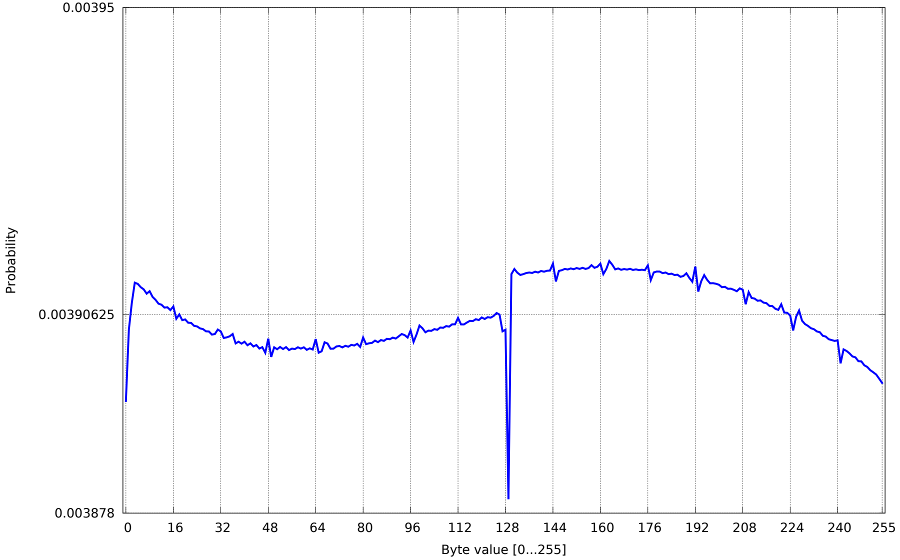
Biases in the RC4 keystream (128 bit uniform keys)

Nadhem AlFardan and Dan Bernstein and Kenny Paterson and Bertram Poettering and Jacob Schuldt

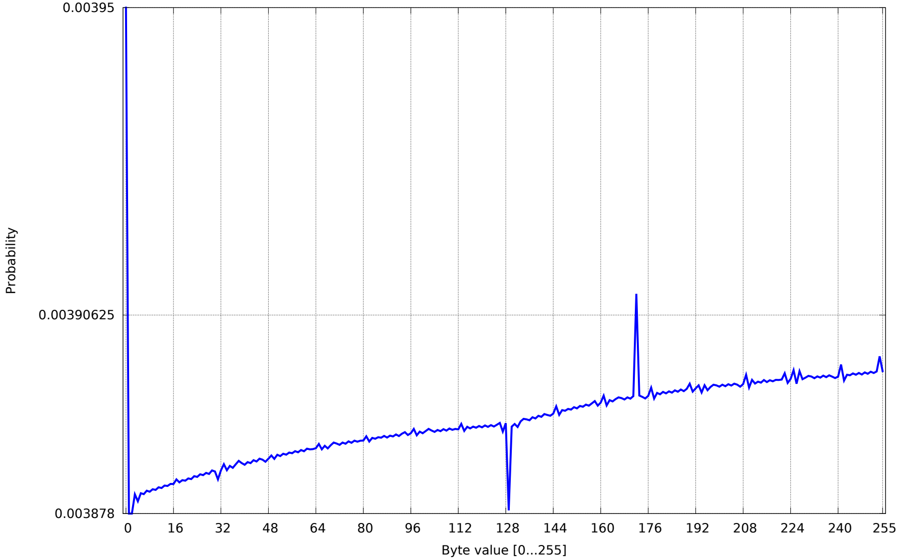
Royal Holloway, University of London
University of Illinois at Chicago

