

Contents

• Analysis	1 - 8
◦ Project Idea	1
◦ Client	1 - 2
◦ Choosing the right algorithms.	3 - 6
◦ Objectives	6 - 8
• Design	9 - 51
◦ Bluetooth	9
▪ Protocol	9/10
▪ Sending files over Bluetooth	10/11
◦ File Storage	11 - 13
▪ Encryption	13
◦ AES	13 - 25
▪ History	13
▪ The Algorithm	14 - 25
▪ Data handling + Before the operation starts.	14 - 16
▪ The operation.	16 - 25
◦ SHA256	25 - 34
▪ The Algorithm	26 - 34
▪ How the data is handled.	26/27
▪ Before the operation starts.	27 - 30
▪ The operation.	30 - 34

○ BLAKE2b	34 - 40
▪ The Algorithm	34 - 40
▪ How the data is read.	34 - 35
▪ The operation.	35 - 40
○ Quick Sort	40 - 41
○ UI Research	42 - 48
▪ Main Program (on PC)	42 - 47
▪ The App	47 - 48
○ The program as a whole	49 - 51
▪ IPSO diagram	49 - 50
▪ Using a USB stick	51
▪ Storing the files at home	51
 • Technical Solution	 52 - 143
○ File structure	52 - 53
○ Configuration of the program	53 - 56/57
○ The PC App GUI	57 - 65
▪ Login Screen	57 - 59
▪ Main Screen	60 - 63
▪ The Information Tab	60 - 62
▪ Encryption and Decryption Status	62 - 63
▪ Settings Screen	63/64
▪ Search Bar	64/65
○ The Mobile App GUI	65 - 69
○ Key Algorithms	70 - 97/98
▪ AES	70 - 87

▪ AES package	70 - 76
▪ AESfiles package	76 - 82
▪ AESstring package	82 - 84
▪ AEScheckKey package	84 - 85
▪ The main package	85 - 87
▪ SHA256	87 - 90
▪ BLAKE2b	90 - 94
▪ The Sorts	95 - 98
◦ The File class	98 - 100
◦ PC app GUI code	100 - 131
▪ The root of the GUI	100 - 101
▪ Login classes	101 - 105
▪ Main Screen	106 - 129
▪ Main Screen code	106 - 120
▪ Main Screen Buttons	120 - 122
▪ Main Screen Popups	122 - 128/129
▪ Main Screen Labels	129
▪ Settings Screen	129 - 131
◦ Mobile App GUI Code	131 - 143
▪ The root of the GUI	131 - 134
▪ Pad Screen	134 - 137
▪ Main Screen	137
▪ File Selection Screen & Shared Bluetooth functions	137 - 142
▪ SHA	142
▪ What is bulldozer.spec?	142 - 143
• Testing	143 - 192

◦ Unit Tests	143 - 152
▪ AES	143 - 150
▪ Testing the core algorithm	144 - 147
▪ Testing AESfiles package	147 - 149
▪ Running the tests	149 - 150
▪ BLAKE2b	151 - 152
▪ Summary	153 - 155
◦ Black-box tests	156 - 197
◦ Fixing failed tests	197 - 200
 • Evaluation	 201 - 205
◦ User Feedback	201 - 202
◦ Evaluation of Objectives	202 - 205
◦ Things I would do to improve the project	205