated when e = 3 (number of corresponding bits)?
- There are two possible solutions for d' – we are searching for the greater number.

Note

Sometimes, a partial compromise of the private key is sufficient to break an RSA key completely. Relevant publications can be found with the phrase “Partial Key Exposure Attack.” For the parameter set shown above, however, there is no known key exposure attack yet.
Please let us know if you find an algorithm that realizes this attack for the parameters used in this challenge.