http://www.isg.rhul.ac.uk/tls/

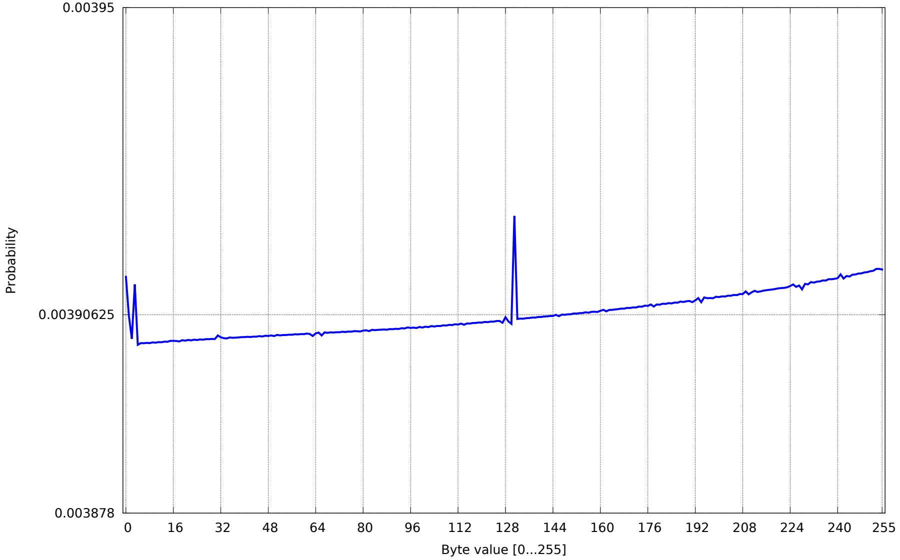
Keystream distribution at position 1



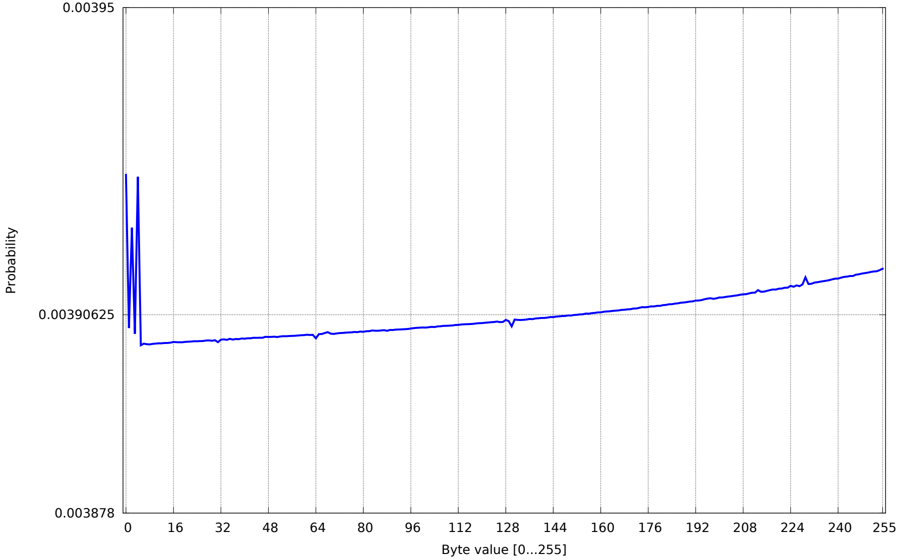
Keystream distribution at position 2



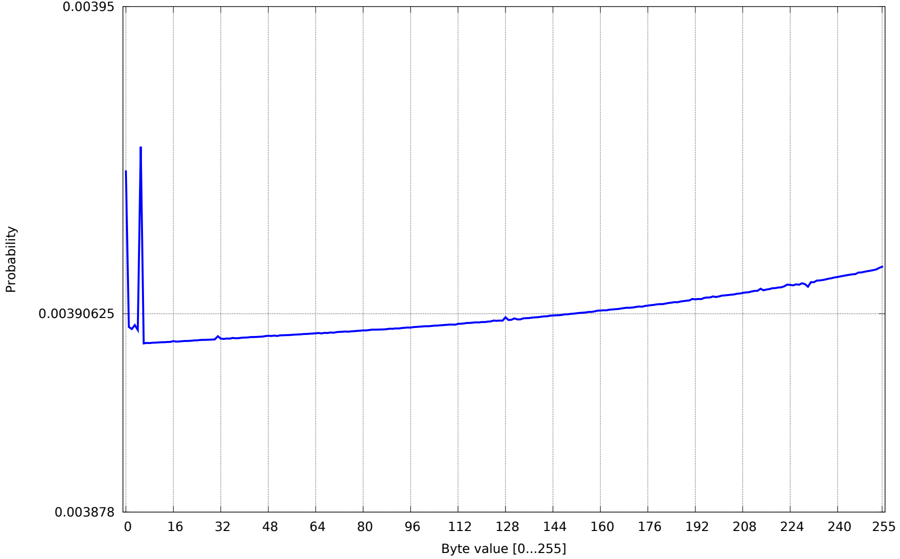
Keystream distribution at position 3



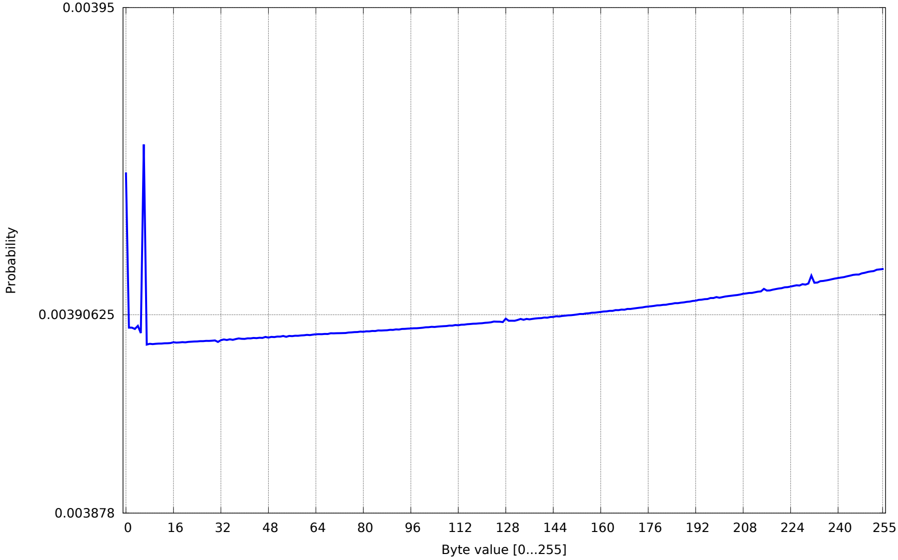
Keystream distribution at position 4



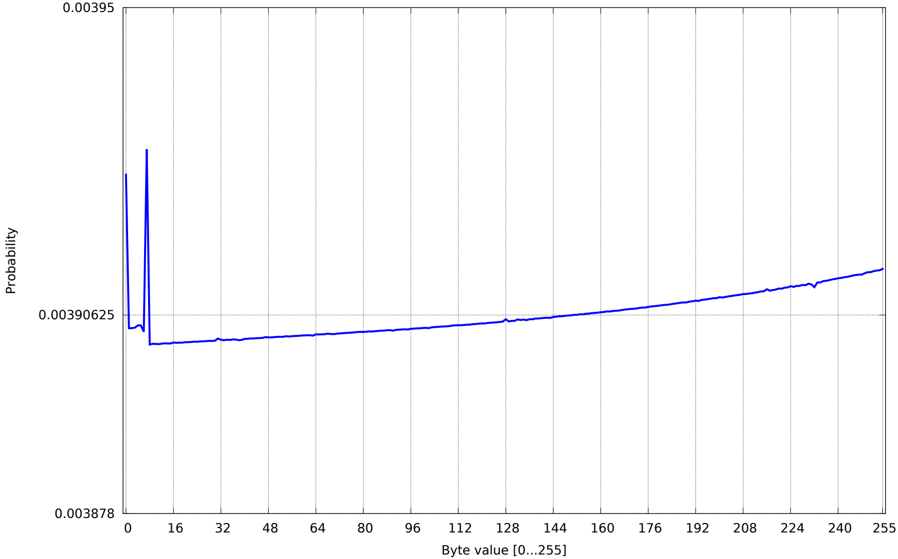
Keystream distribution at position 5



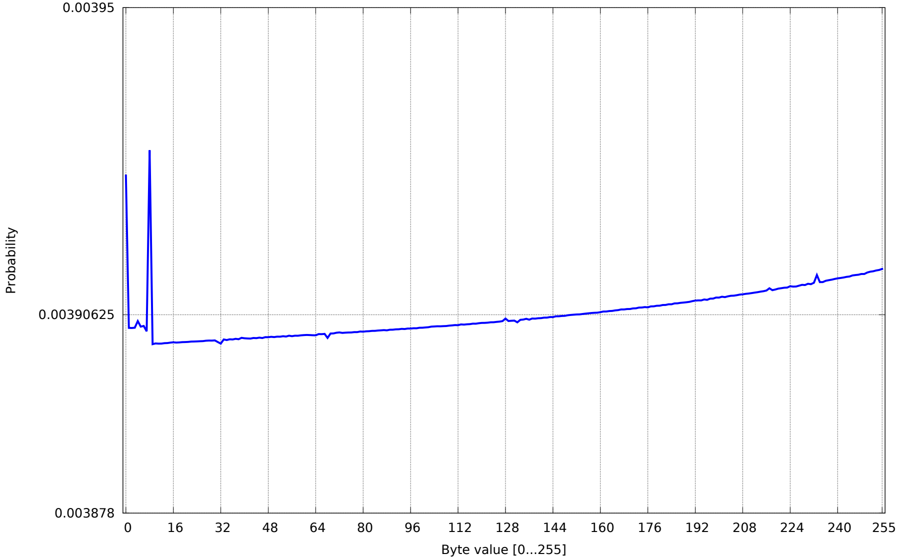
Keystream distribution at position 6



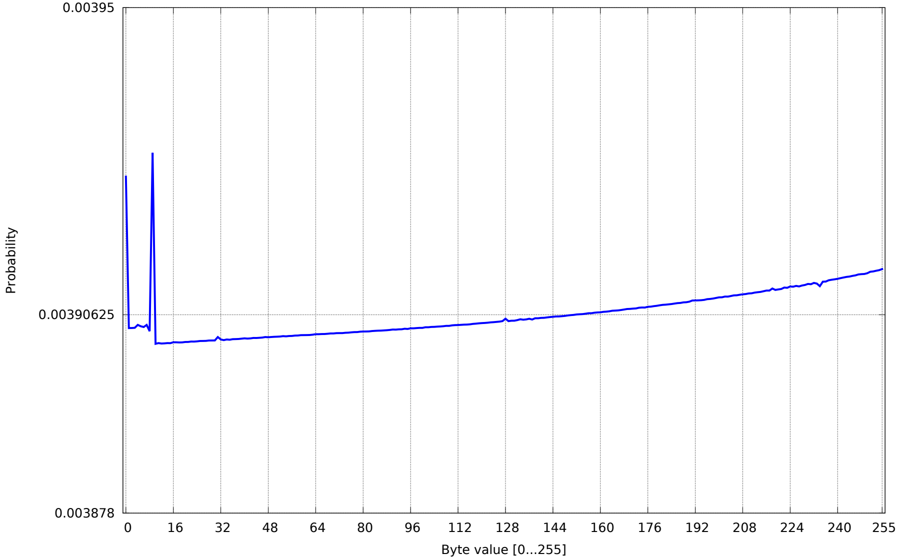
Keystream distribution at position 7



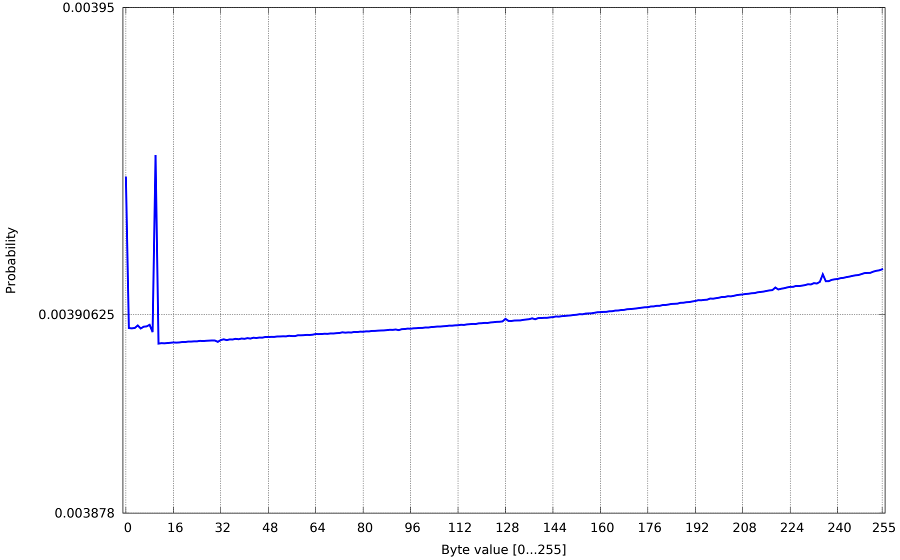
Keystream distribution at position 8



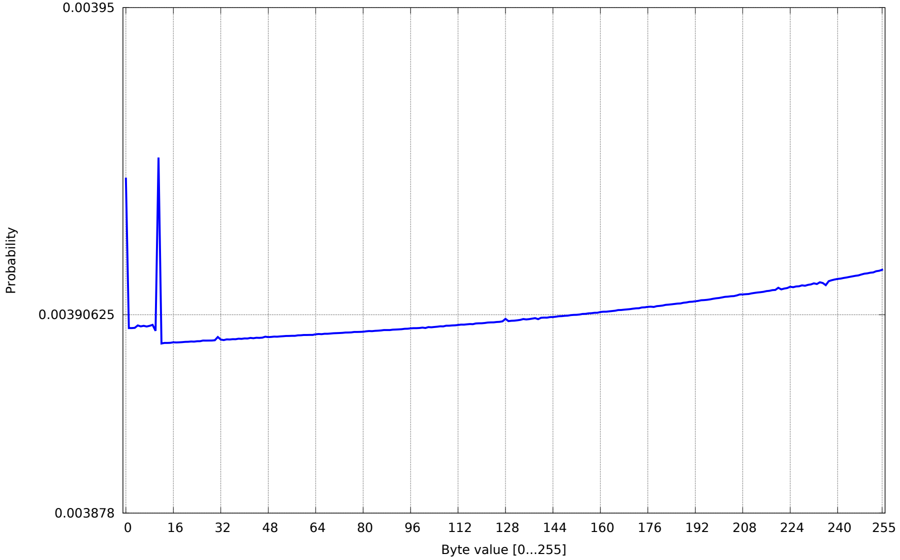
Keystream distribution at position 9



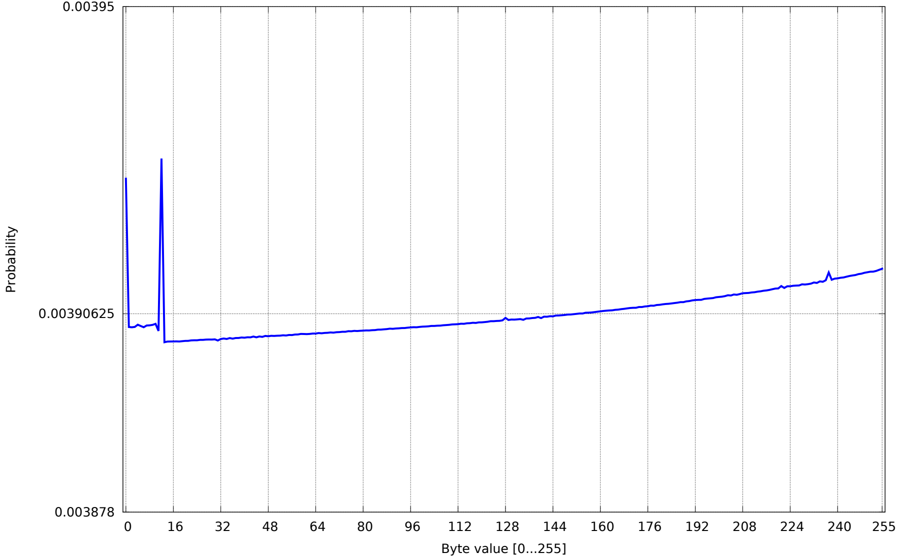
Keystream distribution at position 10



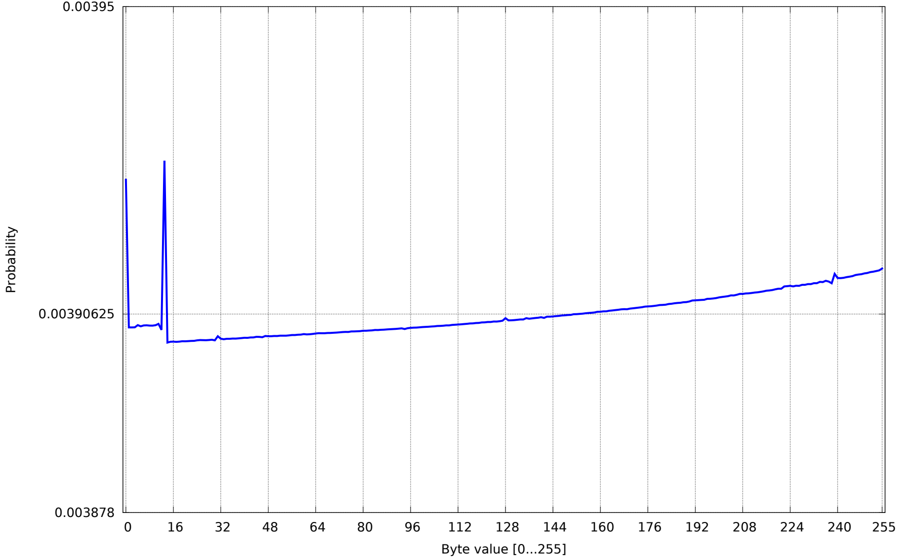
Keystream distribution at position 11



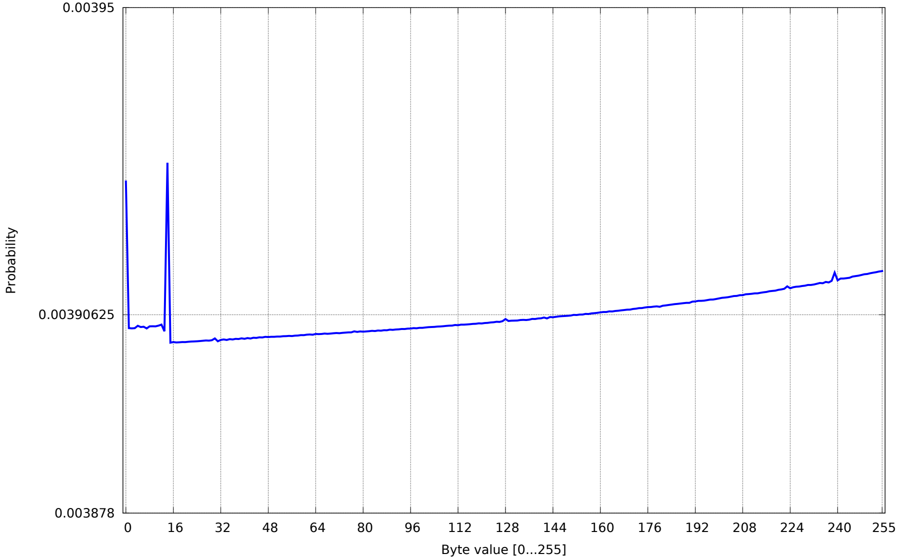
