ACKNOWLEDGEMENT

I thank Almighty god for giving me the courage and determination, as well as guidance in conducting this research study, despite all difficulties.

I am heartily thankful to my supervisor, Dr. Abd Alrasoul, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the project.

Finally, I thank all those who assisted, encourage and supported me during this research.

DEDICATION

Dedicated to my parents, who are simply the best parents of all time's. Thank you for unconditional support with my studies. I am honoured to have you as my parents. Thank you for believing on me, giving me a chance to prove and improve my self through all my walks of life. I am blessed to be your daughter.

ABSTRACT

The use of microcontroller increased rapidly in small or dedicated application because it can be considered a self-contained system with a processor, memory and peripherals and can be used with an embedded system.
In this project I design a cipher capable of translate plain text into cipher text and it's a symmetric key cryptography cipher .This cipher is easy to be modified if some one break it . I download the cipher program into the microcontroller to be capable to make ciphering. The plain text is sent through a parallel port in the computer to the microcontroller that exist in the electronic circuit to do an encryption process and display the ciphertext on the computer screen. And send a signal trough microcontroller outputs to light LEDs as a sign of complete of ciphering.

المستخلص

الاستخدام للمعالج الد قيق يزداد بصوره سريعه في التطبي قات الصغيره هو المخصصه لان يمكن اعتباره نظام متكيف ذاتيا مع معالج وذاكره وطرفيات ويمكن استخدامه مع النظام المضمن.
في هذا المشروع تم تصميم شفره قادره على تحويل النص العادي الى نص مشفر وهي من نوع التشفير المتماثل. وهي ايضا سهله التعديل اذا تم إخترا قها. ن قوم بتحميل برنامج الشفره في المعالج الد قيق ليكون قادر على انجاز عملية التشفير(تحويل النص العادي الى نص مشفر. يتم ارسال النص العادي عن طريق منفذ التوازي في الكمبيوتر إلى المعالج الد قيق الموجود في الدائره الالكترونيه لي قوم بالتشفير و إظهار النص المشفر على شاشه الكمبيوتر ومن ثم ارسال اشاره للثنائيات المضيئه دلاله على انتهاء عملية التشفير.

Table of contents

Content	page
Acknowledgment.	I
Dedication.	II
Abstract.	III
المستخلص.	IV
Table of Content.	V
List of figures	I X
List of Table.	X I
.List of Abbreviations	XII
Chapter One: Introduction.	
1.1 Intoduction to cryptography	1
1.2 Problems Statement.	1
1.3 Proposed Solution.	1
1.4 Objectives.	1
Research Methodology. 1.5	2
.Research outline 1.6	4
Chapter Two: symmetric key cryptography	
2.1 Cryptography	6
2.1.1 Plaintext and Ciphertext	6
2.1.2 Cipher	6
2.1.3 Key	6
2.2 Two Categories	**7**
2.2.1 Symmetric-Key Cryptography	**7**
2.2.2 Asymmetric-Key Cryptography	8
2.3 Three Types of Keys 2.4 Comparison	9 9
2.5 Symmetric-key cryptography	10
2.5.1 Traditional Ciphers	10
2.5.1.1 Substitution Cipher	11
2.5.1.2 Shift Cipher	12
Playfair cipher 2.2.1.3	13

2.2.1.4 Hill cipher	14
2.2.1.5 One-time Pad	15
2.5.1.2 Transposition Ciphers	16
2.5.1.2.1 Rotor machine	17
2.5.2 Simple Modern Ciphers	18
2.5.2.1 XOR Cipher	19
2.5.2.2 Rotation Cipher	19
2.5.2.3 Substitution Cipher: S-box	20
2.5.2.4 Transposition Cipher: P-box	21
2.5.3 Modern Round Ciphers	22
2.5.3.1 Data Encryption Standard (DES	22
2.5.3.2 Advanced Encryption Standard (AES)	24
Chapter Three cryptanalysis Techniques	
3.1 Definition of cryptanalysis	26
3.2 History of cryptanalysis	26
3.3The Cryptanalysis	26
3.3.1 Cryptanalysis	27
3.3.1.1 Ciphertext-only attack	27
3.3.1.2 Known-plaintext attack	28
3.3.1.3 Chosen-plaintext attack	28
3.3.1.4 Chosen-ciphertext attack	29
3.3.2 Brute-force attack	29
3.3.2.1 Dictionary attack	33
3.4 Code Breaking	34
3.5 Frequency analysis for simple substitution cipher	36
3.6 Unbreakable codes	36
Chapter Four Microcontroller	
4.1 Microcontroller s	37
4.2 The difference between computer and microcontroller	38
4.2.1 The computers	38
4.2.2 The microcontrollers	38
4.3 Guidelines to choose the appropriate microcontroller	39
4.4 The basic stamp microcontroller	42
4.4.1 BASIC Stamp Architecture Memory Organization	42
4.4.2 Basic stamp Versions	43
4.4.2.1 The basic stamp 1 module (BS1-IC)	43
4.4.2.2 The basic stamp 2 module (BS2-IC)	45
4.4.2.3 The basic stamp 2e module (BS2E-IC)	47
4.4.2.4 The basic stamp 2sx module	47
4.4.2.5 BS2p24	47
4.4.2.6 The basic stamp 2p40 module (BS2p40)	47
4.4.2.7 The basic stamp 2pe module (BS2PE)	48
4.4.2.8 The basic stamp 2px	49

