VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELAGAVI

A PROJECT REPORT ON

“EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING”

SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF DEGREE OF

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

BY

Ms. ASMITHA	4AL12IS001
Ms. CHAITRA M.D	4AL12IS005
Ms. DIVYA V	4AL12IS011
Ms. SHWETHA	4AL12IS030

UNDER THE GUIDANCE OF

Mr. JAYANTKUMAR A. RATHOD

ASSOCIATE PROFFESSOR

DEPT. OF INFORMATION SCIENCE AND ENGINEERING

ALVA’S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MOODBIDRI-574225, KARNATAKA

2015 – 2016

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225

KARNATAKA

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the Project entitled "EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING" has been successfully completed by

Ms. ASMITHA	**4AL12IS001**
Ms. CHAITRA M.D	**4AL12IS005**
Ms. DIVYA V	**4AL12IS011**
Ms. SHWETHA	**4AL12IS030**

the bona fide students of Department of Information Science & Engineering, Alva's Institute of Engineering and Technology in partial fulfillment for the award of BACHELOR OF ENGINEERING in ***DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING*** *of the* ***VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI*** *during the year 2015–2016. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the Bachelor of Engineering Degree.*

Mr. Jayanthkumar A Rathod	**Mr. Jayanthkumar A Rathod**	**Dr. Peter Fernandes**
Project Guide,	**Associate Professor,**	
Associate Professor, HOD	**Head of the Department**	**Principal**

External Viva

Name of the Examiners **Signature with Date**

1.
2.

ABSTRACT

The existence of small gadget that can used to exchange message and form conversation networks. It proposes two peculiar techniques for authenticating short encrypted messages that are directed to meet the concern of mobile and Ubiquitous applications. In a symbolic portion of such utilization, the familiarity and purity of the communicated messages are of precise interest. In this work, we propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature.

A method and system for authenticating messages is provided. A message authentication system generates an encrypted message by encrypting with a key a combination of a message and a nonce. The message authentication system generates a message authentication code based on a combination of the message and the nonce modulo a divisor. To decrypt and authenticate the message, the message authentication system generates a decrypted message by decrypting with the key the encrypted message and extracts the message and the nonce. The message authentication system then regenerates a message authentication code based on a combination of the extracted message and the extracted nonce modulo the divisor. The message authentication system then determines whether the regenerated message authentication code matches the original message authentication code. If the codes match, then the integrity and authenticity of the message are verified.

Future work will consist in the examination of advanced authentication protocols for one-way and mutual authentication. Other authentication methods (e.g. asymmetric techniques) should be analyzed for the suitability for RFID systems and circuits can be found for this purpose. In this way, the application range for this proposed system will be pushed further. This means that use of parallel execution of multiple blocks will be much more important and have a practical impact in near future.