Keystream distribution at position 12



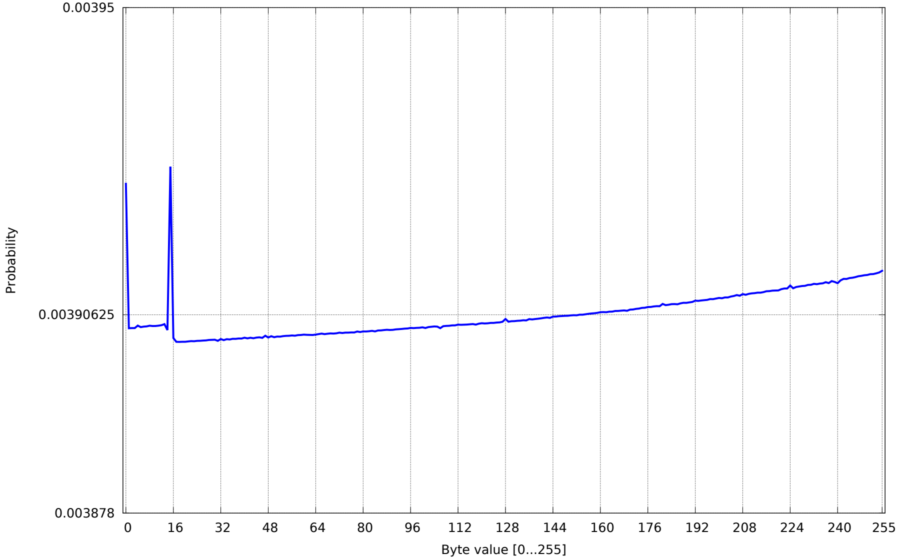
Keystream distribution at position 13



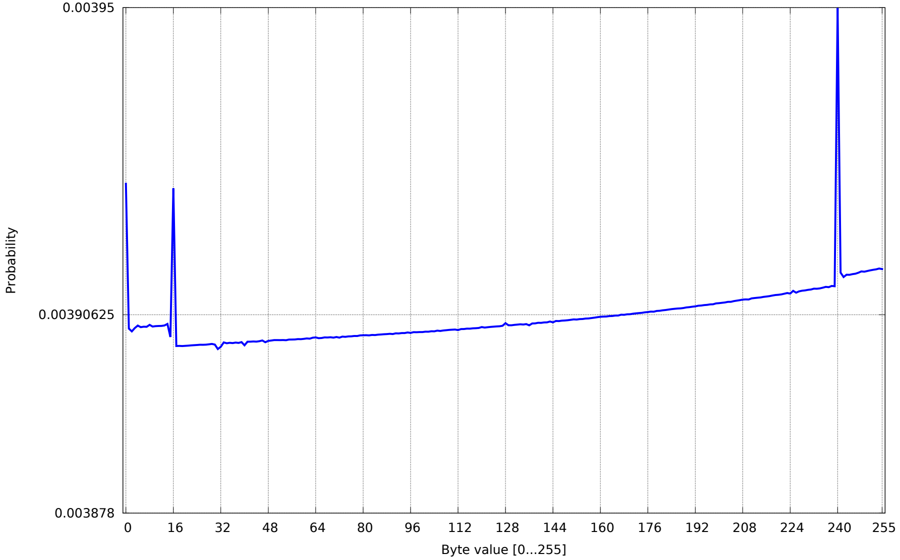
Keystream distribution at position 14



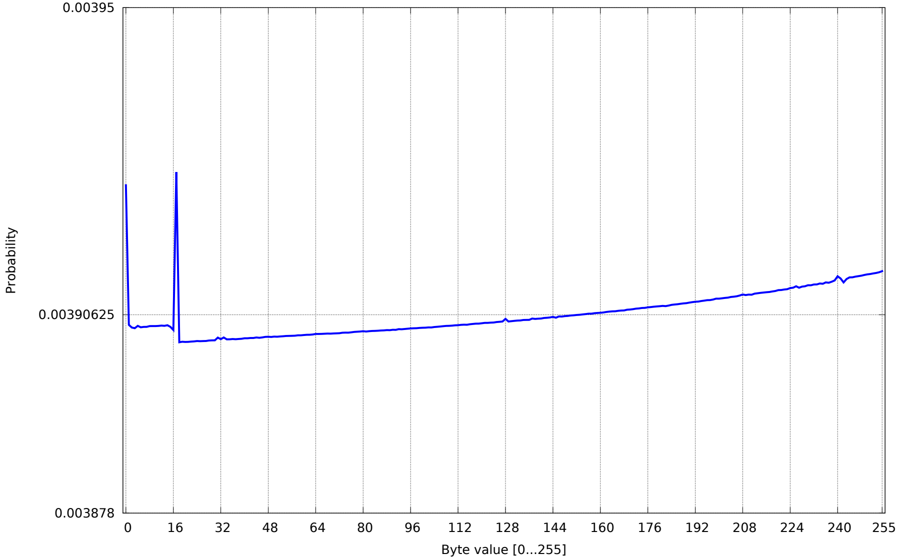
Keystream distribution at position 15



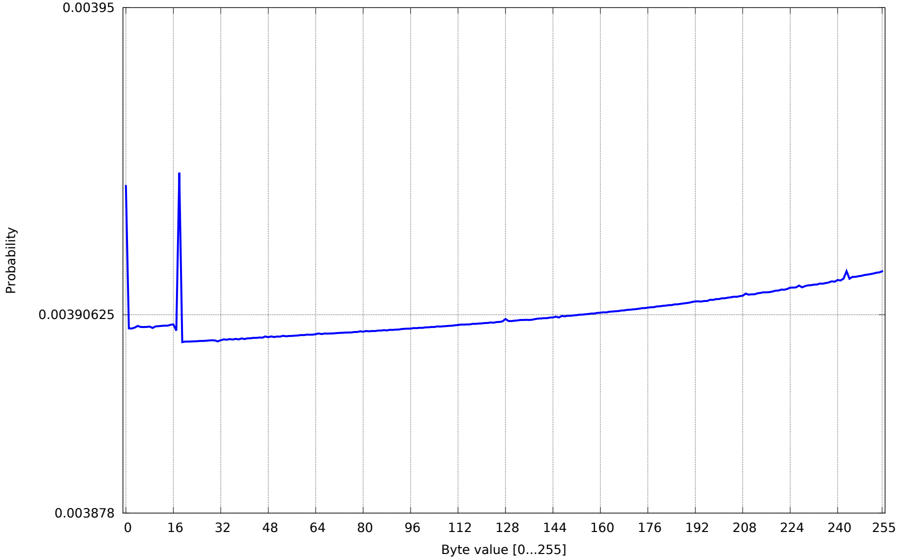
Keystream distribution at position 16



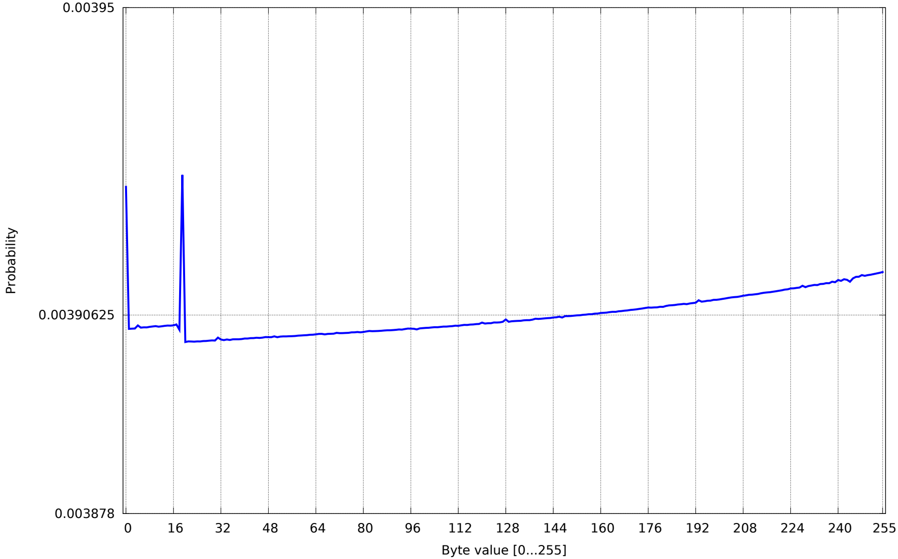
Keystream distribution at position 17



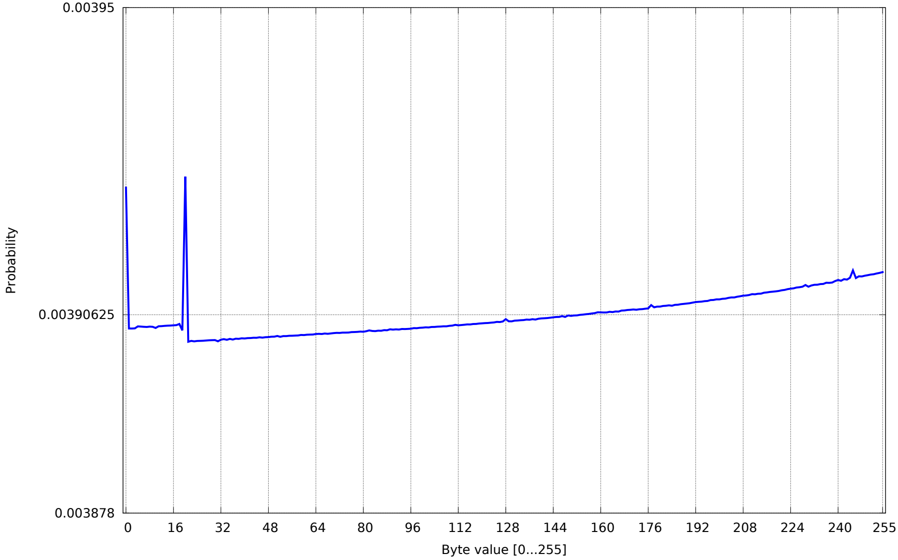
Keystream distribution at position 18



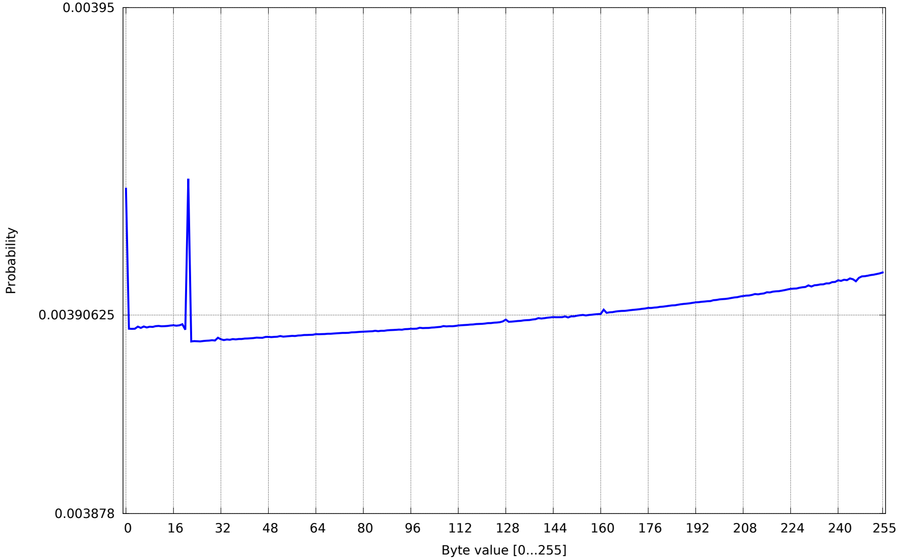
Keystream distribution at position 19



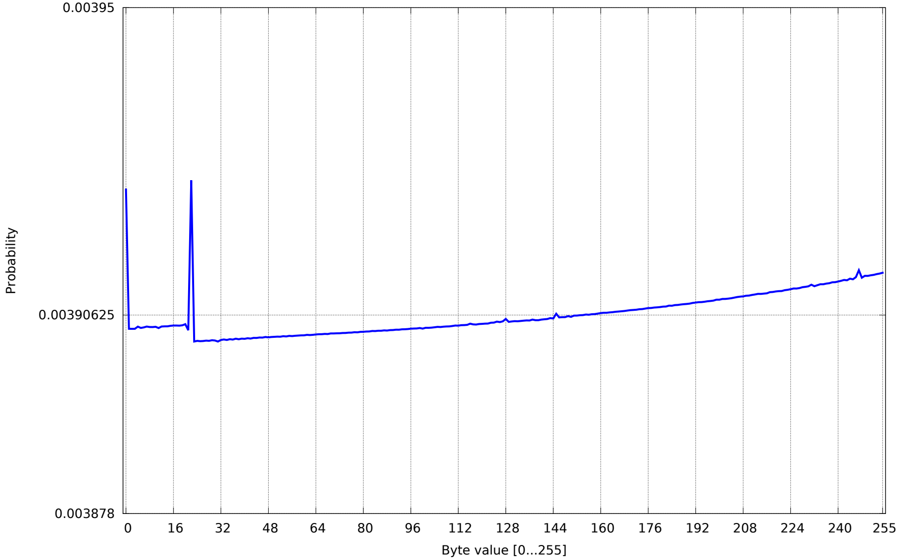
Keystream distribution at position 20



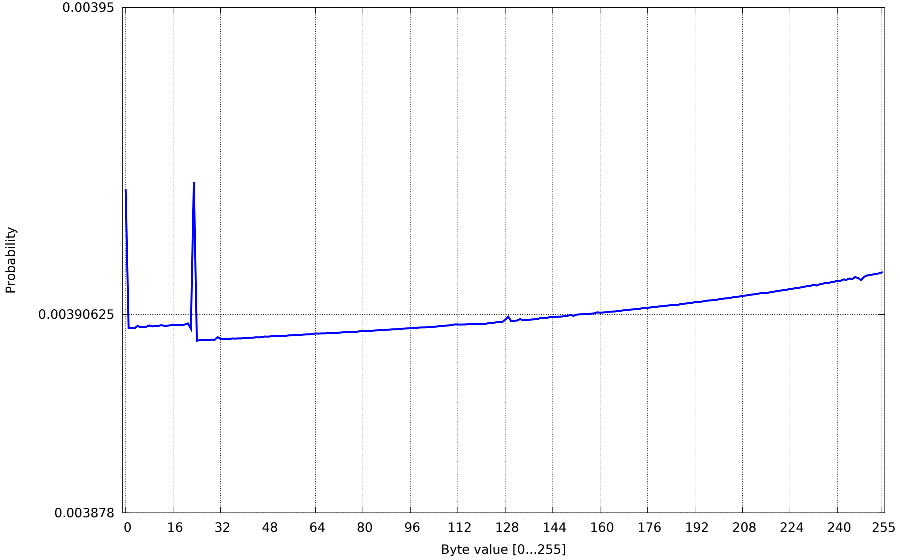
Keystream distribution at position 21



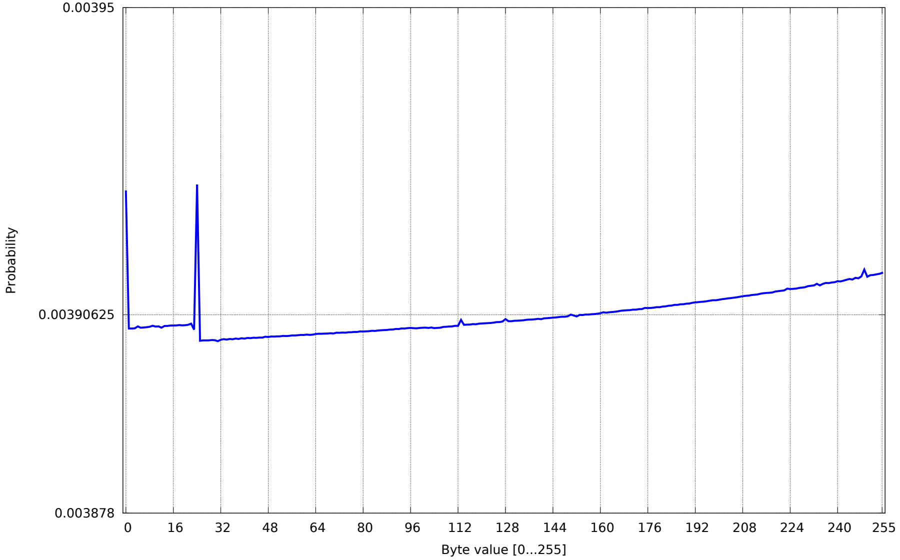
Keystream distribution at position 22



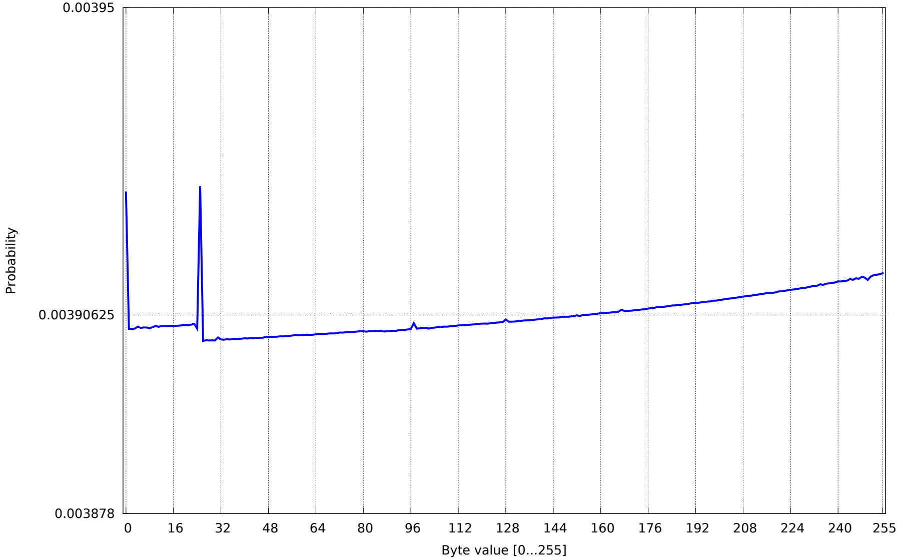
Keystream distribution at position 23



