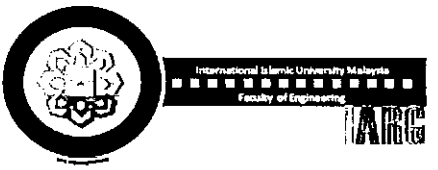
Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM PRESS
2011



Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM Press
2011

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Topics in Coding, Cryptography and Information Security

Contents

Chapter 14

Implementation of RSA Algorithm

Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa

14.1. Introduction

14.1.1. Background

The algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at Massachusetts Institutes of Technology (MIT). The letters RSA are the initials of their surnames. Originally, it was invented at a Passover Seder in Schenectady, New York. Clifford Cocks is a British mathematician working for one of the United Kingdom intelligence agency known as GCHQ, as a head mathematician. He described an equivalent system in an internal document in 1973, but given the relatively expensive computers needed to implement it at that time. It was mostly considered a curiosity invention and it was never deployed as far as publicly known. However, his discovery was not revealed until 1997 due to its top secret classification and Rivest, Shamir and Adleman formulated RSA independently of Cocks' work.

MIT was granted US patent 4405829 for a "Cryptographic communications system and method" that used the algorithm in 1983. The patent expired on 21 September 2000. Since a paper describing the algorithm had been published in August 1977, prior to the December 1977 filing date of the patent application, regulations in much of the rest of the world prohibited patents elsewhere and only the United States patent was granted. Had Cocks' work been publicly known, a patent in the United States would not have been possible either [2].

14.1.2. Problem

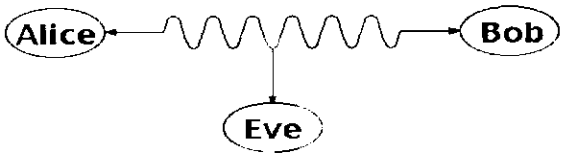


Fig.14. 1: Illustration of Alice-Bob communication