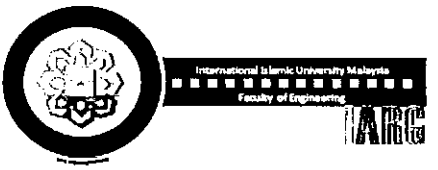

# Topics in Coding, Cryptography and Information Security

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 15

# GSM Security: Problems and Solutions

**Rashid A. Saeed and Othman O. Khalifa**

## 15.1. Introduction

The wireless technology is progressing very fast and become one of the driving forces of the digital explosion and dividend. It becomes one of the basic facilities in our life, which everyone must have. With a mobile handset, anyone can be connected any where at any time. Every day, millions of people are making phone calls, sending messages, etc by pressing a few buttons. Global System for Mobile Communications (GSM) is the most widely used cellular standard, mostly in Europe and Asia and Limited coverage and support in USA. GSM was designed to grow and meet the needs of new technologies. GSM is currently composed of EDGE, 3GSM, and GPSR. Each member of the family is designed to solve a particular need. EDGE is an upper level component used for advanced mobile services such as downloading music clips, video clips, and multimedia messages. GPSR is designed for "always-on" systems that are needed for web-browsing. Not many people known about how this communications been happening and even less is known about the security measures and protection behind the systems. The aim of security for mobile systems is to make the system as secure as the public network and to prevent communication cloning. The use of air interface at the transmission media allows a number of potential threats from eavesdropping. Usually the only air interface part of the GSM network is encrypted. The signal is decrypted at the base station (BS) and then transmitted in clear text across the network. The encryption on the air part was broken in 1998. In this chapter we discuss the GSM security problems and challenges.

## 15.2. GSM architecture

Global System for Mobile Communications GSM is the world's largest mobile phone network, which is covering all Europe, most of Asia and all Africa. It is used by over two billion people across more than 212 countries. GSM was designed in 1982 and became live in 1991 by 3GPP [1]. The 3rd Generation Partnership Project (3GPP) is collaboration between groups of telecommunications associations, known as the organizational partners. A typical GSM network contains Base Stations, a Base Station Concentrator, various databases (MSC, VLR, HLR, AuC, etc), switches and terminals. Various different signal protocols (including SS7) are used to transfer the information between the key elements of the network. The air interface works on four main frequency bands. The range of the wireless