

List of contents

Thanks	--
List of Figures	--
List of Tables	--
General Introduction	01
 CHAPTER I: Introduction to Cryptography	
1. Introduction	04
2. Security Properties	04
2.1. Authentication	04
2.2. Non-Repudiation	04
2.3. Confidentiality	05
2.4. Integrity	05
3. Cryptology	05
4. Cryptography	06
4.1. Symmetric Key Encryption	06
4.1.1. Principle	06
4.1.2. Small taxonomy of classic symmetric encryption	07
4.1.2.1. Caesar cipher	07
4.1.2.2. Vigenere cipher	07
4.1.3. Substitution and transposition (or confusion and diffusion)	08
4.1.4. Modern and powerful techniques	08

4.1.4.1. DES (Data Encryption Standard)	08
4.1.4.2. Triple DES	09
4.1.4.3. AES (Advanced Encryption Standard)	10
4.2. Public Key Encryption	11
4.3. Key security	11
4.3.1. Key Distribution	11
4.3.1.1. Case of Symmetric Key Encryption	12
4.3.1.2. Case of Public Key Encryption	12
4.3.2. Key Exchange	12
4.3.2.1. Diffie-Hellman protocol	12
4.3.2.2. Quantum key Distribution	13
4.4. Difference between Symmetric Key and Public Key Encryption	14
4.5. Complexity of cryptographic algorithms	15
4.6. Encryption modes	15
4.6.1. Block cipher mode	15
4.6.1.1. Electronic Code Book (ECB) mode	15
4.6.1.2. Cipher Block Chain (CBC) mode	16
4.6.1.3. Cipher FeedBack (CFB) mode	17
4.6.1.4. Output FeedBack (OFB) mode	18
4.6.1.5. Counter (CTR) mode	18
4.6.2. Stream cipher mode	19
4.7. Hash function	19
4.8. Digital signature	20

5. Cryptanalysis	21
5.1. Ciphertext only attacks (COA)	21
5.2. Known plaintext attacks (KPA)	21
5.3. Chosen plaintext attacks (CPA)	21
5.4. Chosen ciphertext attacks (CCA)	21
5.5. Man-in-the-middle attacks (MITMA)	21
5.6. Side Channel Attacks (SCA)	22
5.7. Brute Force Attacks (BFA)	22
6. Conclusion	23

CHAPTER II: AES Cipher

1. Introduction	25
2. Mathematical preliminaries	25
2.1. Addition	25
2.2. Multiplication	26
2.3. Polynomials with coefficients in $GF(2^8)$	27
3. AES Algorithm Using 512 Bit Key (specification)	29
3.1. Cipher	29
3.1.1. SubBytes()	30
3.1.2. ShiftRows()	31
3.1.3. MixColumns()	32
3.1.4. AddRoundKey()	32
3.2. Inverse cipher	33

3.2.1. InvSubBytes()	33
3.2.2. InvShiftRows()	34
3.2.3. InvMixColumns()	34
3.2.4. Inverse of AddRoundKey()	34
4. Key management	35
4.1. Key length requirements	35
4.2. Key expansion and rounds	35
5. Advantages and disadvantages of 512-bits AES	37
6. Complexity analysis	37
7. Experiences and results (memory space and encryption time)	38
8. Explanatory example	39
9. Conclusion	40

CHAPTER III: High Lightweight Encryption Standard (HLES)

1. Introduction	42
2. The proposed algorithm	42
2.1. The Encryption Algorithm (E)	42
2.1.1. General Schemes of the encryption algorithm	43
2.1.2. Overview of the operation	44
2.1.3. The encryption algorithm transformations	44
2.1.3.1. Bytes substitution	44
2.1.3.2. SH-Z transformation	45

2.1.3.3. Key-Xor and L-Xor transformations	48
2.2. Decryption algorithm (D)	48
2.2.1. Overview of the operation	48
2.2.2. Details of the decryption algorithm	49
2.2.2.1. Inverse of S-Box	49
2.2.2.2. Inverse of SH-Z	50
2.2.2.3. Inverse of Key-Xor and L-Xor transformations	50
2.3. Sub key generator	50
2.4. Complexity of the algorithm	52
2.5. Analysis of Security of the method	52
2.6. Analysis of performance of the algorithm	53
3. Conclusion	54

CHAPTER IV: Implementation & Experimental Results

1. Introduction	56
2. Environment of development	56
2.1. Operating system	56
2.2. Programming language	56
2.3. Programming tool, platform, and environment	57
3. Architecture of the application	57
3.1. GUE (Graphical User Interface)	57
3.2. The principal classes	58
4. Tests and experimental results	64
4.1. Criteria of the encryption time	64

4.1.1. Tests and results	64
4.1.2. The encryption evolution vis-a-vis the file size	69
4.2. Evolution of the memory space	70
4.3. Study of the method security	71
5. Conclusion	72
General Conclusion.....	73