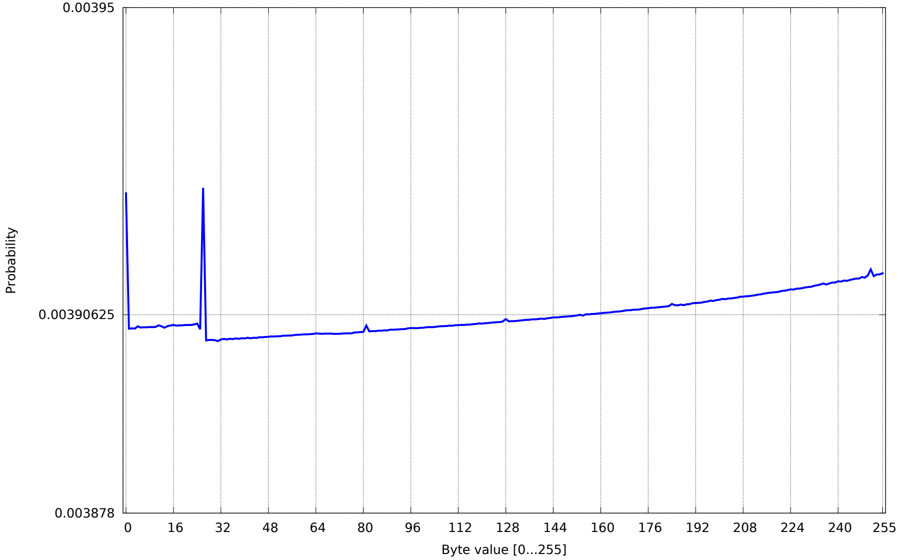
Keystream distribution at position 24



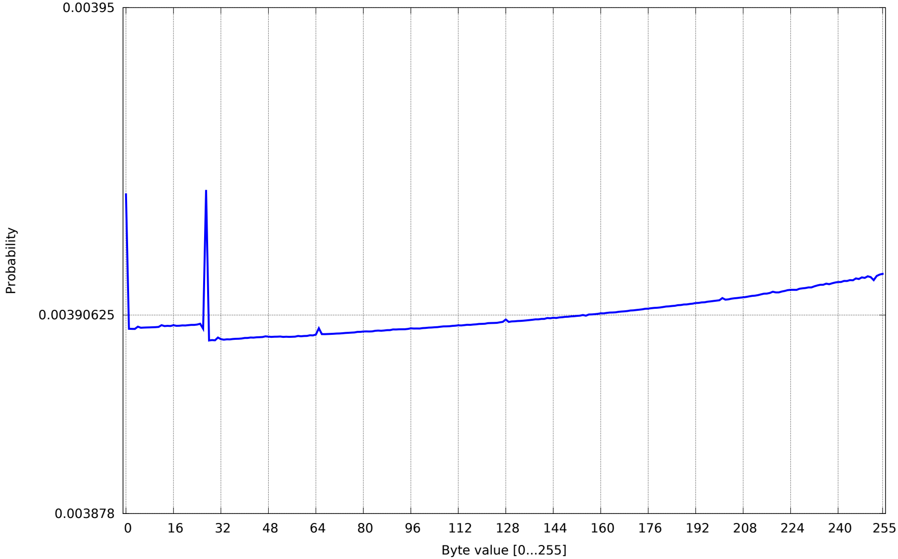
Keystream distribution at position 25



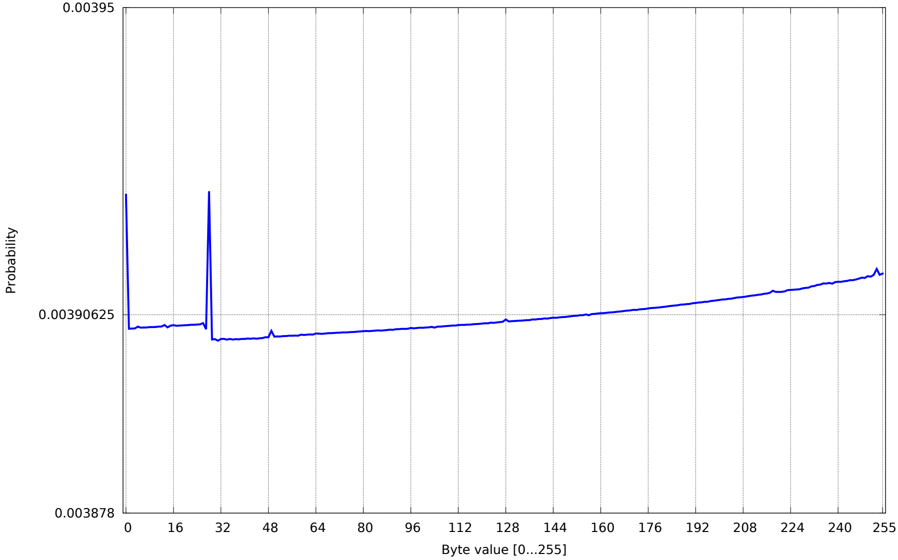
Keystream distribution at position 26



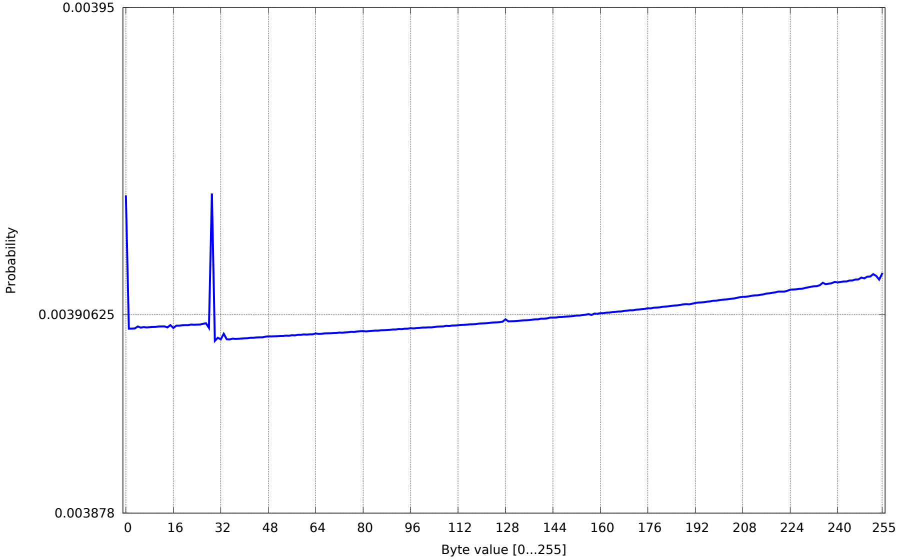
Keystream distribution at position 27



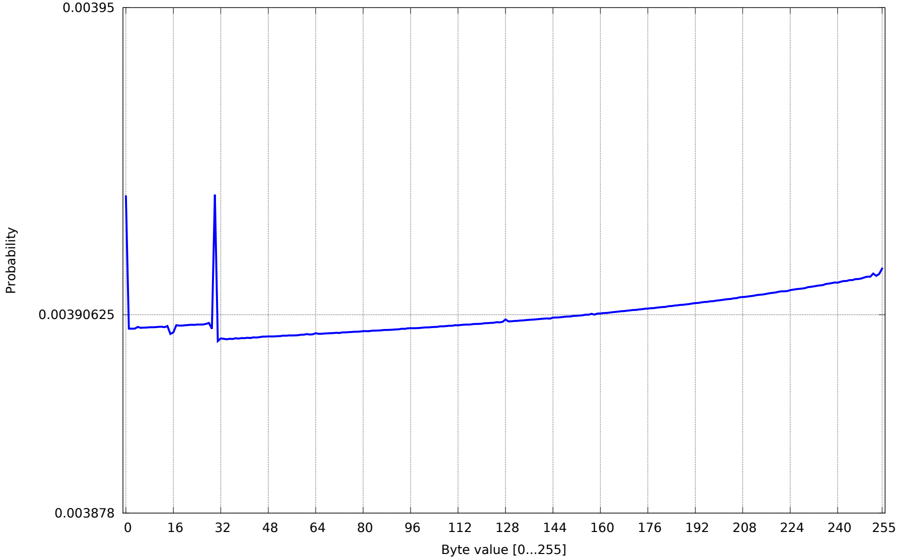
Keystream distribution at position 28



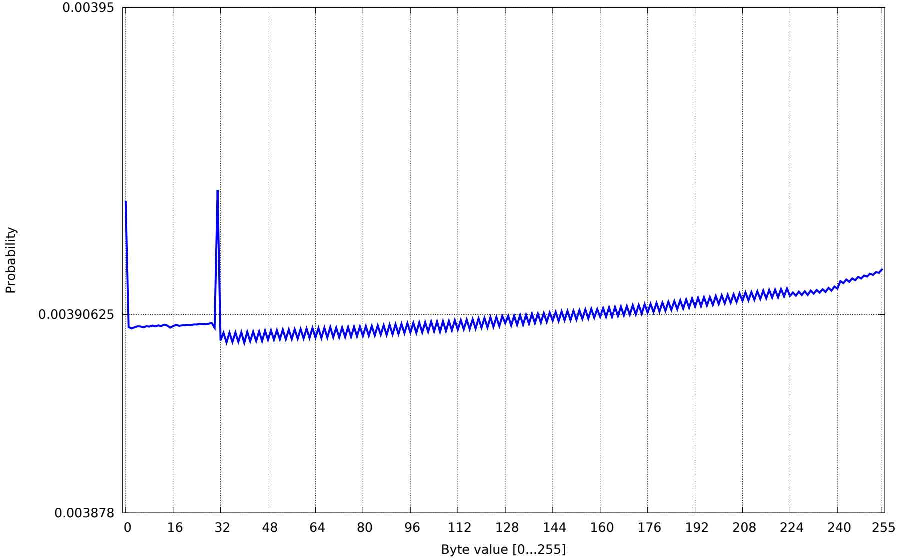
Keystream distribution at position 29



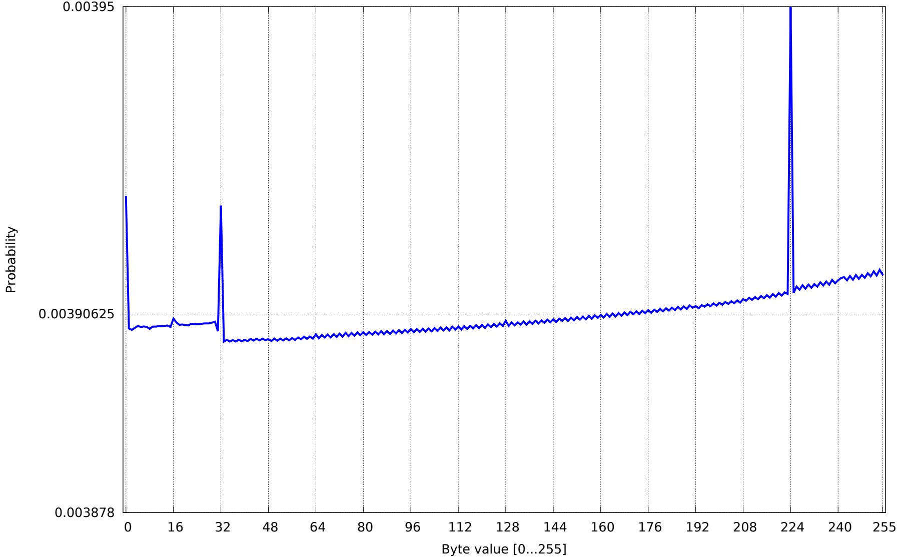
Keystream distribution at position 30



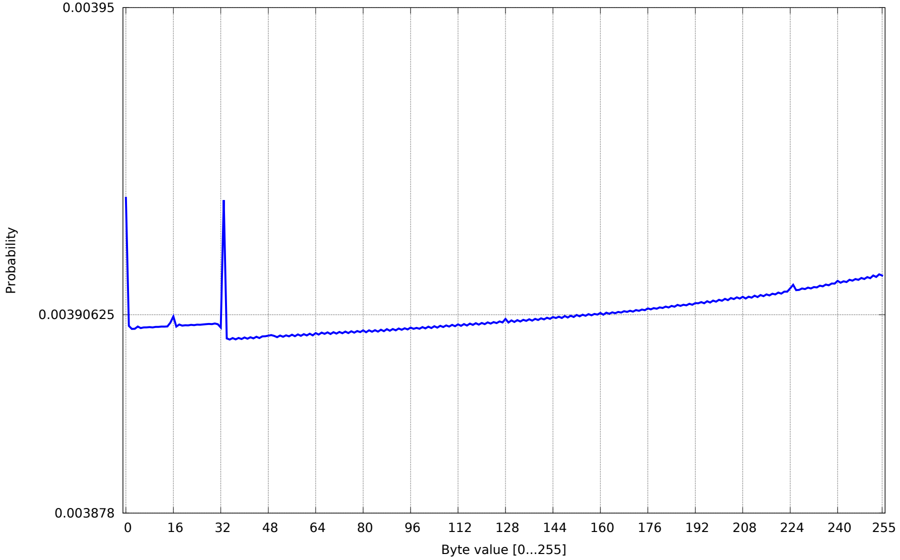
Keystream distribution at position 31



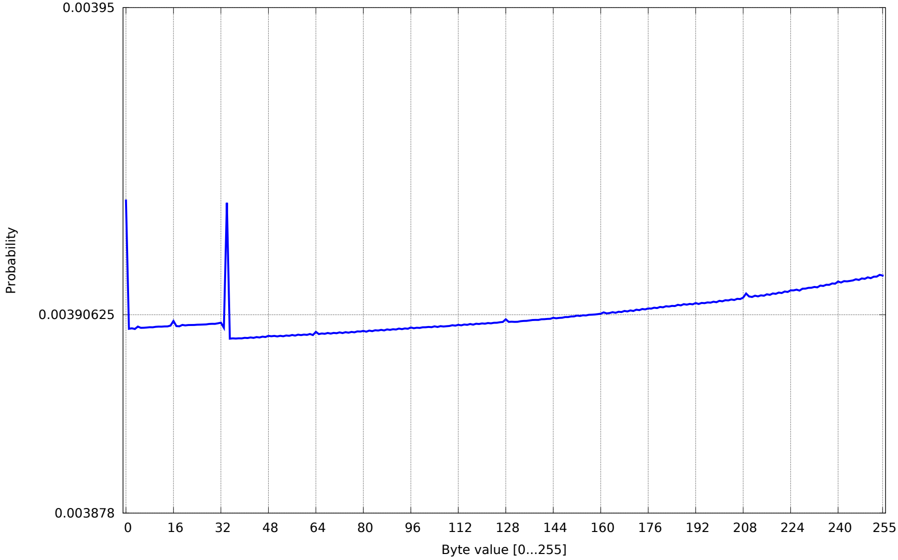
Keystream distribution at position 32



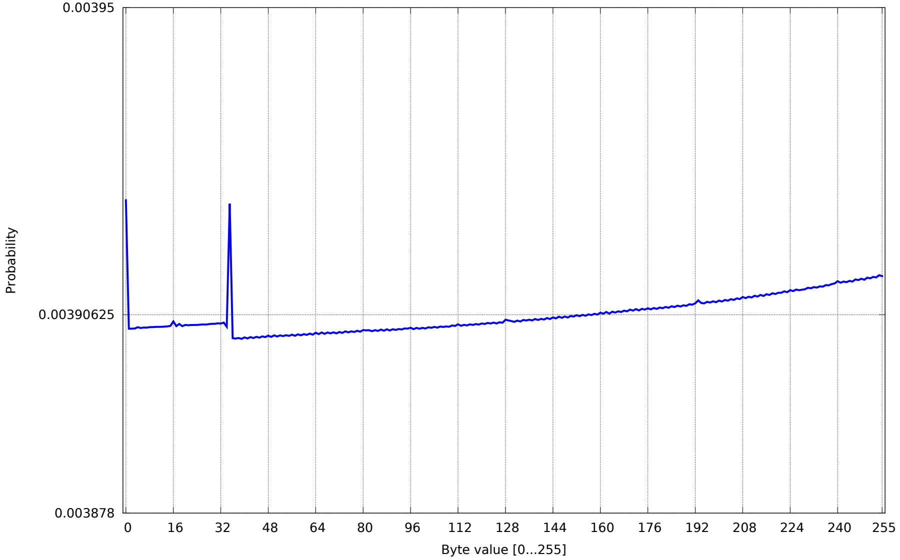
Keystream distribution at position 33



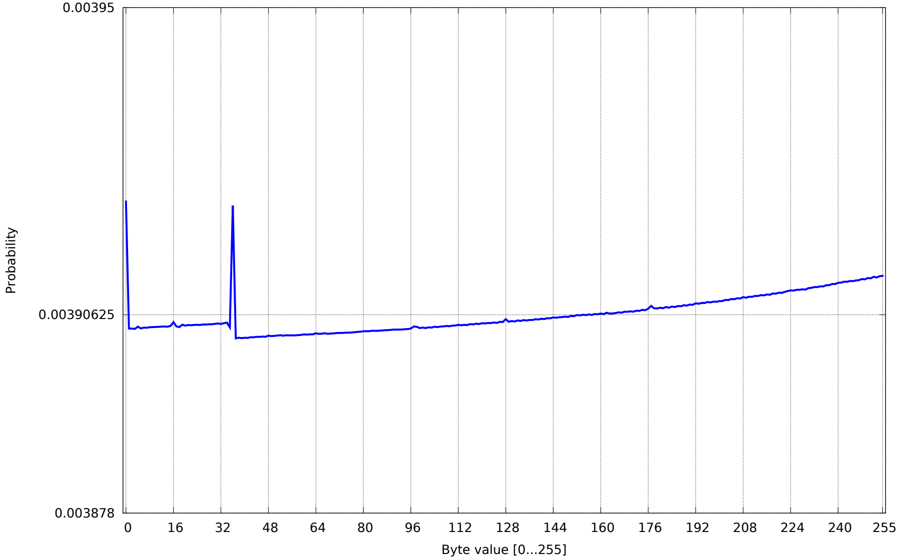
Keystream distribution at position 34



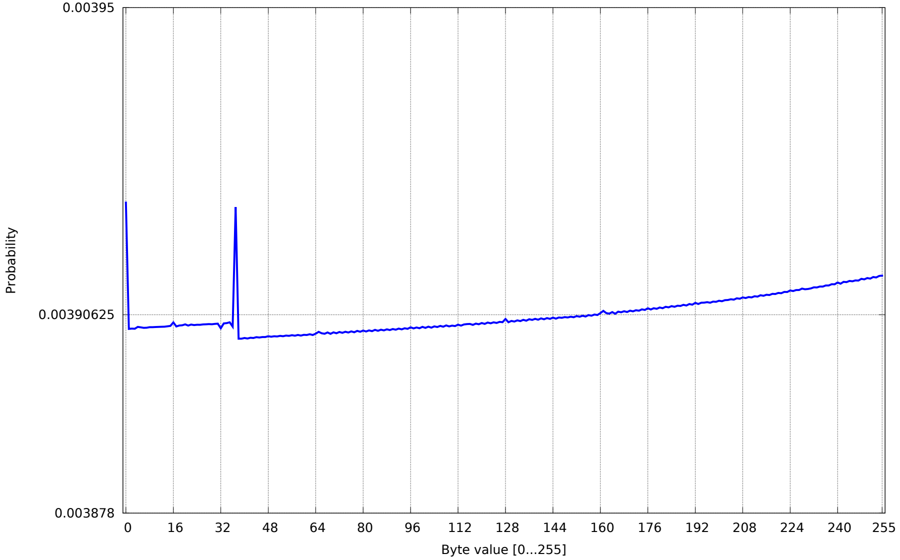
