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

14th 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 14th May 2017 .....

Czech Technical University in Prague
Faculty of Information Technology

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

V několika větách shrňte obsah a přínos této práce v českém jazyce.

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

Abstract

Keywords RSA, cipher, timming attack

Contents

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.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce eget dignissim odio. Curabitur eu tellus dui. Cras eu malesuada nisl, sit amet sodales est. Pellentesque ullamcorper congue nisl, vel mollis lacus hendrerit eu. Pellentesque vitae mattis orci, quis tempus quam. Donec pulvinar quam congue arcu imperdiet, at vulputate odio interdum. Integer at sodales odio. In gravida diam in imperdiet convallis. Proin et ullamcorper elit. Phasellus eget fringilla augue. Donec id ex mi.

Mauris faucibus facilisis ultricies. Quisque non convallis ex. Nulla facilisi. Fusce eleifend justo eu nibh molestie hendrerit. Vestibulum a mi vel felis scelerisque semper. Sed nec dapibus nunc. Quisque eget leo ut ante pulvinar laoreet. Pellentesque ullamcorper fermentum lobortis.

Integer in malesuada augue, id auctor ante. Aliquam non lectus rutrum, suscipit mauris non, blandit est. Nulla lobortis felis vitae auctor malesuada. Nam tristique libero eros, vitae commodo nisi eleifend vel. In a accumsan lacus. Pellentesque condimentum luctus augue. Nam in ex sed lectus bibendum tempus. Donec ac porttitor purus.

Duis maximus, risus quis ullamcorper pulvinar, enim mi malesuada magna, eu dictum eros velit sed turpis. Integer et elit vestibulum, congue libero vel, vehicula risus. Suspendisse egestas sodales scelerisque. Phasellus eleifend lobortis venenatis. Ut vitae consequat mi, quis condimentum enim. Nullam placerat erat placerat odio porta, a condimentum odio congue. Aliquam erat volutpat. Donec imperdiet metus sodales dolor commodo iaculis.

Integer sed sapien faucibus, placerat lacus maximus, elementum justo. Curabitur tempus velit eget mauris tempor, nec varius diam efficitur. Nullam consequat, erat vitae egestas vehicula, nunc metus tempor velit, et dapibus urna ex consequat mauris. Praesent a sem id enim iaculis lacinia. Nam sagittis neque est, sed elementum lacus aliquet dignissim. Ut vitae odio vel lorem porta malesuada ac eget mi. Duis sit amet tristique justo. Proin aliquam

diam a suscipit pulvinar.

Chapter 3

Analysis

Chapter 4

Realisation

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

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce eget dignissim odio. Curabitur eu tellus dui. Cras eu malesuada nisl, sit amet sodales est. Pellentesque ullamcorper congue nisl, vel mollis lacus hendrerit eu. Pellentesque vitae mattis orci, quis tempus quam. Donec pulvinar quam congue arcu imperdiet, at vulputate odio interdum. Integer at sodales odio. In gravida diam in imperdiet convallis. Proin et ullamcorper elit. Phasellus eget fringilla augue. Donec id ex mi.

Mauris faucibus facilisis ultricies. Quisque non convallis ex. Nulla facilisi. Fusce eleifend justo eu nibh molestie hendrerit. Vestibulum a mi vel felis scelerisque semper. Sed nec dapibus nunc. Quisque eget leo ut ante pulvinar laoreet. Pellentesque ullamcorper fermentum lobortis.

Integer in malesuada augue, id auctor ante. Aliquam non lectus rutrum, suscipit mauris non, blandit est. Nulla lobortis felis vitae auctor malesuada. Nam tristique libero eros, vitae commodo nisi eleifend vel. In a accumsan lacus. Pellentesque condimentum luctus augue. Nam in ex sed lectus bibendum tempus. Donec ac porttitor purus.

Duis maximus, risus quis ullamcorper pulvinar, enim mi malesuada magna, eu dictum eros velit sed turpis. Integer et elit vestibulum, congue libero vel, vehicula risus. Suspendisse egestas sodales scelerisque. Phasellus eleifend lobortis venenatis. Ut vitae consequat mi, quis condimentum enim. Nullam placerat erat placerat odio porta, a condimentum odio congue. Aliquam erat volutpat. Donec imperdiet metus sodales dolor commodo iaculis.

Integer sed sapien faucibus, placerat lacus maximus, elementum justo. Curabitur tempus velit eget mauris tempor, nec varius diam efficitur. Nullam consequat, erat vitae egestas vehicula, nunc metus tempor velit, et dapibus urna ex consequat mauris. Praesent a sem id enim iaculis lacinia. Nam sagittis neque est, sed elementum lacus aliquet dignissim. Ut vitae odio vel lorem porta malesuada ac eget mi. Duis sit amet tristique justo. Proin aliquam

diam a suscipit pulvinar.

Conclusion

Bibliography

Appendix A

Acronyms

GUI Graphical user interface

XML Extensible markup language

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