MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Summer Job

Author: Matthias Minihold, ECRYPT-NET

February 2018

Introduction (1/2)

A summer job in an Austrian weekly magazine is typically not too exciting. Assisting journalists, fetching coffee – but one day was different. A mysterious letter arrived. While puzzled colleagues stared at the numbers, unintelligible gibberish to them, you, a hobby cryptographer, immediately recognize them as ciphertext...

Listing 1: Mysterious Letter

```
n = 630548215070129547156718332495889632234434145411971275888376
98760326022525278792613527673894410568910003629553586814142438653
64036495787076991281894914321386319005907747292149900153691027609
6488477634484971781148430952891504011795209806188681,
e = 65535,
C = 260001881613721017824586936303188695001388592045904665092472
88942141164031599839518883636044733874134275920853545431417961290
80184672223816580749894418698048606652831169868033217049601384826
7000849901358921268835393640309700090528873965122393 1.
```

Introduction (2/2)

After timidly writing some definitions on a piece of paper at first, recalling what is often taught in introductory courses in cryptology, it is clear: Textbook-RSA was used by the sender of the message.

After some numerical experiments on your smartphone with the modulus n, using an app connected to the SageMath cloud, you make the following observation – gaining more and more confidence on the way in finally becoming an aspiring student of cryptology:

$$\sqrt{n} = 2511071912690135497619093339586712468024080571127684488625095982415620518894940\\6184735295788387561135167529432680752864558.99999999999999999999999999999999999\\9999999999999999999999999999999999999999999999999999999999999881\ldots$$

Challenge

Telling your colleagues how to solve the riddle, today's task is set:

1. Find an algorithm to factor the RSA modulus n with the peculiar property: $\sqrt{n} \approx k \in \mathbb{N}$.
2. Decrypt the ciphertext c, after completely recovering the private key d: $m = \mathsf{Dec}_d(c)$.
3. Finally, pass the information on to your colleagues, give the key to your local cyber-police department, submit the solution to MysteryTwister, take a selfie, and call it a day!

The solution consists of the complete plaintext of the letter. Please enter the solution in capital letters with spaces between the words.

Reminder: Textbook-RSA

KeyGen: Generates the public key $pk = (N,e)$ and the private key $sk = d$, where d has to be kept secret. The following relations hold:

- $N = p \cdot q$ with prime numbers $p, q \in \mathbb{P} \subseteq \mathbb{N}$,
- $e \in \mathbb{N}$ co-prime to $\varphi(N) := (p-1)(q-1)$, i.e. $\gcd(e, \varphi(N)) = 1$, and
- $d \in \mathbb{N}$ such that $e \cdot d = 1 \mod \varphi(N)$, i.e. $d := e^{-1} \mod \varphi(N)$ s.t. $m = m^{e \cdot d} \mod N$.

Enc: Encryption computes $c := m^e \mod N$.

Dec: Decryption using d: $m = c^d = m^{e \cdot d} \mod N$.

Hints & Info

Hint: If you use SageMath, the following helps with conversions:
from sage.crypto.util import ascii_to_bin, bin_to_ascii, ascii_integer

Additional Information: The scenario is inspired by a real incident from 1997. The message is fictive, it starts with "`Hi`".
Generally, this attack is successful only in negligibly many cases if realistic prime generation is used, of course.