SYMMETRIC-KEY ENCRYPTION IN E-LEARNING AND E-LEARNING FOR SYMMETRIC-KEY ENCRYPTION

Presented By

Mohamed Sidi Mohamed Esseyssah

Supervised By

Dr. Sameh S. Daoud Dr. Hatem M. Bahig

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENT FOR THE **M.SC.** DEGREE
(COMPUTER SCIENCE)
SUBMITTED TO
DEPARTEMENT OF MATHAMETICS
FACULTY OF SCIENCE
AIN SHAMS UNIVERSITY
CAIRO, EGYPT

AIN SHAMS UNIVERSITY

Author: **Mohamed Sidi Mohamed Esseyssah**

Title: **Symmetric-Key Encryption in E-Learning and E-Learning for Symmetric-Key Encryption**

Division: **Computer Science**

Department: **Department of Mathematics**

Faculty: **Faculty of Science**

Degree: **M.Sc.** Year: **2011**

Contents

2 Symmetric-key Encryption

3 E-Learning System for Symmetric-Key Encryption

4 Symmetric-Key Encryption in E-Learning

List of Tables

List of Figures

Acknowledgements

I would like to acknowledge *my father* and *mother* who rearing my inspiration. I would not have been able to pursue a master degree or complete this dissertation without their support and encouragement. I would like to thank *Prof. Sameh S. Daoud* for his kind help and valuable discussion and supervision. I would like to express my sincere thank and great gratitude to *Dr. Hatem M. Bahig* for his continuous help, valuable discussion, and supervision, I really appreciate his great effort for helping me to achieve my master degree. I would like to express my thank to *Dr. Hazem M. Bahig* for his helpful discussions and comments in classical encryptions part.

Abstract

Symmetric-key encryptions are the most important elements in many cryptographic systems. We develop an interactive step-by-step visualization system known as *LearnCrypto* that can be used to help in teaching and understanding of symmetric-key encryptions. LearnCrypto system consists of two applications, a web-based application dedicated for classical symmetric-key encryptions and a windows application dedicated for modern symmetric-key encryptions. Also, we study how to use these encryptions for protecting the source code of our e-learning system.

Keywords: Affine cipher, AES, DES, e-learning, Hill cipher, permutation cipher, shift cipher, substitution cipher, Vigenère cipher.

Summary

The widespread use of computers and internet makes information security an increasingly important problem. The most important tool to achieve information security is *Cryptology*. Cryptology, from the Greek *kruptos* (hidden) and *logos* (science), is the science of secure information. In particular, it studies how two entities can send/receive secret messages over an unsecure channel. This can be achieved by encryptions. In symmetric-key encryptions (SKEs), the two entities have to share a common secret key. To enhance understanding of SKEs, we can exploit the electronic technologies to develop an educational system that instructors can use for demonstration purposes and that students can use for tutoring purposes. This exploiting and using of electronic technologies for learning purposes is known as *E-Learning*.

This thesis presents an interactive step-by-step visualization system called *LearnCrypto*, which helps in learning SKEs. For classical SKEs, we developed a web-based application using C# 2.0, ASP 2.0, ADO, HTML, CSS, JavaScript, and SQL database server 2000. For modern SKEs, we developed a windows version using C# 2.0. We also studied how to use SKEs to protect e-learning systems. The thesis consists of an introduction, five chapters, two appendices and the bibliography.

Introduction: It briefly shows the importance of developing an e-learning system for encryptions and the importance of securing an e-learning system using encryptions.

***Chapter One**:* in this chapter, we present fundamental concepts of e-learning, such as its definition, its types, its advantages and disadvantages, and some used models for evaluating e-learning systems.

***Chapter Two**:* This chapter provides a survey on SKE. It gives definition of SKE, types of SKE, some possible attacks on SKE and then demonstrates some examples of SKE.

***Chapter Three**:* In this chapter, we describe our e-learning system, showing the main tools and options that can be used for improving and enhancing the understanding of SKEs. We show how the web-based application is used for learning classical SKEs and how the windows application is exploited for learning modern SKEs. We also give our experience and results which were concluded from using our system during two academic years 2008-2009 and 2009-2010 at Faculty of Science, Ain Shams University.

***Chapter Four**:* This chapter includes how to secure e-learning systems. In particular, it studies how to secure e-learning systems using SKEs. At the end of this chapter we explain how we used SKEs to protect the source code of our web-based system.

***Chapter Five**:* This chapter summarizes the achieved results, and the future work.

Appendix A: It contains definitions for some terms which are not defined in the previous chapters.

Appendix B: It contains installation steps of *LearnCrypto* system.

Some Notations

Expresion/Symbol	**Meaning**
$\mathbb{Z}_n$	$\mathbb{Z}_n = \{0,1,\ldots,n-1\}$, where *n* is a positive integer.
a mod b	Remainder after division of *a* by *b*.
gcd(a, b)	Greatest common divisor for *a* and *b*.
n!	The factorial of *n.*
$\varphi(n)$	The Euler's phi-function, $\varphi(n)$, is equal to the number of integers *x* such that $1 \leq x < n$ and *gcd(x, n) = 1*.
$GF(p^n)$	A Galois field, $GF(p^n)$, is a finite field of order p^n, where *p* is a prime number.
$\binom{n}{k}$	The binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, where *n* is nonnegative integer and $0 \leq k \leq n$.
$\prod_i^n x_i$	$\prod_i^n x_i = x_1 x_2 \cdots x_n$.
$\sum_{i=0}^{n} x_i$	$\sum_{i=0}^{n} x_i = x_1 + x_2 + \cdots + x_n$.