بسم الله الرحمن الرحيم

Sudan University of Science & Technology

(SUST)

College of Graduate Studies

In collaboration with

Center for Engineering Technical Studies (CETS)

Data Encryption Using a Microcontroller

تشفير البيانات باستخدام المتحكم الد قيق

By:

Abd El Rahman Ali Elgezouli

B.Sc in Engineering

Faculty of Engineering& Technology

University of Helwan

1993

A thesis Submitted in Partial Fulfillment of

the Requirement of the Degree of

Master of Science in Telecommunication Engineering

Department Electronic Engineering

Faculty of Engineering& Technology

Supervisor:

Dr. Abdel Rasoul Jabar Alzubaidi

Jan, 2010

الآية القرآنية

قال تعالى:
بسم الله الرحمن الرحيم

اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ
(1)خَلَقَ الإِنسَانَ مِنْ عَلَقٍ (2)
اقْرَأْ وَرَبُّكَ الأَكْرَمُ (3) الَّذِي
عَلَّمَ بِالْقَلَمِ (4) عَلَّمَ الإِنسَانَ
مَا لَمْ يَعْلَمْ (5)

صدق الله العظيم
سورة العلق (الآيات 1-5)

Dedication

For my wife who helped me with my deepest love.

Acknowledgements

I am most grateful to my supervisor, Dr. Abdel Rasoul Jabar Alzubaidi who has guided me through this work.

I am indebted to him for his unceasing encouragement support and advice.

I would like to thank every body who contributed to the success of this research.

Without them this work would never have come into existence.

Abstract

Encryption technology is the art of protecting information by converting it into specific symbols illegible texts called encrypted, and can not be solved only through a secret key is to break the encryption and converts it to plain text unreadable . .

Purpose of encryption is to ensure the conservation of privacy and not to allow anyone to tamper with or viewed as either confidential or very special, no one can understand the substance of that information or messages, only to have its own secret key and that is through a process of decoding or data to the re-original form as plain text and require both encryption and decryption processes use some of the secret instructions commonly referred to as private keys and encryption techniques used by some of the key itself in the two processes, while those keys vary from one operation to another in the techniques of other advanced economies.

This research touched on the History of encryption and the different types and has had a Caesar encryption method using the microcontroller, and the work program and a special chamber program. .

The world is witnessing more attention to systems and encryption techniques in order to obtain safe systems to ensure information.

تـــجـريـــد

تقنية التشفير هي فن حماية المعلومات عن طريق تحويلها إلى رموز معينة غير مقروءة تدعى النصوص المشفرة, ولا يمكن حلها إلا من خلال مفتاح سري يقوم بفك ذلك التشفير ويحوله إلي نص عادى مقروء.

الهدف من التشفير هو ضمان حفظ الخصوصيات وعدم السماح لأحد بالعبث بها أو الاطلاع عليها كونها إما سرية أو خاصة جدا , ولا يمكن لأحد أن يفهم مضمون تلك المعلومات أو الرسائل إلا من لديه المفتاح السري الخاص بها والذي تتم عن طريقه عملية فك التشفير أو إعادة البيانات إلى صيغتها الأصلية كنص عادى وتتطلب كل من عمليتي التشفير وفك التشفير استخدام بعض التعليمات السرية التي يشار إليها عادة بمفاتيح خاصة وتستخدم بعض تقنيات التشفير المفتاح نفسه في العمليتين في حين تختلف تلك المفاتيح من عملية لأخرى في تقنيات أخرى متقدمة.

هذا البحث تطرق إلى نبذة تاريخية عن التشفير و أنواعه المختلفة و قد أجرينا طريقة قيصر للتشفير باستخدام المتحكم الدقيق , وعمل برنامج ودائرة خاصة بالبرنامج

ويشهد العالم المزيد من الاهتمام بأنظمة التشفير و تقنياته وذلك للحصول على أنظمة آمنة لتأمين المعلومات.

Contents

Figure No. Title Page No.

List of Tables

Abbreviations

AES	Advanced Encryption Standard
ASSPs	Application Specific Standard Products
CR	Condition Register
DES	Data Encryption Standard
FPRs	Floating point Registers
GPRs	General Purpose Registers
IAR	Instruction address Register
IDEA	International Data Encryption Algorithm
LED	Lighting Emitting diode
LR	Link Register
NIP	Next Instruction Pointer
OSC	Organic Semiconductors Center
PIC	Personal Internet Communicator
PGP	Pretty good privacy
RISC	Reduce Instruction Set Computing
RES	Reset Input/ Output
SPI	Serial Peripheral Interface
SCI	Serial Communication Interface
VIN	Unregulated power
VSS	System ground