

List of figures

CHAPTER I: Introduction to Cryptography

Figure I.1: Symmetric key encryption	06
Figure I.2: Caesar cipher	07
Figure I.3: Vigenere cipher	07
Figure I.4: Triple DES	09
Figure I.5: Public Key Encryption	11
Figure I.6: Quantum key Distribution	13
Figure I.7: Electronic Code Book (ECB) mode	16
Figure I.8: Cipher Block Chain (CBC) mode	17
Figure I.9: Cipher FeedBack (CFB) mode	17
Figure I.10: Output FeedBack (OFB) mode	18
Figure I.11: Counter (CTR) mode	19
Figure I.12: Hash function	20
Figure I.13: Man-in-the-middle attacks (MITMA)	22

CHAPTER II: AES Cipher

Figure II.1: Byte substitution	30
Figure II.2: Substitution values in hexadecimal form	31
Figure II.3: Shift rows	31
Figure II.4: Inverse values of SubBytes() function in hexadecimal form	33

Figure II.5: Inverse of ShiftRows function	34
Figure II.6: Round Structure of AES	37

CHAPTER III: High Lightweight Encryption Standard (HLES)

Figure III.1: General architecture of the proposed algorithm	43
Figure III.2: General code of the encryption algorithm	44
Figure III.3: Byte substitution	45
Figure III.4: SH-Z transformation	46
Figure III.5: Data block	46
Figure III.6: Sub-key block	46
Figure III.7: The result block	47
Figure III.8: The encryption / decryption algorithm	48
Figure III.9: General code of the decryption algorithm	49
Figure III.10: Inverse of Byte substitution	50
Figure III.11: The pseudo code of sub-key generation	51

CHAPTER IV: Implementation & Experimental Results

Figure IV.1: architecture of the application	57
Figure IV.2: user Control 1	61
Figure IV.3: user Control 2	61
Figure IV.4: user Control 3	62
Figure IV.5: user Control 4	62

Figure IV.6: user Control 5	63
Figure IV.7: principal classes	63
Figure IV.8: Encryption / Decryption time for TXT File	65
Figure IV.9: Encryption / Decryption time for JPG File	66
Figure IV.10: Encryption / Decryption time for PNG File	67
Figure IV.11: Encryption / Decryption time for MP3 File	68
Figure IV.12: Encryption / Decryption time for MP4 File	69
Figure IV.13: change of time comparing with the size of data for the three algorithms ...	70