MysteryTwister C3

A CRYPTO CHALLENGE BY CRYPTOOL

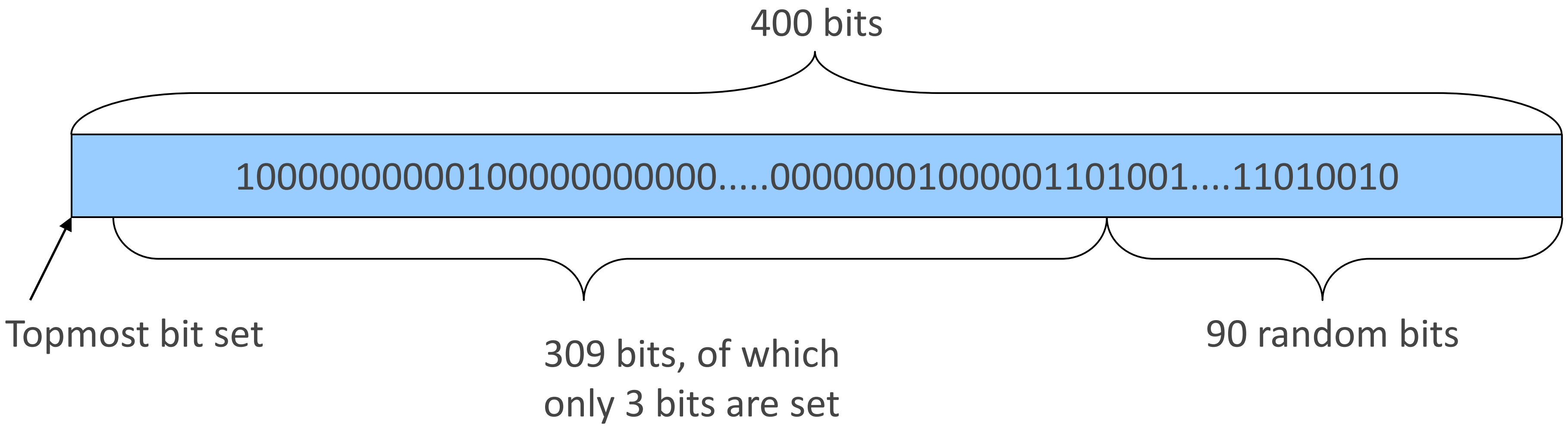
Finding Special Private RSA Keys

Level III Challenge

Special Private RSA Keys

- Using small keys improves performance.
- However, it has been shown (Wiener, 1990) that if $d<=0.25 \log(N)$, the private exponent d can be reconstructed from the public key (N,e).
- Smart, Inc. uses special private keys designed such that they are:
    - Larger than the minimum bound recommended by Wiener, and
    - Still very efficient because of their low Hamming weight.

Structure of the keys



400 bits

10000000000100000000000.....00000001000001101001....11010010

Topmost bit set

309 bits, of which
only 3 bits are set

90 random bits

Challenge

- Are the keys safe to use ?
- Try to reconstruct the private key that corresponds to the public key given on the website.