

# 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

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

▪ 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

---

◦ <b>Unit Tests</b>	<b>143 - 152</b>
▪ <b>AES</b>	<b>143 - 150</b>
▪ Testing the core algorithm	144 - 147
▪ Testing AESfiles package	147 - 149
▪ Running the tests	149 - 150
▪ <b>BLAKE2b</b>	<b>151 - 152</b>
◦ <b>Black-box tests</b>	<b>152 - 192</b>

• <b>Evaluation</b>	<b>193 - 196</b>
---------------------	------------------

---

◦ <b>Evaluation of Objectives</b>	<b>193 - 196</b>
◦ <b>Things I would do to improve the project</b>	<b>196</b>