CZECH TECHNICAL UNIVERSITY IN PRAGUE
FACULTY OF INFORMATION TECHNOLOGY

ASSIGNMENT OF BACHELOR'S THESIS

Title:	Timing Attack on the RSA Cipher
Student:	Martin Andrýsek
Supervisor:	Ing. Jiří Buček
Study Programme:	Informatics
Study Branch:	Information Technology
Department:	Department of Computer Systems
Validity:	Until the end of winter semester 2018/19

Instructions

Review known timing side channel attacks on RSA decryption and signing operations. Create a demonstration application that will perform timing attack on RSA in order to determine the private key. The application will be used in courses on cryptology and computer security as a part of laboratory exercises. Consider an attack on a local computer or over the network and evaluate its time complexity.

References

Will be provided by the supervisor.

prof. Ing. Róbert Lórencz, CSc.
Head of Department

prof. Ing. Pavel Tvrdík, CSc.
Dean

Prague March 7, 2017

Czech Technical University in Prague
Faculty of Information Technology
Department of Computer Systems

Bachelor's thesis

Timing Attack on the RSA Cipher

Martin Andrýsek

Supervisor: Ing. Jiří Buček

12th May 2017

Acknowledgements

THANKS (remove entirely in case you do not with to thank anyone)

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular that the Czech Technical University in Prague has the right to conclude a license agreement on the utilization of this thesis as school work under the provisions of Article 60(1) of the Act.

In Prague on 12th May 2017 ....

Citation of this thesis

Andrýsek, Martin. *Timing Attack on the RSA Cipher*. Bachelor's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2017.

Abstrakt

Tato prace se zabyva utokem na sifru RSA casovym postrannim kanalem. Pomoci mereni casu podepisovani predgenerovanych zprav, je utocnik schopen postupne uhadnout kazdy bit soukromeho klice. Vysledkem prace je demonstrativni aplikace, ktera bude pouzita ve vyuce predmetu, zabyvajicimi se pocitacovou bezpecnosti.

Klíčová slova Replace with comma-separated list of keywords in Czech.

Abstract

This thesis is focused on replication of timing attack on RSA cipher, which is done by measuring time of square and multiply algorithm. Implementation should be used for education purposes, mainly in security courses.

Keywords RSA, cryptoanalysis, timming attack, side channel, square and multiply

Contents

Introduction **1**

1 State-of-the-art **3**

2 RSA **5**
- 2.1 Principle . . . 5
- 2.2 Optimalization . . . 6

3 Attacks **7**
- 3.1 Attack on multiply . . . 7
- 3.2 Attack on square . . . 7

4 Realisation **9**

Conclusion **11**

Bibliography **13**

A Acronyms **15**

B Contents of enclosed CD **17**

List of Figures

Introduction

Chapter 1

State-of-the-art

Chapter 2

RSA

RSA is public-key cryptosystem which was invented by Ron Rivest, Adi Shamir and Leonard Adleman. The cryptosystem was published in the 1977.

2.1 Principle

The cipher is based on modular exponation. The whole process of crypting message is divided to four steps

2.1.1 Key generation

- Generate p and q, which have to be distinct prime numbers.
- Compute n, where $n = p * q$
- Compute Euler's totient function $\Phi(n)$. Because we know p and q it is simple to compute it.

$$\Phi(n) = (p - 1) * (q - 1)$$

- Generate e such as $\gcd(e, \Phi(n)) = 1$
- Compute $d = e^{-1} \bmod \Phi(n)$
- The pair (e, n) is released as public key
- The pair (d, n) is secret private key

2.1.2 Key distribution

Alice would like to send Bob secret message. Bob generates public key (e, n) and his private key (d, n). Bob sends Alice public key using reliable route (it has not to be secret route), Alice uses it to encrypt her message and sends it to Bob. Bob decrypts her message using his private key.

2.1.3 Encryption

Encryption is done by using public keypair (e, n):

$$c = |m^e|_n$$

where m is plaintext message and c is encrypted message which will be sent to reciever.

2.1.4 Decryption

Decryption is done similar thanks to relation $e * d \equiv 1 \pmod{\Phi(n)}$. We can simply power ciphertext to our private exponent d to obtain original message.

$$|c^d|_n = |(m^e)^d|_n = |m^{e*d}|_n = |m^1|_n = m$$

2.2 Optimalization

Because we generally use high value of modulus n. The exponation of such high numbers is very time consuming so there are some algorithms to increase speed of computation

2.2.1 Square and Multiply

This optimalization uses bitwise representation of the exponent we use. Cycling through all bits from MSB (most significant bit) we determine which operation will be performed for each bit. For bits equal to 1 we perform squaring preset value then we multiply it with the base of exponation. For bits equal to 0 we just perform squaring part.

Algorithm 1 Square & Multiply algorithm

```
function SQUARE_AND_MULTIPLY(m, e, n)
    c ← 1
    k ← BitLen(e)
    for i ← k − 1, 0 do
        c ← c^2
        if e[i] == 1 then                      ▷ ith bit of exponent e
            c ← c ∗ m
        end if
    end for
    return c
end function
```

2.2.2 Chinese remainder theorem

CHAPTER 3

Attacks

3.1 Attack on multiply

3.2 Attack on square

Chapter 4

Realisation

Conclusion

Bibliography

Appendix A

Acronyms

MSB Most significant bit

LSB Least significant bit

Appendix B

Contents of enclosed CD

```
readme.txt ....................... the file with CD contents description
exe ................................... the directory with executables
src ..................................... the directory of source codes
  wbdcm ..................................... implementation sources
  thesis .............. the directory of LaTeX source codes of the thesis
text ........................................ the thesis text directory
  thesis.pdf .......................... the thesis text in PDF format
  thesis.ps ............................. the thesis text in PS format
```