Keystream distribution at position 35



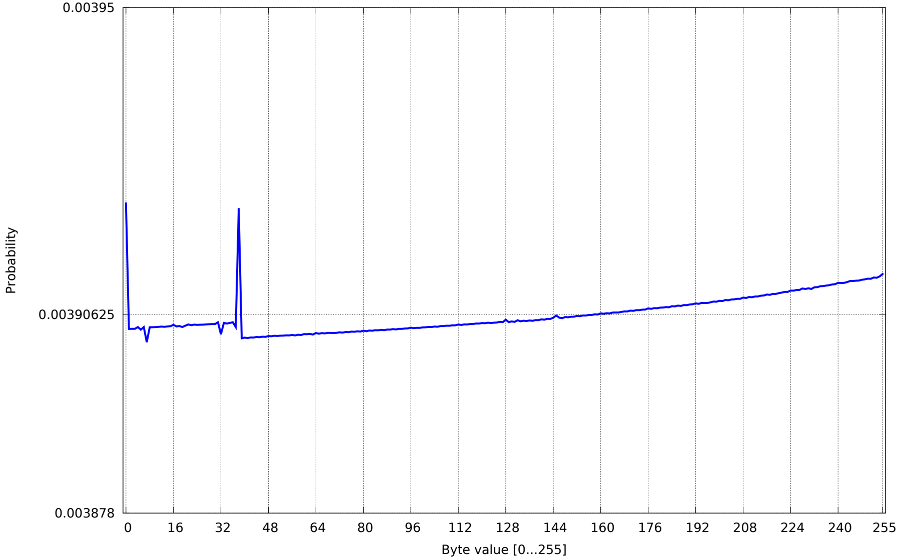
Keystream distribution at position 36



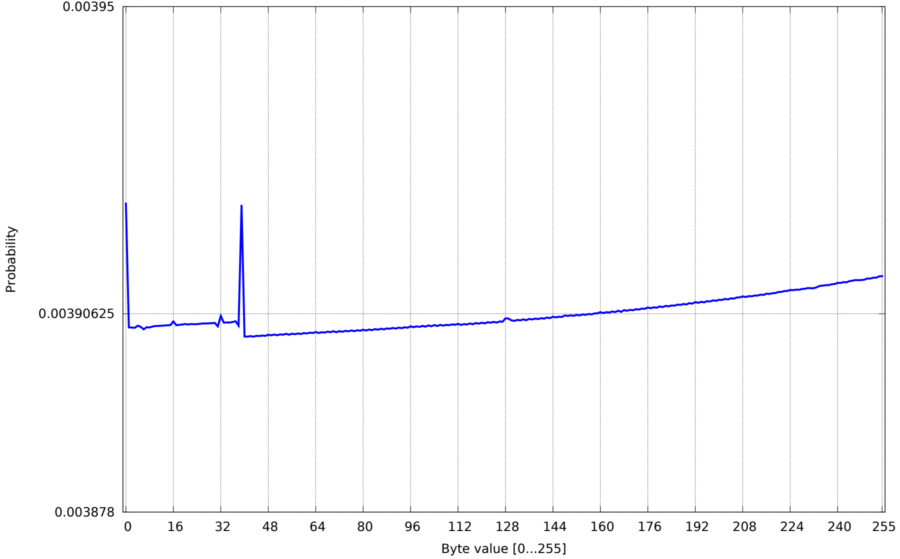
Keystream distribution at position 37



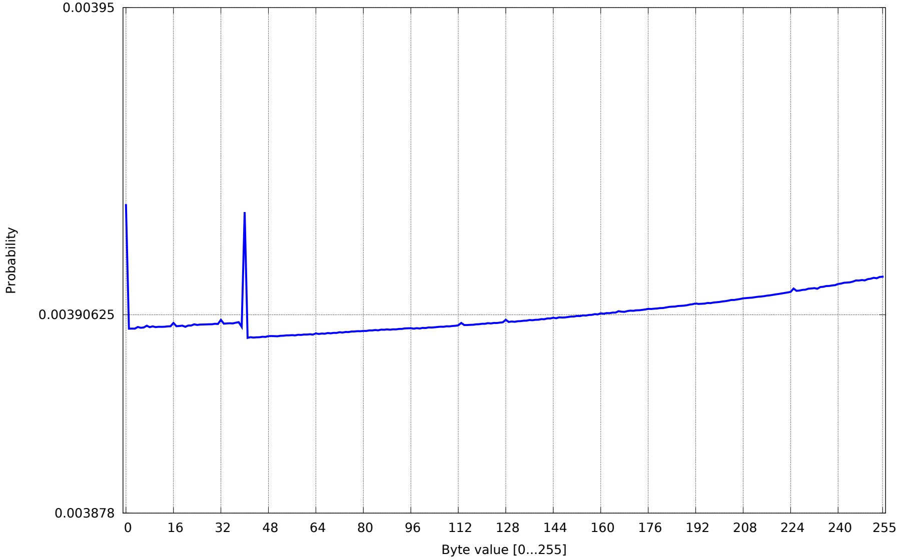
Keystream distribution at position 38



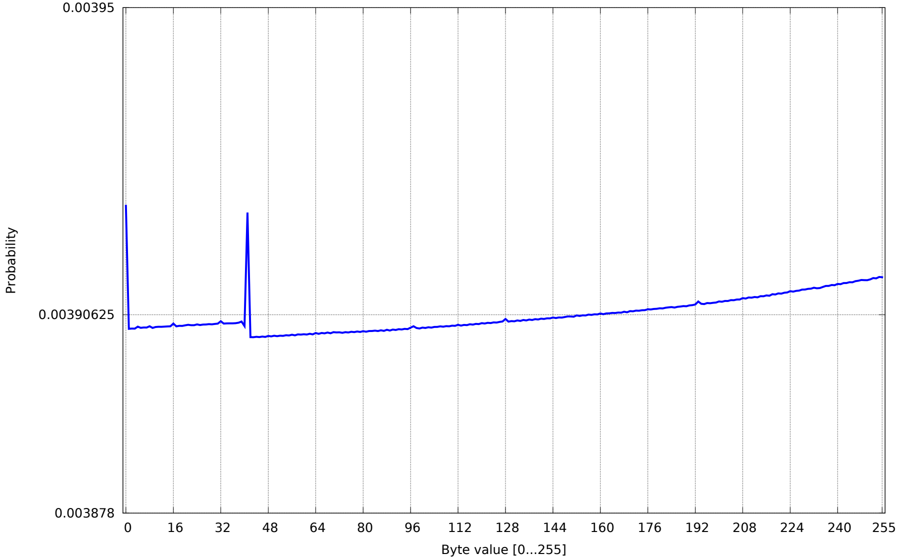
Keystream distribution at position 39



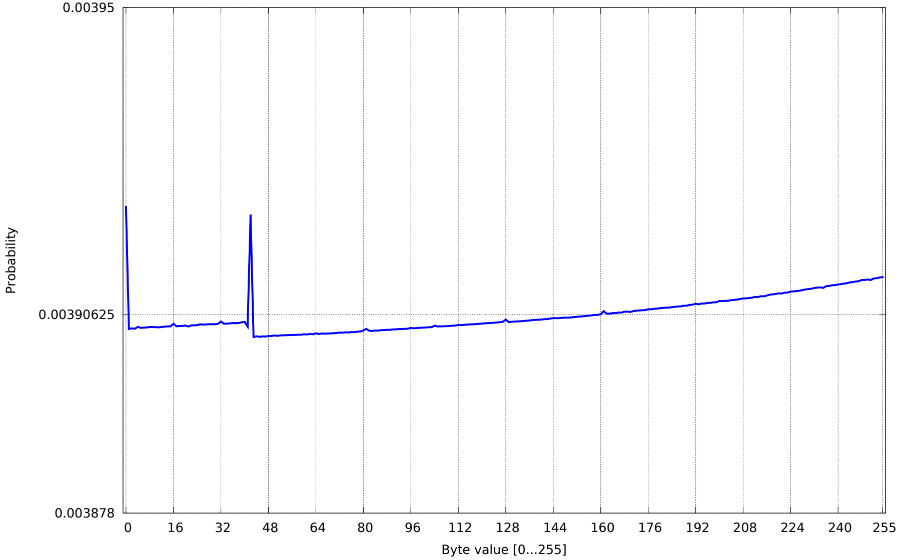
Keystream distribution at position 40



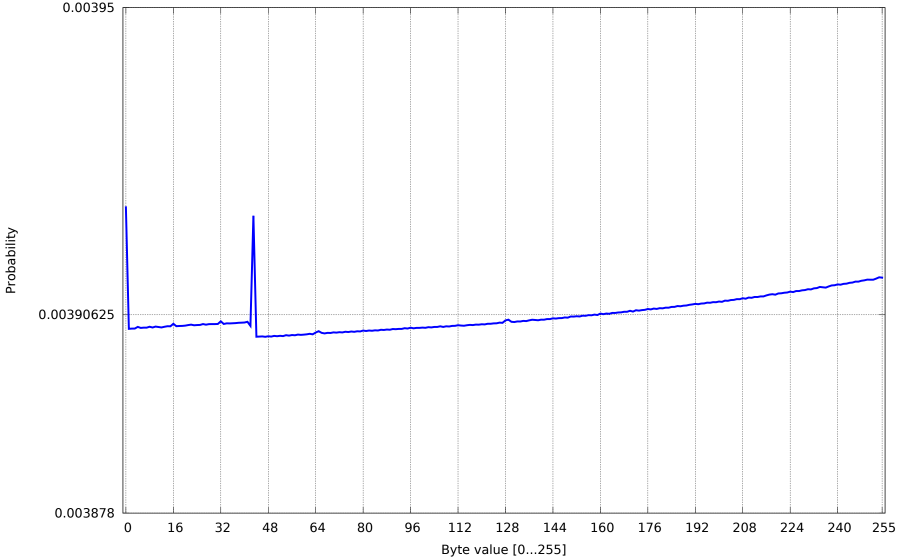
Keystream distribution at position 41



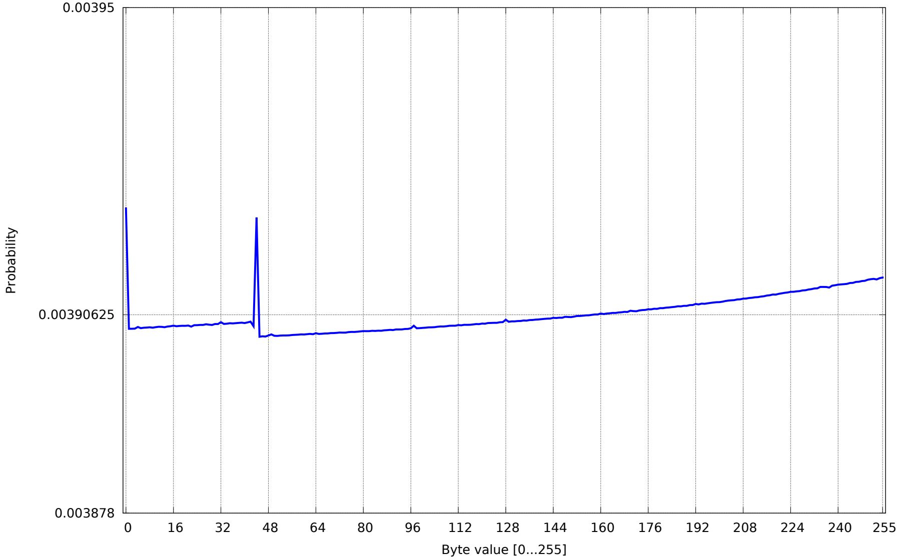
Keystream distribution at position 42



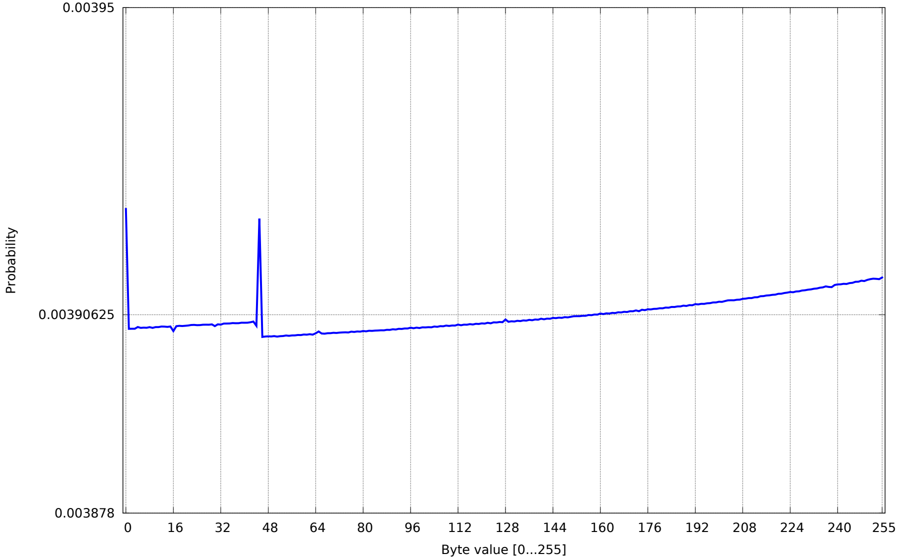
Keystream distribution at position 43



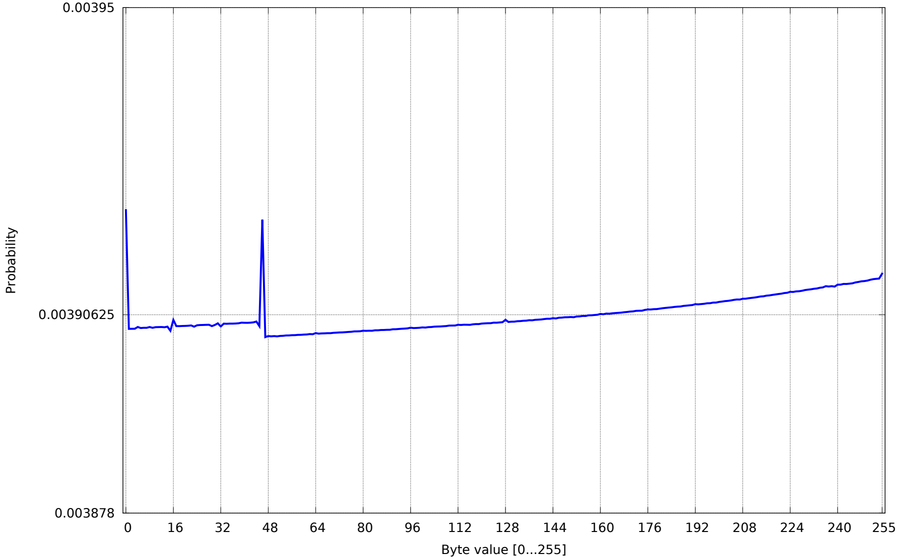
Keystream distribution at position 44



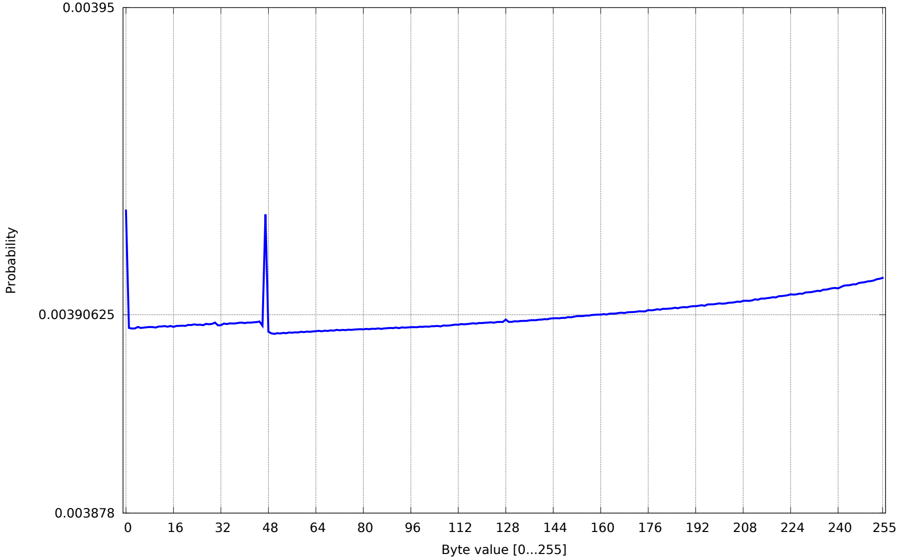
Keystream distribution at position 45



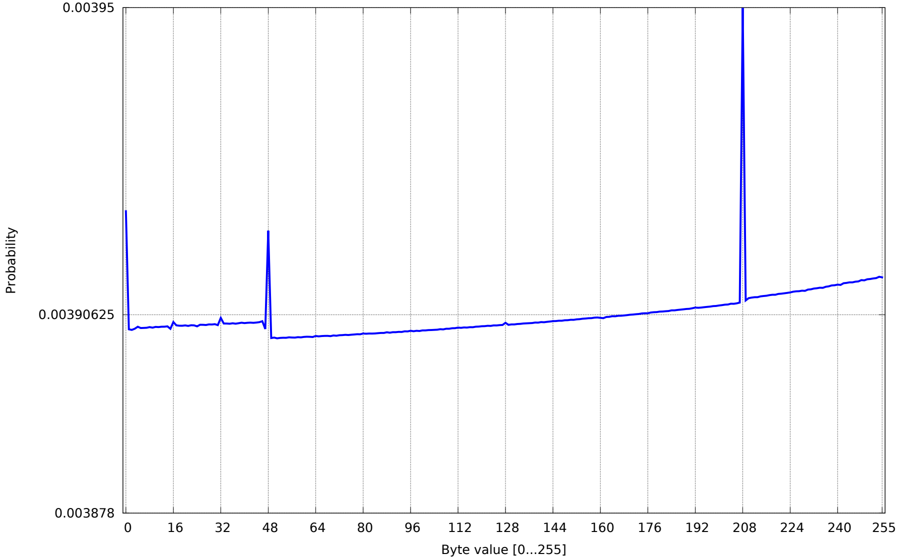
Keystream distribution at position 46



