Demonstration of the Acoustic Cryptanalysis

Tomas Fabsic, Ondrej Gallo, Viliam Hromada

Slovak University of Technology in Bratislava

CryptArchi 2017

Contents

Contents

About the attack

- We repeated the attack described in:
  Genkin, D., Shamir, A., Tromer, E. (2014). *RSA key extraction via low-bandwidth acoustic cryptanalysis.*
- Source of the exploited acoustic signal: coils and capacitors within the laptop's voltage regulator.

Contents

Attacked laptop

- The type of laptop matters, not every laptop can be attacked.
- We used Lenovo ThinkPad T61 laptop.
- The laptop ran the RSA implementation from GnuPG 1.4.14..

Microphone

- Needs to be sensitive above acoustic spectrum. (40kHz in case of our laptop)
- We used equipment from Bruel&Kjaer:
    - microphone 4190
    - preamplifier 2669
    - amplifier and power supply 5935

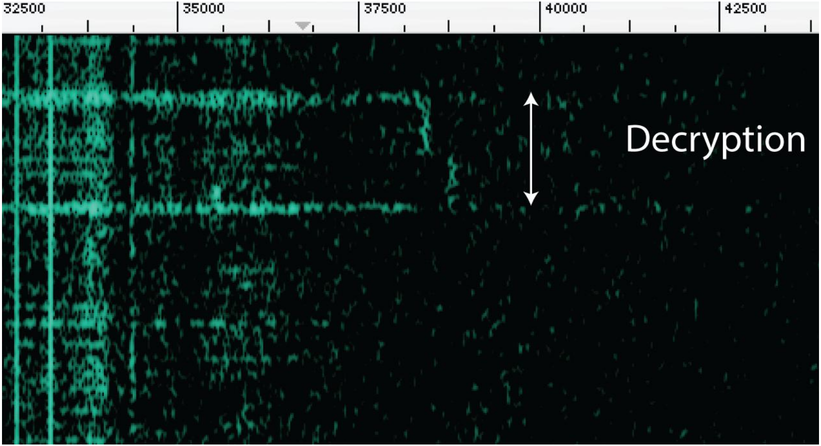
Computer for signal analysis

- A personal computer for analysis of the recorded acoustic signal.
- Contained the baudline signal analysis tool (freeware).

Contents

RSA decryption in GnuPG 1.4.14.

- Uses the Chinese remainder theorem:
  - Firstly $y^d \mod p$ is computed.
  - Afterwards $y^d \mod q$ is computed.
- How does the frequency spectrum of the acoustic signal during decryption look like?


32500
35000
37500
40000
42500
Decryption

Contents

- There is a relationship between position of lines in the spectrogram and the value of the secret primes.
- This can be exploited to reveal the value of the secret primes.

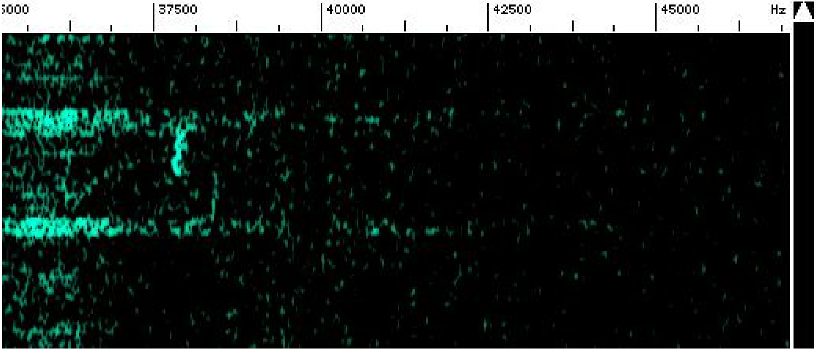
- We can do an adaptive chosen ciphertext attack.
- We reveal the value of the secret prime q bit by bit.
- We know the length of q.
- We know q starts with 1.

To reveal the second bit of q we:

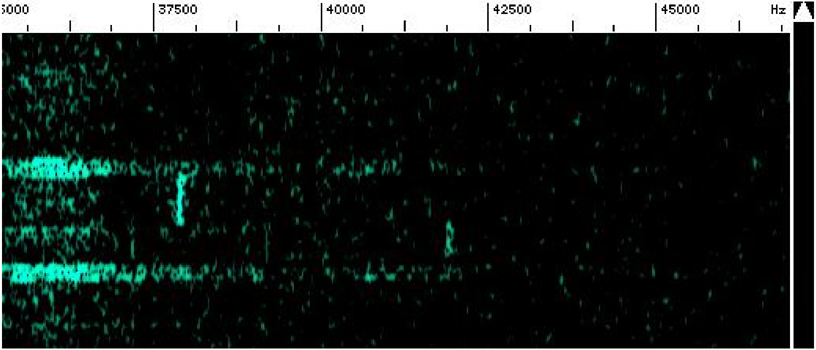
- Make the laptop decrypt the ciphertext $y = 1011\,1111\,1111\,1111\,1111\ldots$, where y has the same length as q.
- The decryption algorithm firstly computes $c = y \mod q$ and exponentiates c instead of y.
- In case the second bit of q is 0, c has a "random looking" structure $\Rightarrow$ ordinary pattern in the spectrogram.
- In case the second bit of q is 1, c has a "very special" structure $\Rightarrow$ strange pattern in the spectrogram.
- Observing the spectrogram, we can detect scenario occurred and determine the value of the second bit.

After learning the second bit, we construct a new ciphertext to reveal the third bit in the same fashion...

Spectrogram when the second bit is 0:



Spectrogram when the second bit is 1:



The End

Thank you for your attention!