Introduction to Cryptography

A Seminar Report

Submitted to the APJ Abdul Kalam Technological University

in partial fulfillment of requirements for the award of degree

Bachelor of Technology

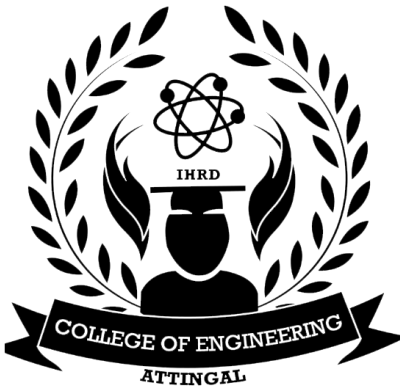
in

Computer Science Engineering

by

Bijin Benny

CEA19CS018



DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

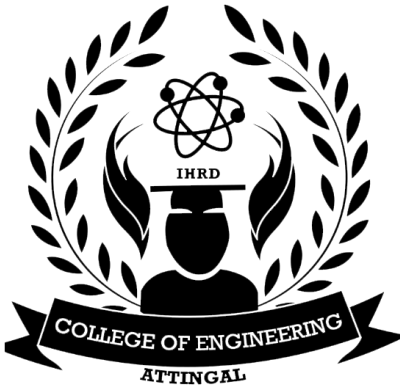
COLLEGE OF ENGINEERING ATTINGAL

KERALA

December 2022

DEPT. OF COMPUTER SCIENCE ENGINEERING COLLEGE OF ENGINEERING ATTINGAL

2022 - 23



CERTIFICATE

This is to certify that the report entitled **Introduction to Cryptography** submitted by **Bijin Benny** (CEA19CS018), to the APJ Abdul Kalam Technological University in partial fulfillment of the B.Tech. degree in Computer Science Engineering is a bonafide record of the seminar work carried out by him under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

MS. Syama S.R
(Seminar Guide)
Assistant Professor
Dept.of CSE
College of Engineering
Attingal

Ms. Remya R.S
(Seminar Coordinator)
Assistant Professor
Dept.of CSE
College of Engineering
Attingal

Ms. Suma M.S
Professor and Head
Dept.of CSE
College of Engineering
Attingal

DECLARATION

I Bijin Benny hereby declare that the seminar report **Introduction to Cryptography** , submitted for partial fulfillment of the requirements for the award of degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of MS. Syama S.R

This submission represents my ideas in my own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources.

I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Attingal
21-12-2022

Bijin Benny

Abstract

Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. Cryptography has often been used to protect the wrong things, or used to protect them in the wrong way. There are a number of cryptographic primitives—basic building blocks, such as block ciphers, stream ciphers, and hash functions. Block ciphers may either have one key for both encryption and decryption. I start with basic concepts of cryptography and move towards its history. Main concentration is on various algorithms including DES, RSA. Here we also discussed cryptographic hash functions-MD family, SHA family and RIPEMD, BLAKE.

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the Emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well.

Bijin Benny CEA19CS018

Acknowledgement

I take this opportunity to express my deepest sense of gratitude and sincere thanks to everyone who helped me to complete this work successfully. I express my sincere thanks to **Ms. Suma M.S**, Head of Department, Computer Science Engineering, College of Engineering Attingal for providing me with all the necessary facilities and support.

I would like to express my sincere gratitude to **Ms. Remya R.S** and **Prof. Seminar coordinator 2**, department of Computer Science Engineering, College of Engineering Attingal for their support and co-operation.

I would like to place on record my sincere gratitude to my seminar guide **MS. Syama S.R**, Assistant Professor, Computer Science Engineering, College of Engineering Attingal for the guidance and mentorship throughout the course.

Finally I thank my family, and friends who contributed to the successful fulfilment of this seminar work.

Bijin Benny

Contents

List of Figures

List of Tables

Chapter 1

Introduction

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography

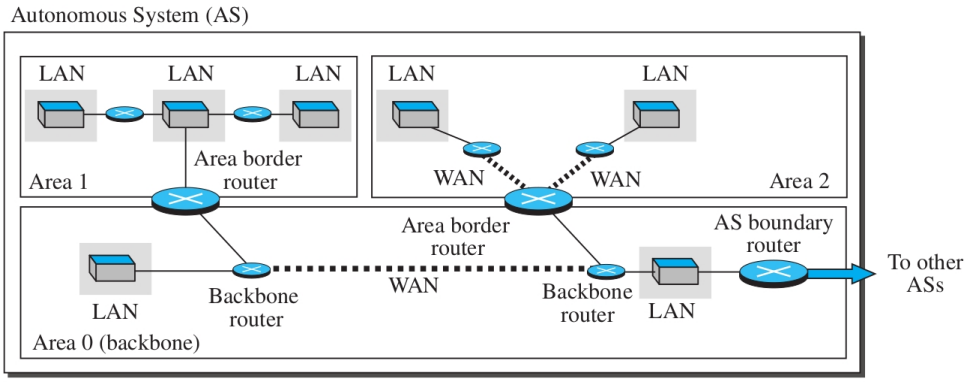


Figure 1.1: Autonomous System Hierarchy

1.1 section1

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

1.1.1 title 2

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

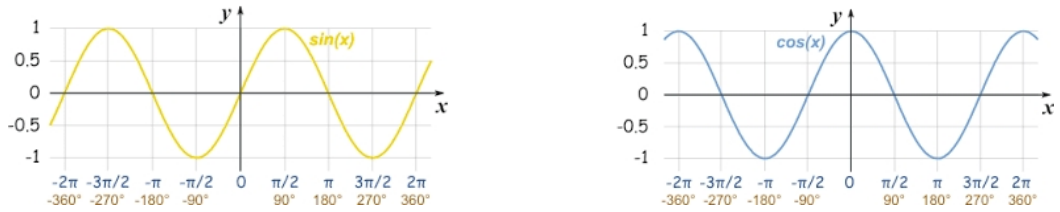
The system is described by the equation 1.1 below. Here y is the ordinate and x is the abscissa , m is the slope and c a constant.

$$y = mx + c \tag{1.1}$$

Page centered and unnumbered multiple equations. The * symbol supresses equation numbering.

$$2x - 5y = 8$$
$$3x + 9y = -12$$

Side by side figures can be created using this environment. See fig 1.2 below.



(a) Sine Wave (b) Cosine Wave

Figure 1.2: The Sine and Cosine waves

Chapter 2

Results

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus,

quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Table 2.1: test table

Sl. No	Item 1	Itm 2
1	37	45
2	42	23
3	47	1
4	52	-21
5	57	-43
6	62	-65
7	67	-87
8	72	-109
9	77	-131
10	82	-153

Chapter 3

Conclusion

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

References

[1] HU, Yun Chao, et al., *Mobile edge computing?A key technology towards 5G*, ETSI white paper, 2015, vol. 11, no 11, p. 1-16.

[2] @online Raspberry pi, `https://www.raspberrypi.org/` Online; accessed 10-June-2019

[3] HU, Yun Chao, et al., *Mobile edge computing?A key technology towards 5G*, ETSI white paper, 2015, vol. 11, no 11, p. 1-16.