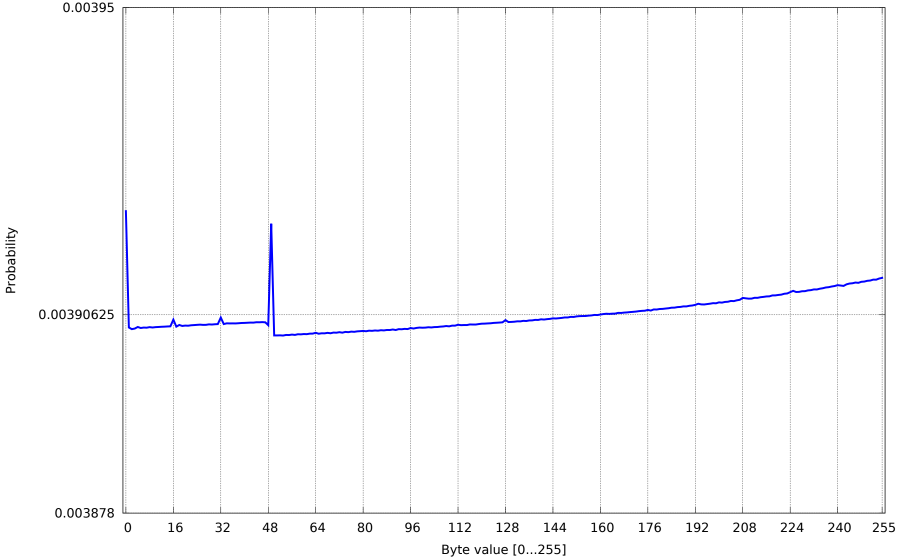
Keystream distribution at position 47



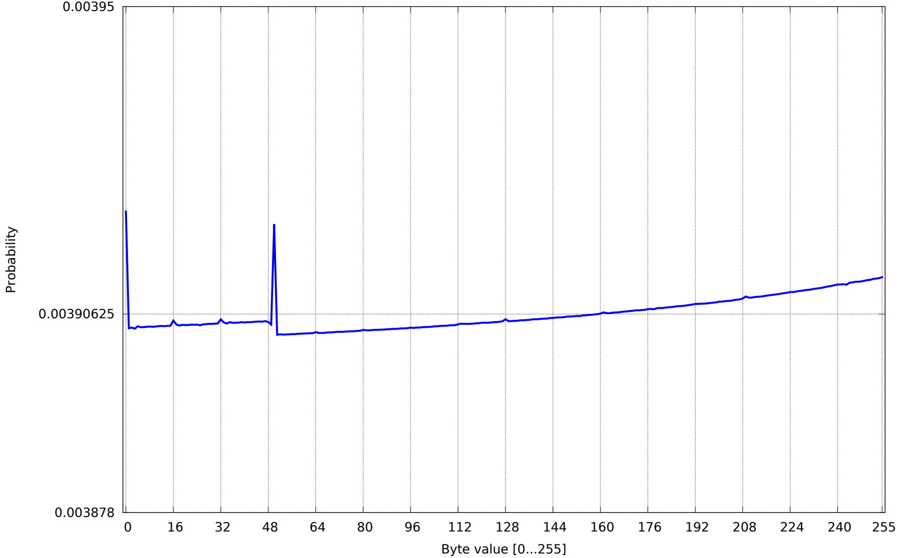
Keystream distribution at position 48



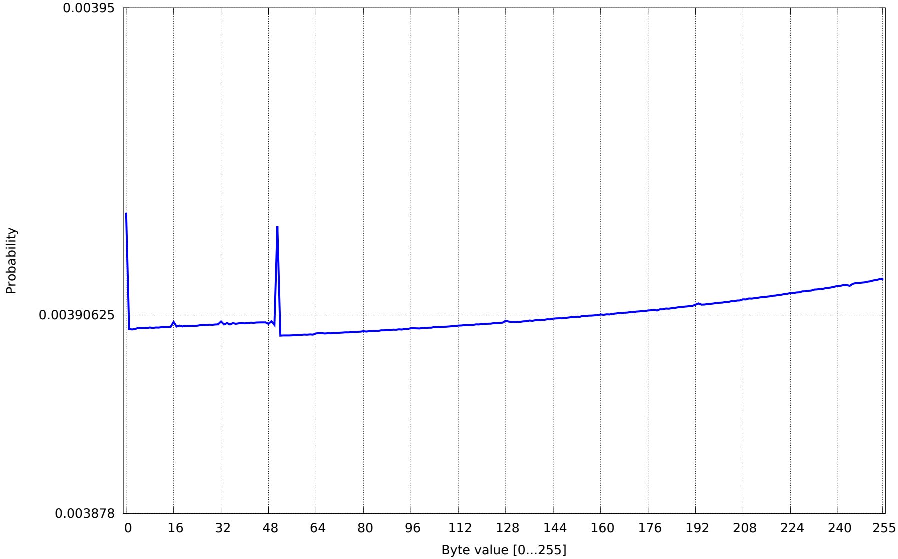
Keystream distribution at position 49



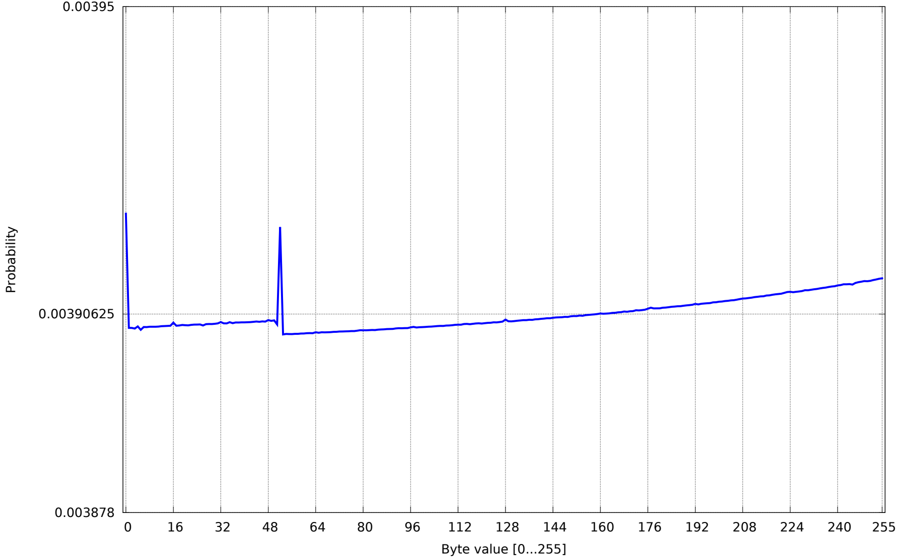
Keystream distribution at position 50



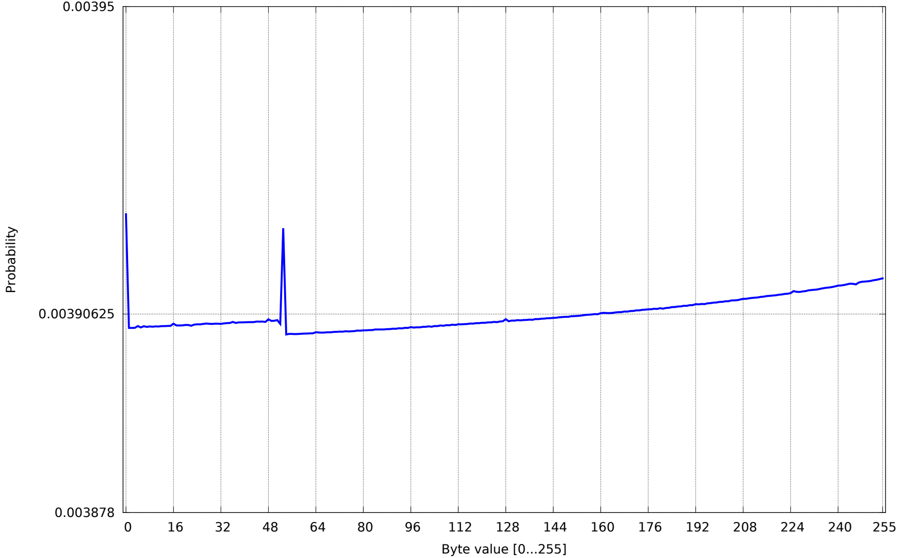
Keystream distribution at position 51



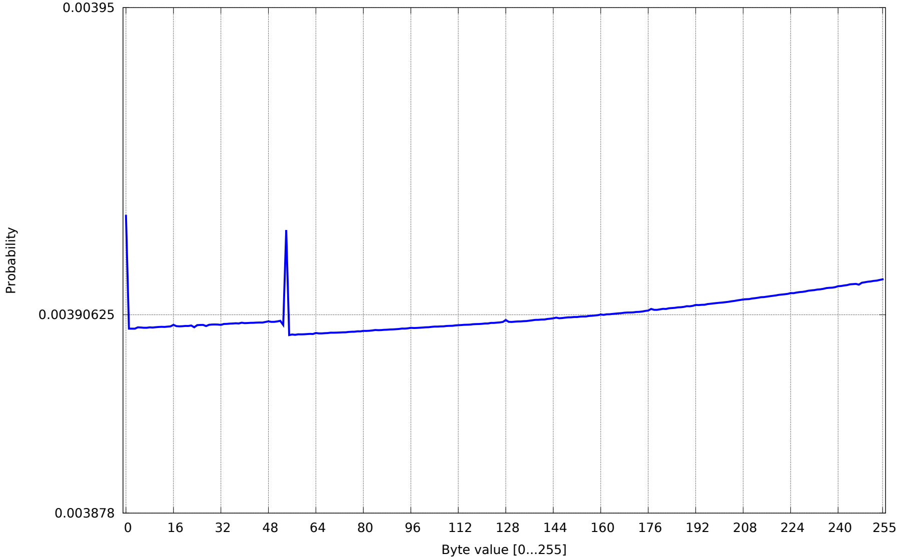
Keystream distribution at position 52



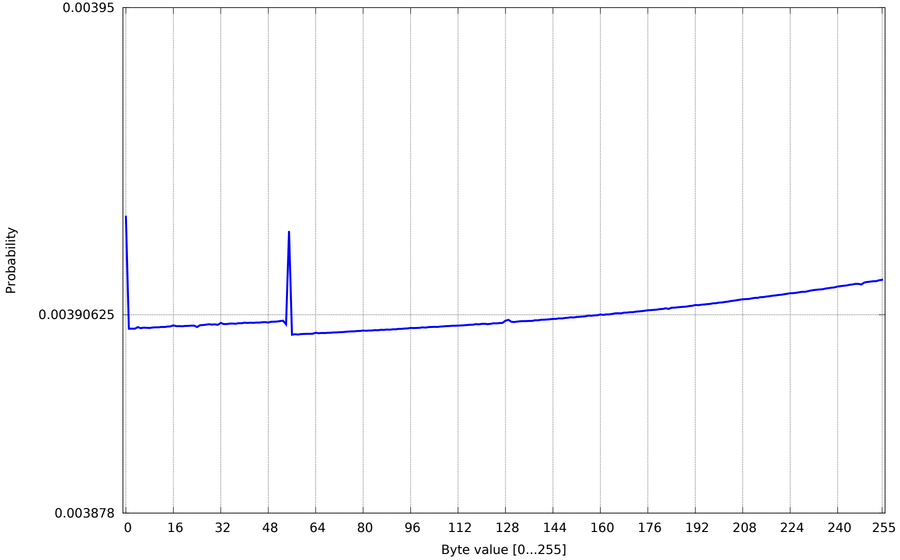
Keystream distribution at position 53



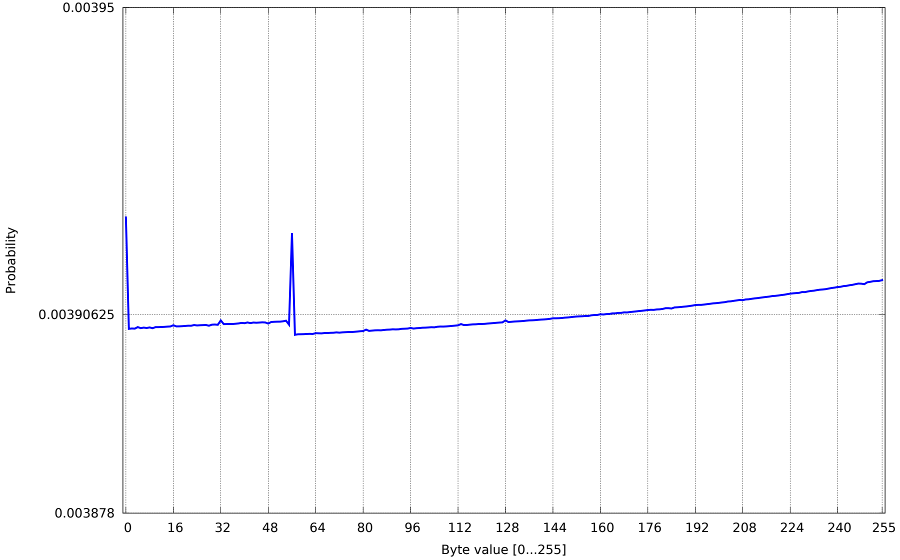
Keystream distribution at position 54



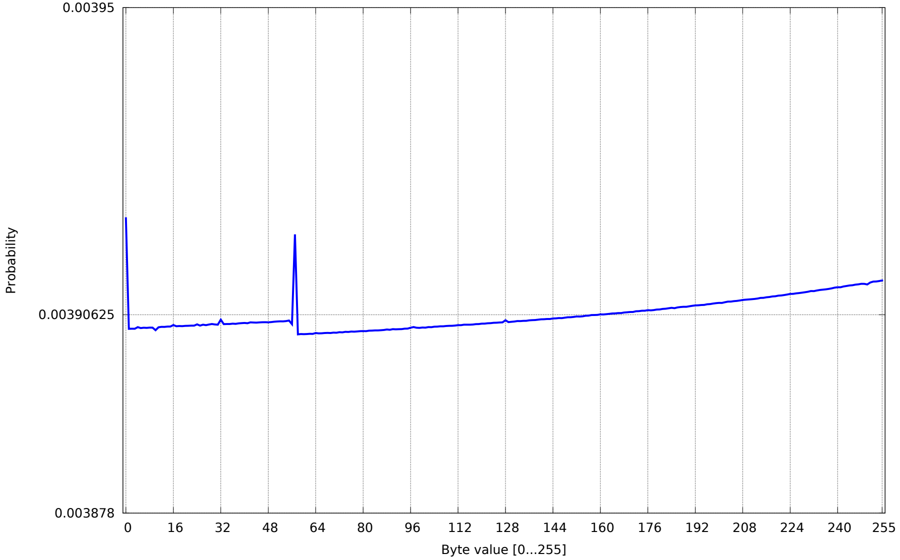
Keystream distribution at position 55



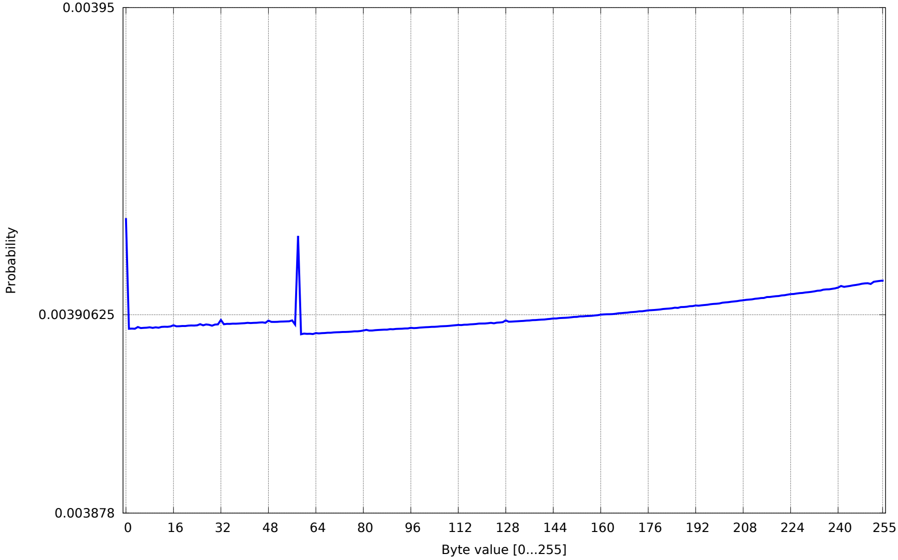
Keystream distribution at position 56



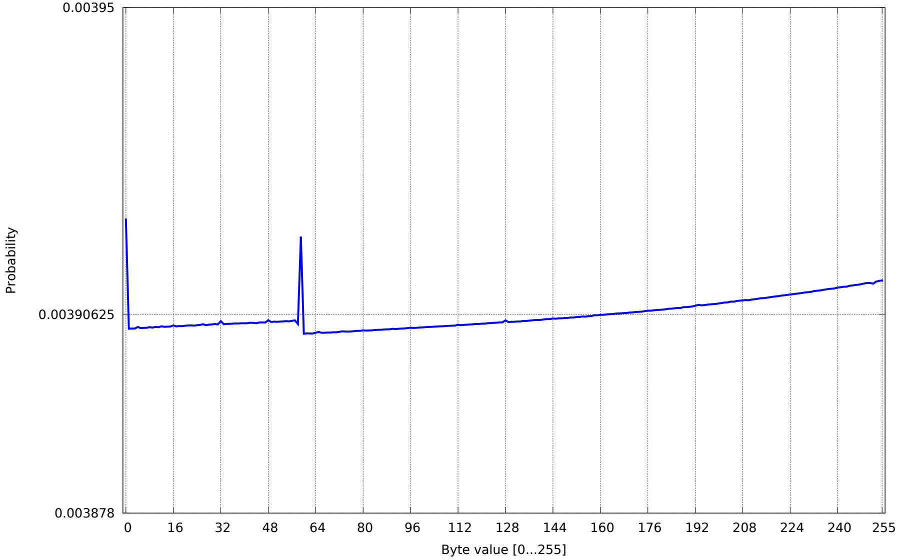
Keystream distribution at position 57



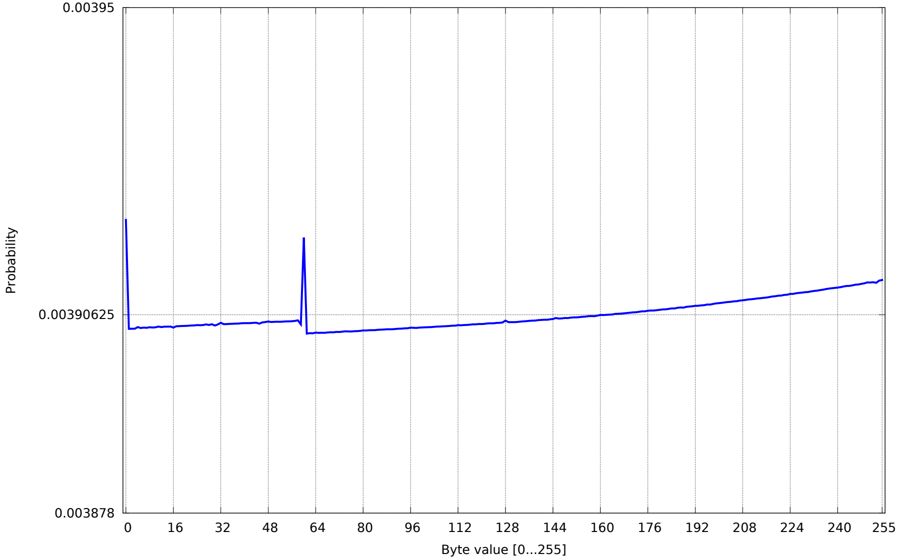
Keystream distribution at position 58



