

TABLE OF CONTENTS

DEDICATION	iv
ACKNOWLEDGMENTS	v
ABSTRACT.....	vi
ملخص الرسالة.....	viii
TABLE OF CONTENTS.....	ix
LIST OF TABLES	xiii
LIST OF FIGURES	xiv
Chapter 1. Introduction to Cryptology	1
1.1. Introduction.....	1
1.2. Cryptography	2
1.3. A Brief History of Cryptography	3
1.3.1. Ancient Egyptian	3
1.3.2. Ancient Greece.....	3
1.4. Classical Cryptographic Techniques.....	4
1.4.1. Columnar transpositions:	4
1.4.2. Substitution techniques:	6
1.4.3. Caesar cipher (Monoalphabetic cipher)	7
1.4.4. The Playfair cipher.....	9
1.5. Polyalphabetic Substitution	10
1.5.1. Vigenère Ciphers	10
1.5.2. Jefferson Cylinder:.....	11
1.5.3. Jefferson's wheel cipher:	12
1.6. Cipher machines.....	12
1.6.1. Rotor machine	14
1.6.2. The Second World War	14
1.7. Enigma	14
1.7.1. Post Decryption.....	15
Chapter 2. Basics Of Cryptography.....	17
2.1. What is cryptography	18
2.2. Encryption and Decryption	19
2.2.1. Encryption Advantages:.....	21
2.2.2. Encryption Limitations:	22
2.2.3. Dimensions of cryptography:.....	22
2.2.4. Classification of Cryptographic Techniques.....	23
2.3. Basic Types of Cryptographic Systems	24
2.3.1. Symmetric cryptography.....	24
2.3.2. Types of symmetric ciphers	26
2.3.3. Key Management	27
2.3.4. Symmetric Cipher Model.....	28
2.3.5. Security of Secret-Key Encryption	28
2.4. Public - Key Cryptography	30
2.4.1. Why use public key encryption?.....	32
2.4.2. Advantage and Disadvantages of Public Key Encryption	32
2.4.3. Pretty Good Encryption	33

2.5.	Using keys in cryptography:	35
2.5.1.	What is a key?	35
2.5.2.	Key length	35
2.5.3.	How relevant is key length?	36
2.5.4.	Cryptographic Strength	36
Chapter 3.	Important Concepts	38
3.1.	Mathematical Basics	39
3.1.1.	Exclusive OR	39
3.1.2.	The modulo Function	40
3.1.3.	Modular arithmetic	41
3.1.4.	The congruence relation	41
3.1.5.	Remainders	42
3.1.6.	Prime numbers	42
3.1.7.	Entropy	43
3.1.8.	Confusion and diffusion	43
3.2.	Shift register	43
3.2.1.	Linear feedback shift register	45
3.2.2.	Tap Sequences of Linear Feedback Shift Register	46
3.2.3.	Maximal Length Tap Sequences	47
3.2.4.	NLFSR (Non-Linear Feedback Shift Register)	48
3.3.	Random Number Generator	49
3.3.1.	Pseudorandom Generators	50
3.3.2.	Classical versus modern PRNG	51
3.3.3.	How random number generator works?	55
3.3.4.	What makes a good random number generator?	56
3.4.	Randomness Tests	58
3.4.1.	Theoretical Tests	58
3.4.2.	Empirical Tests	59
3.4.3.	Statistical Tests	59
3.4.4.	Unpredictability	60
Chapter 4.	Symmetric Key Cryptography	61
4.1.	Definition	61
4.2.	Stream Cipher	65
4.2.1.	The one-time pad	65
4.2.2.	Synchronous stream ciphers	66
4.2.3.	Self-synchronizing stream ciphers	67
4.2.4.	RC4 Stream Cipher Algorithm:	70
4.2.5.	Known Weaknesses	73
4.2.6.	Application of RC4	74
4.2.7.	Implementation	74
4.3.	Block Cipher	74
4.3.1.	ECB mode	75
4.3.2.	CBC mode	77
4.3.3.	CFB mode	78
4.4.	OFB mode	80
4.4.1.	RC6 as an AES Candidate	84

4.4.2.	Details of RC6.....	86
4.4.3.	Encryption and decryption.....	87
Chapter 5.	Evaluation Criteria.....	89
5.1.	Appearance	89
5.1.1.	Period	89
5.1.2.	Statistical measures	91
5.2.	Measures of complexity.....	92
5.2.1.	Linear complexity	93
5.3.	Boolean functions	96
5.4.	Representation.....	96
5.4.1.	Truth Tables	97
5.4.2.	Hamming weight.....	97
5.4.3.	Hamming distance	98
5.5.	Correlation	98
5.5.1.	Balance.....	98
5.5.2.	Imbalance.....	98
5.6.	Algebraic Normal Form.....	99
5.6.1.	Algebraic weight.....	99
5.6.2.	Algebraic order	99
5.6.3.	Linear function.....	100
5.6.4.	Affine functions	100
5.7.	The Walsh-Hadamard Transform	100
5.8.	Power Spectrum	101
5.8.1.	Polarity Spectrum.....	101
5.8.2.	Parseval's equation	101
5.8.3.	Nonlinearity	102
5.8.4.	Correlation Immunity and Resilience	103
5.8.5.	Correlation Immunity.....	104
5.8.6.	Resilience.....	104
5.8.7.	Autocorrelation	105
5.8.8.	Autocorrelation Function.....	105
5.8.9.	The Propagation Criteria.....	106
5.8.10.	Avalanche Effect.....	106
5.8.11.	Bent Functions	107
Chapter 6.	Results, Conclusion, And Future Work	108
6.1.	The Key Idea.....	108
6.2.	NIST Tests	110
6.2.1.	Frequency test	110
6.2.2.	Frequency test within a block	111
6.2.3.	Runs test.....	111
6.2.4.	Rank test.....	111
6.2.5.	Discrete Fourier transform test	111
6.2.6.	Linear complexity test.....	111
6.2.7.	Serial test.....	112
6.2.8.	Approximate entropy test.....	112
6.2.9.	Cumulative sums (CuSum) test	112

6.2.10.	Universal statistical test	112
6.3.	Sample of our implementation.....	112
6.4.	RC4 stream cipher.....	116
6.5.	RC6 block cipher	118
6.6.	Conclusion and Future Work.....	121
REFERENCES		122