4.4.2.9 The Spin Stamp	49
4.4.2.10 The Javelin Stamp	49
4.5 BASIC Stamp Model Comparison Tables	52
4.6 BASIC Stamp Programming Kit Comparison	53
4.7 OEM Basic Stamp Design and Modules Overview	55
4.7.1 OEM modules	55
4.7**.2 Basic stamp OEM design consideration**	56
Chapter Five Hardware Design	
5.1 Computer	**58**
5.2 combinational circuits	**58**
5.3 Parallel port	59
5.3.1 Parallel Port Anatomy	60
5.3.2 Pin outs	61
5.4 BS2 Microcontroller	62
5.4.1 Features	62
5.5 ULN2003	62
5.5.1 Description	63
5.5.2 Feature	63
5.6 Light Emitting Diodes (LEDs)	64
5.6.1 Testing an LED	64
5.6.2 Colors and materials	65
Chapter Six Software Implementation	
6.1 BASIC Stamp Programming	68
6.2 Equipment Needed	68
6.3 Programming	68
6.3.1 Install and run the BASIC Stamp Editor software	69
6.4 Flow Chart	72
Chapter Seven test and Result	
7.1 Materials	73
7.2 Method	73
7.3 Results	74
Chapter Eight Conclusion and recommendations	
8.1 Conclusion	75
8.2 Recommendations	75
References	76
Appendix A ULN2003A Data Sheet.	**78**
Appendix B	83

List of Figures

Number of figure	Name of figure	Page number
Fig 1.1	programming the microcontroller	2
Fig 1.2	Steps of Cipher process	3
Fig 1.3	Encryption block diagram	4
Fig 2.1	cryptography components	6
Fig 2.2	categories of cryptography	7
Fig 2.3	symmetric key cryptography	8
Fig 2.4	asymmetric key cryptography	8
Fig 2.5	keys used in cryptography	9
Fig 2.6	comparison between two categories of cryptography	10
Fig 2.7	Traditional ciphers	11
Fig 2.8	Transposition cipher	17
Fig 2.9	A series of three rotors from an Enigma machine, used by Germany during World War II	18
Fig 2.10	XOR cipher	19
Fig 2.11	Rotation cipher	20
Fig 2.12	S-box	21
Fig 2.13	P-box: straight, expansion, and compression	22
Fig 2.14	DES	23
Fig 2.15	AES	25
Fig 3.1	A typical distribution of letters in English language text	35
Fig 4.1	BASIC Stamp 2(Rev. G) (Stock# BS2-IC).	46
Fig 4.2	StampSpin Stamp	49
Fig 4.3	Javelin	50
Fig 5.1	parallel pin outs	60
Fig5.2	ULN2003 Pin Configurations	63
Fig 5.5	LED Example	64
Fig 5.6	LED Circuit symbol	64
Fig 5.7	Circuit design	67

Fig 1.6	Test your PC connection to the BASIC Stamp	69
Fig 6.2	Verify that the BASIC Stamp was detected On one of the COM ports.	70
Fig 6.3	Entering the $STAMP and $PBASIC directives from the toolbar	70
Fig 6.4	how to run program	71
Fig 6.5	Flow chart	72
Fig 7.1	Circuit Hard ware	73
Fig 7.2	Circuit connected to a computer	74

List of Tables

Number of table	**Name of table**	**Page number**
Table 2.1	5×5 table containing the key word	13
Table 2.2	AES configuration	24

Table 3.1	Type of attacks on encrypted messages	30
Table 3.2	Average time required for Exhaustive key search	32
Table 4.1	BASIC Stamp 1 Series Comparison	44
Table 4.2	BASIC Stamp2 Pin Descriptions	46
Table 4.3	BASIC Stamp 2 (BS2), with sub-variants	48
Table 4.4	Comparison between BS1, BS2 and BS2e	52
Table 4.5	Comparison between BS2sx, BS2p24, BS2p40, BS2pe and BS2px	53
Table 4.6	Comparison between Kits of basic stamps	53
Table 5.1	Parallel port pins discription	61
Table 5.2	LED types and properties	65

Abbreviations

Abbreviation	Abbreviation Description
AES	Advanced Encryption Standard
A\D	Analog to Digital Converter
ASCII	American Standard Code for Information Interchange
AlGasp	Aluminum Gallium arsenide
AlGaInP	Aluminium Gallium indium phosphide
AlGaP	Aluminium gallium phosphide
AIN	Aluminium Nitride

BS	BASIC Stamp
CPU	Central Processing Unit
COA	Ciphertext-Only Attack
CPA	Chosen-Plaintext Attack
CCA	Chosen-Ciphertext Attack
CDROM	Compact Disk Read Only Memory
DES	Data Encryption Standard
D\A	Digital to Analog Converter
DIP	Dual Inline Package
EPP	Enhanced Parallel Port
ECP	Extended Capabilities
EEPROM	Electrically Erasable Programmable Read-Only Memory
I^2C	**Inter-Integrated Circuit**
I\O	Input / Output.
IC	Integrated Circuit.
IEEE	Institute of Electrical and Electronic Engineers.
InGaN	Indium Gallium Nitride
KPA	known-Plaintext Attack
LED	Light Emitting Diodes
LCD	Liquid Crystal Display
NPN	Negative-Positive-Negative (transistor)
OS	Operating System
OEM	Original Equipment Manufacturer
P-box	Permutation box
PC	Personal Computer.
PWM	Pulse width modulator
PIC	Programmable Interface Controller
PCB	Printed Circuit Board
RAM	Random Access Memory
ROM	Read Only Memory
S-box	Substitution box
SRAM	Static RAM
SOIC	Small outline integrated circuit
Sin	Serial input line
SPP	Standard Parallel Port
TTL	Transistor-transistor logic
TV	Television
UART	Universal Asynchronous Receiver / Transmitter
ZnSe	Zinc selenide