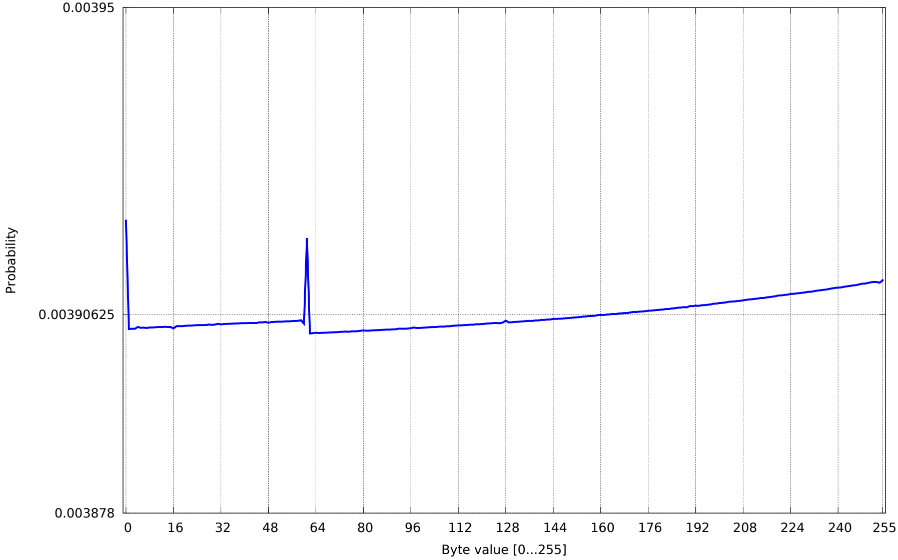
Keystream distribution at position 59



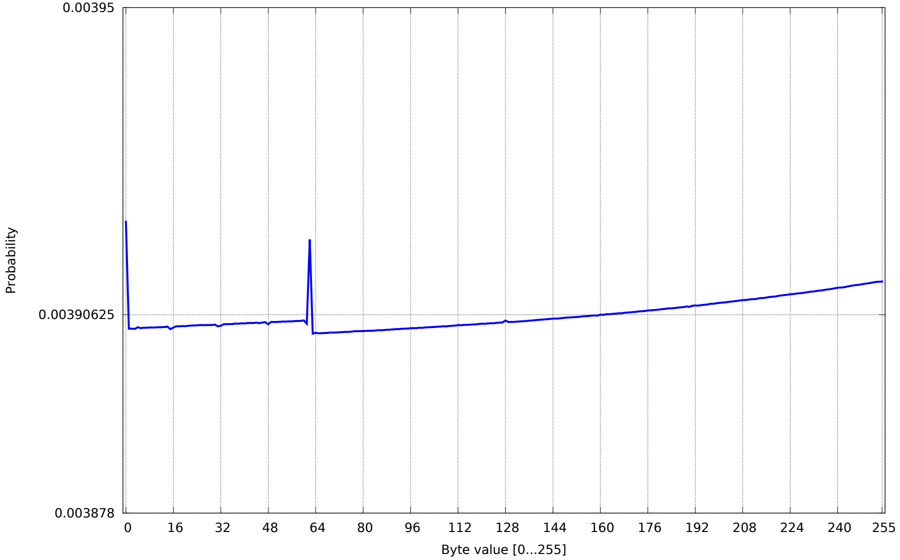
Keystream distribution at position 60



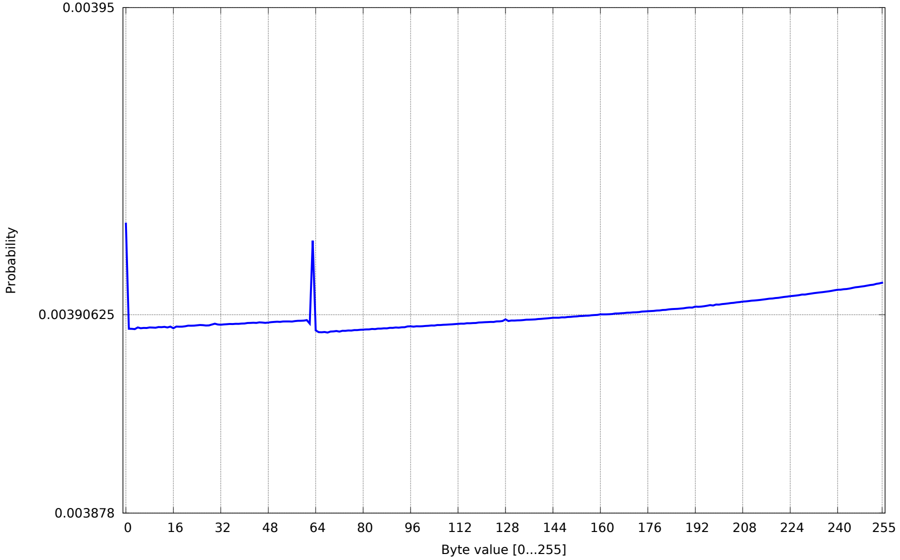
Keystream distribution at position 61



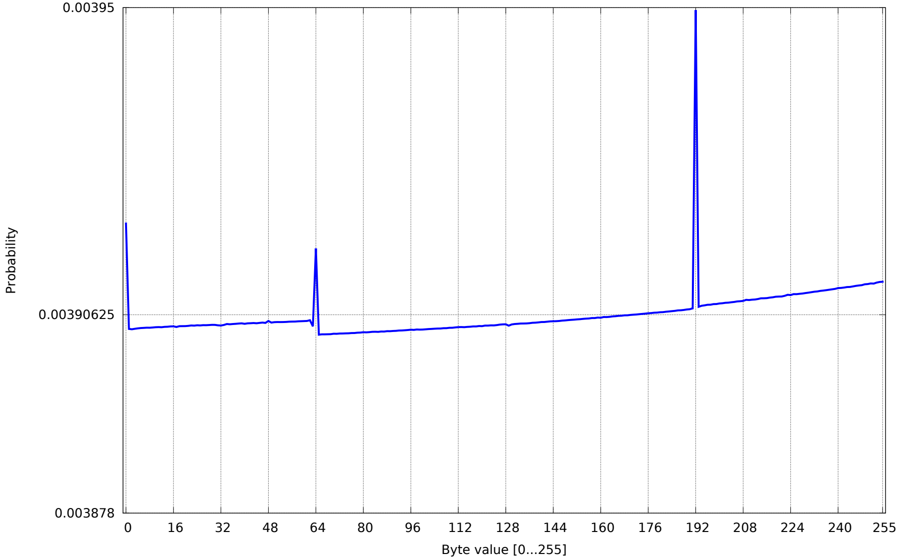
Keystream distribution at position 62



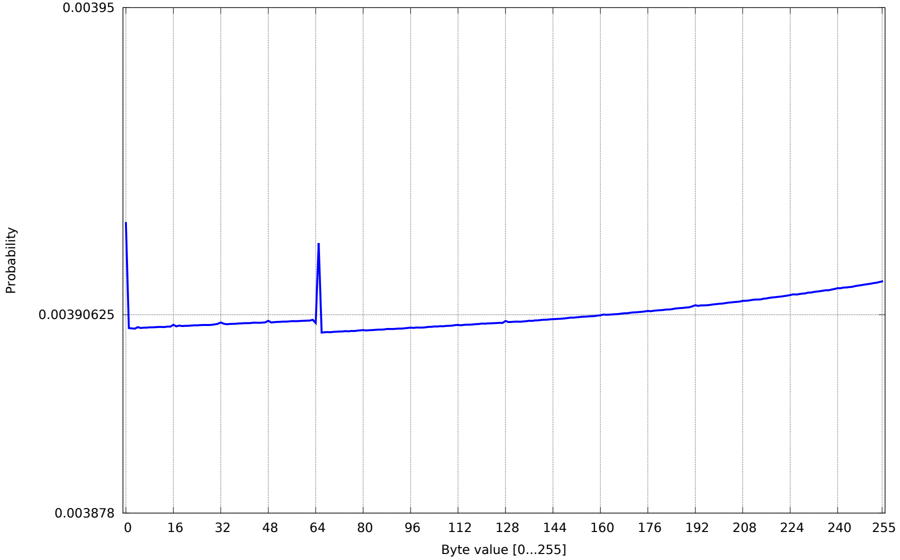
Keystream distribution at position 63



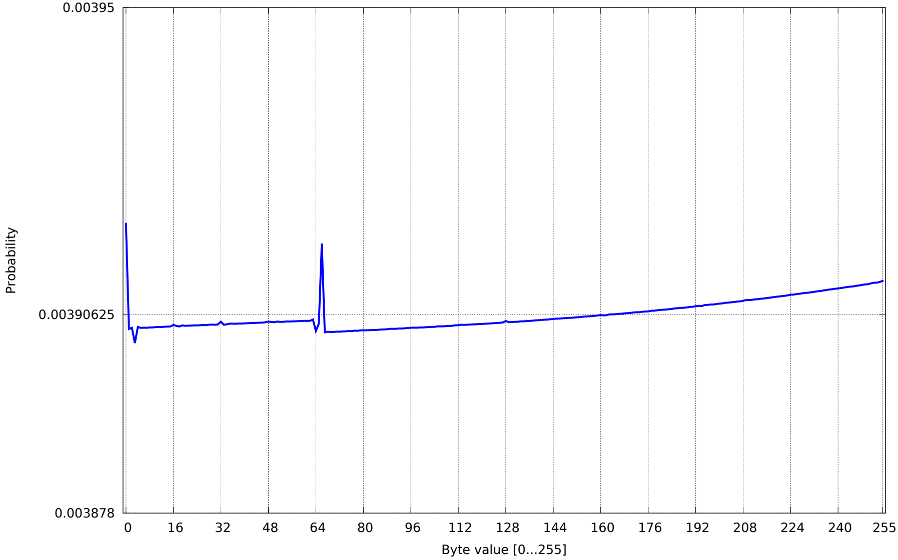
Keystream distribution at position 64



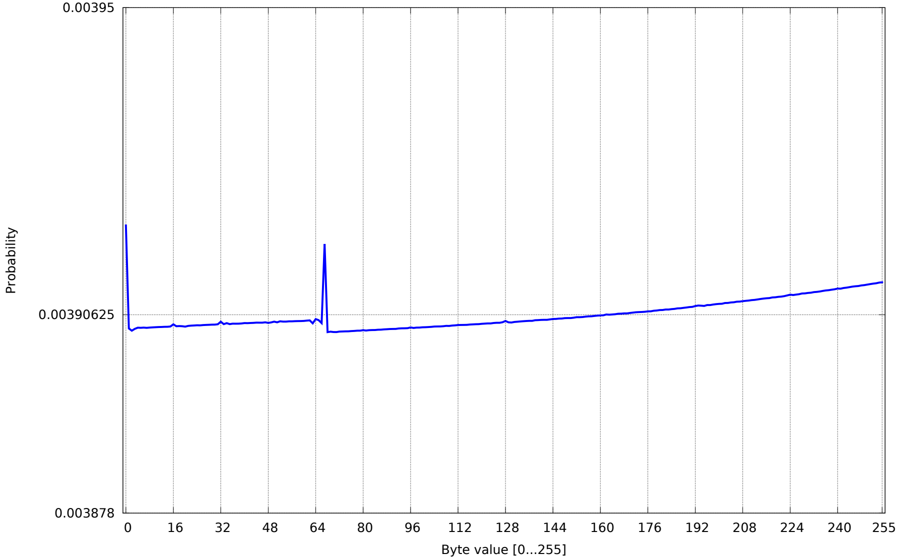
Keystream distribution at position 65



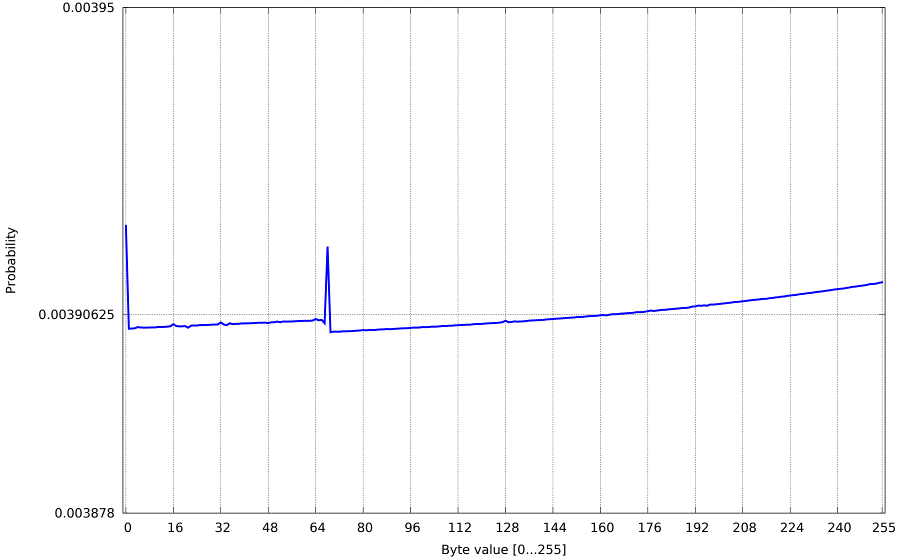
Keystream distribution at position 66



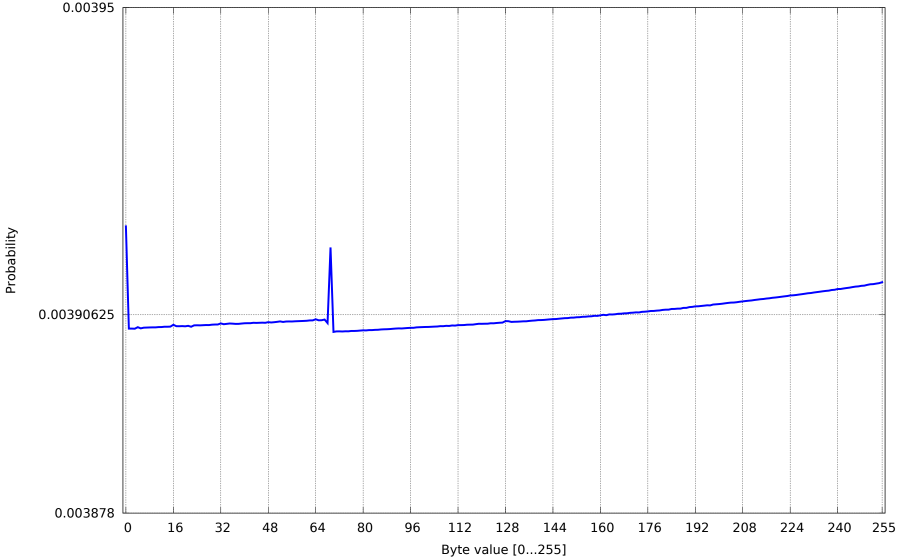
Keystream distribution at position 67



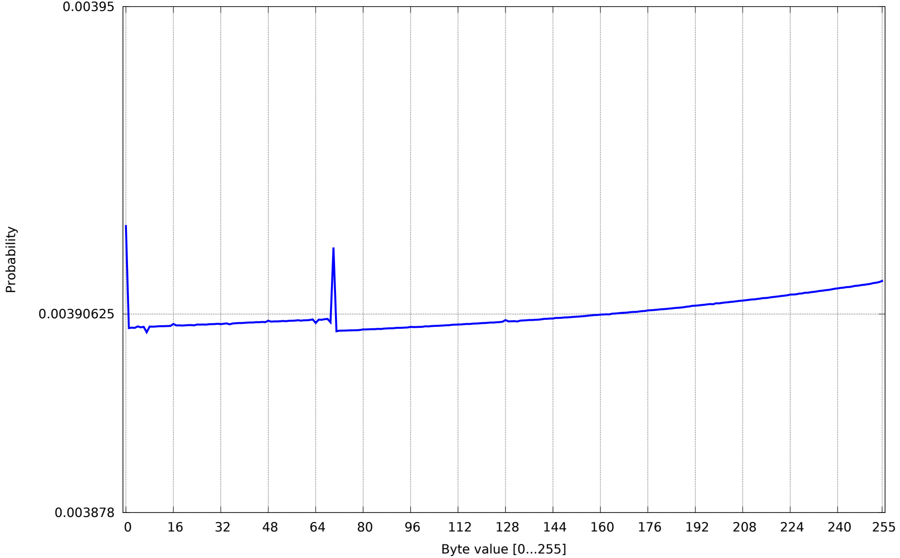
Keystream distribution at position 68



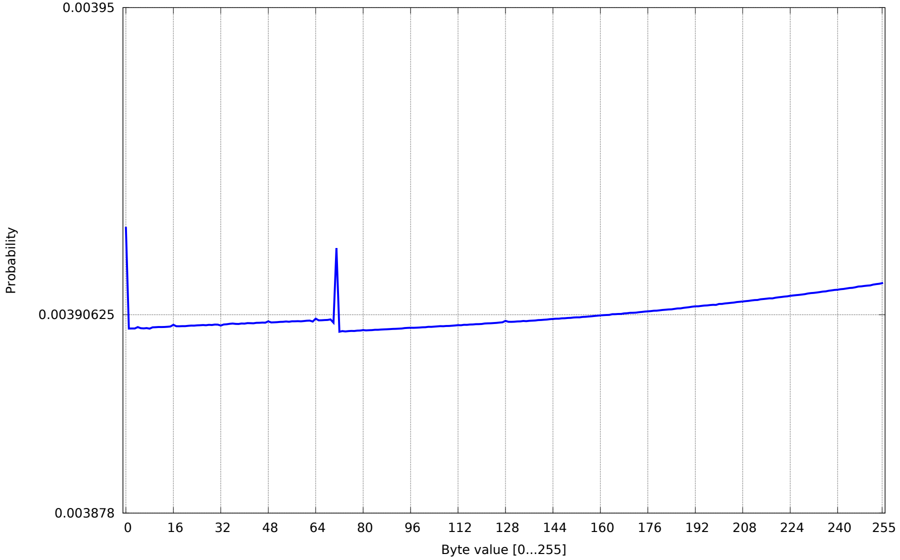
Keystream distribution at position 69



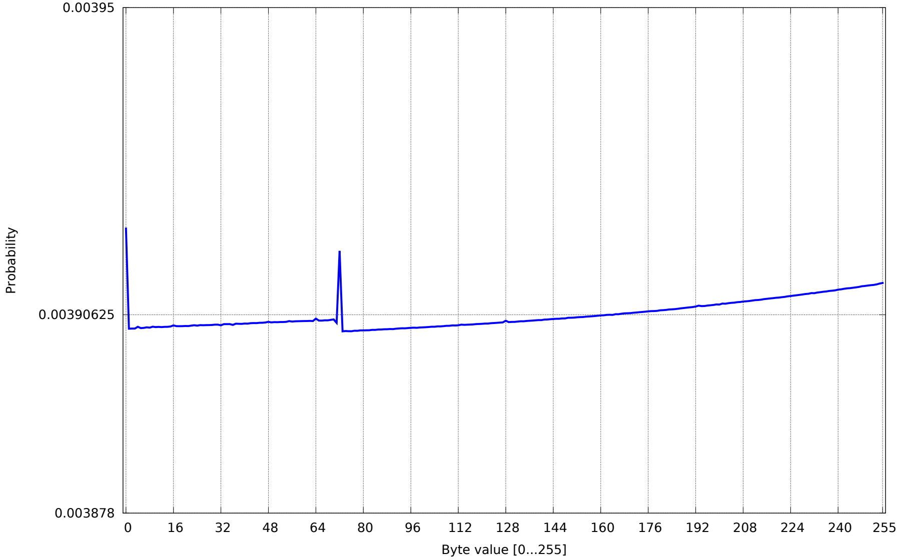
Keystream distribution at position 70



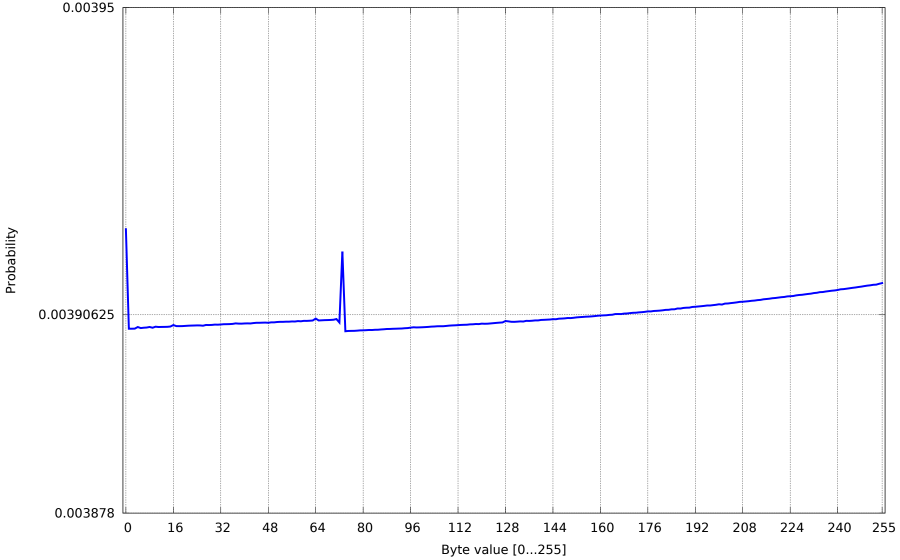
Keystream distribution at position 71



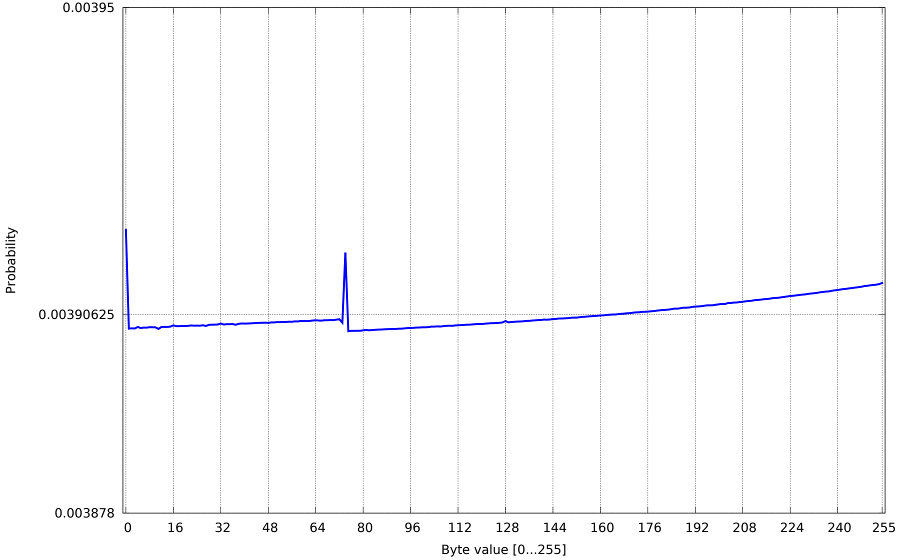
Keystream distribution at position 72



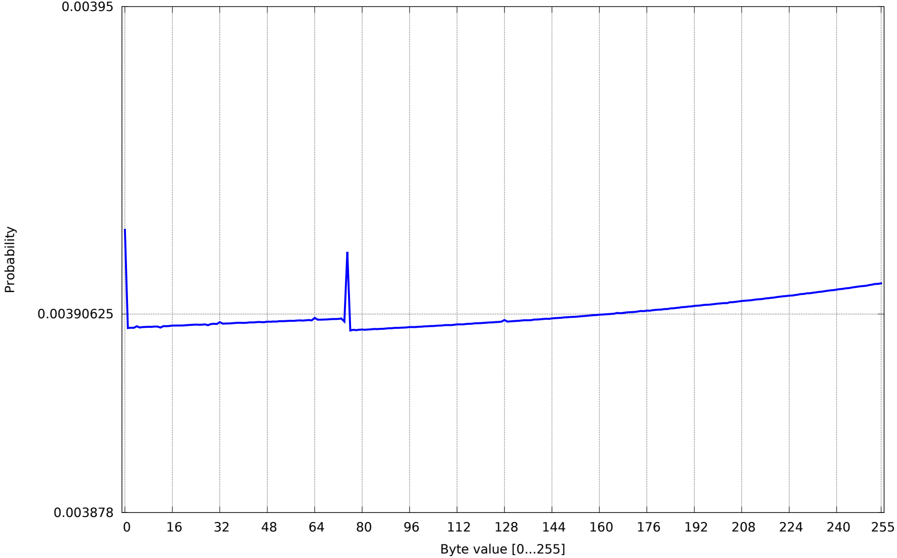
Keystream distribution at position 73



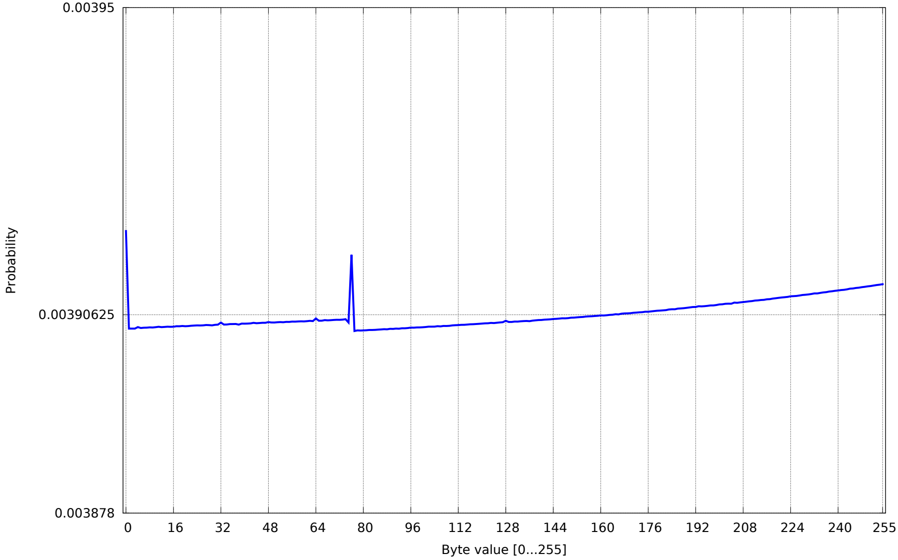
Keystream distribution at position 74



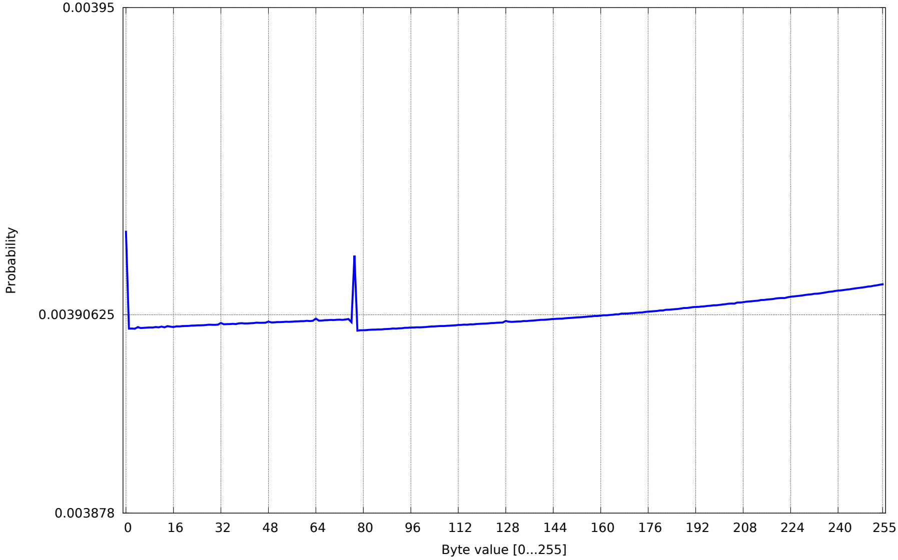
Keystream distribution at position 75



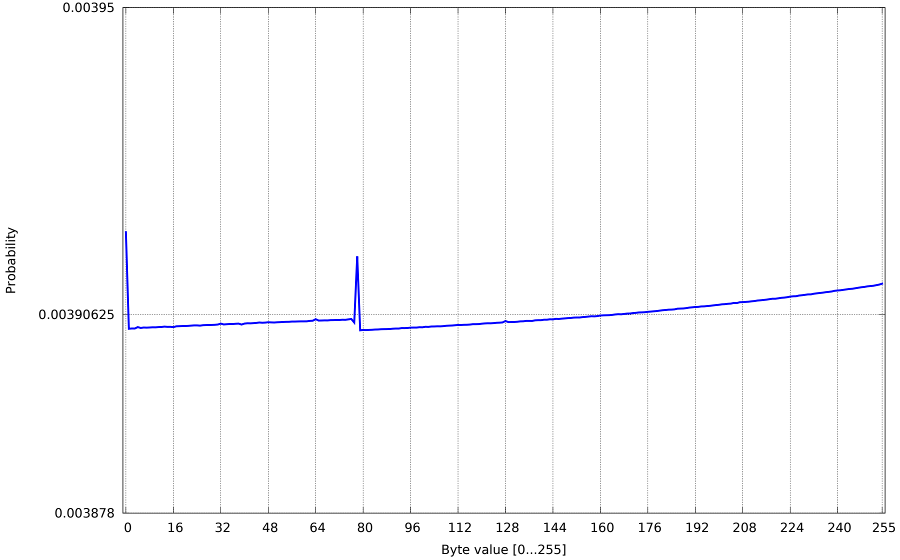
Keystream distribution at position 76



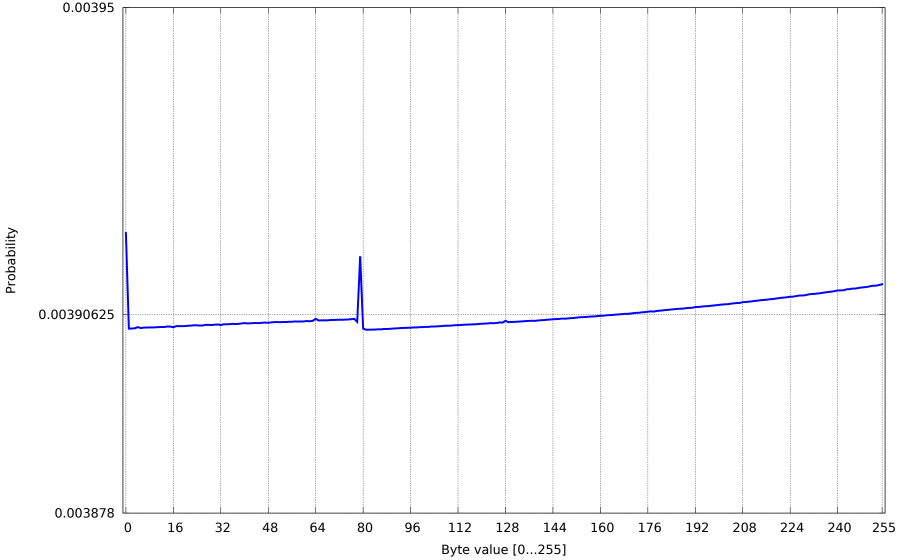
Keystream distribution at position 77



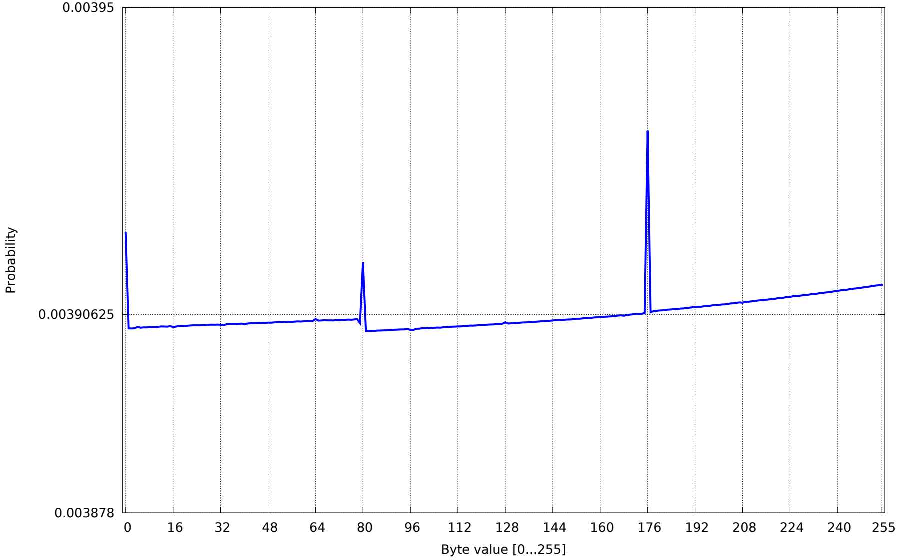
Keystream distribution at position 78



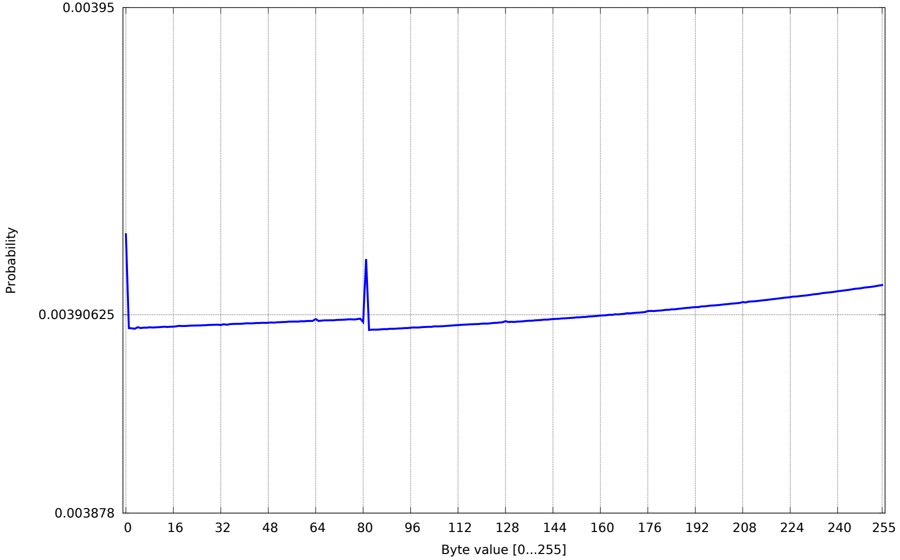
Keystream distribution at position 79



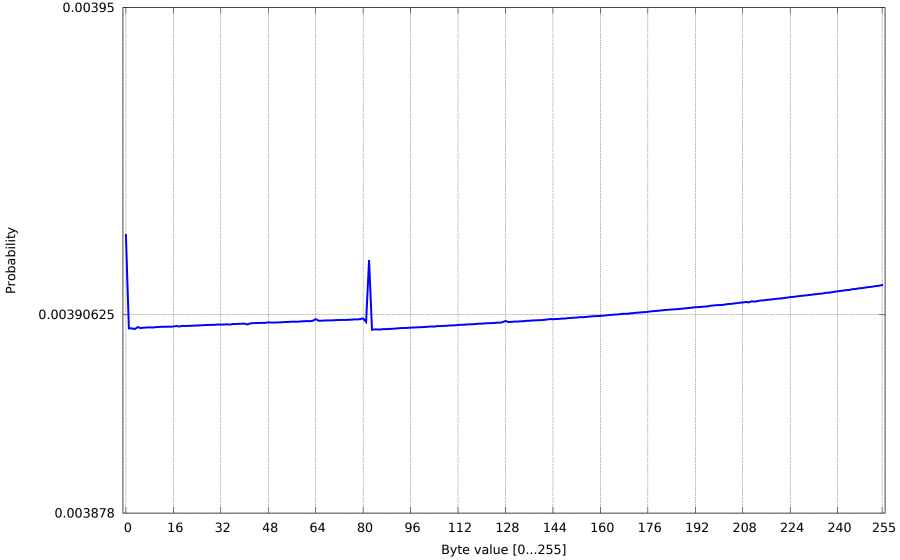
Keystream distribution at position 80



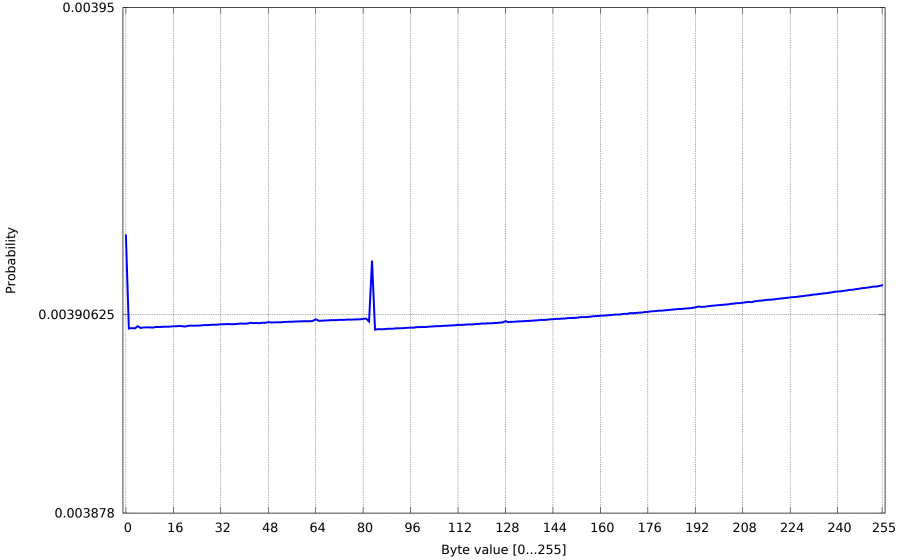
Keystream distribution at position 81



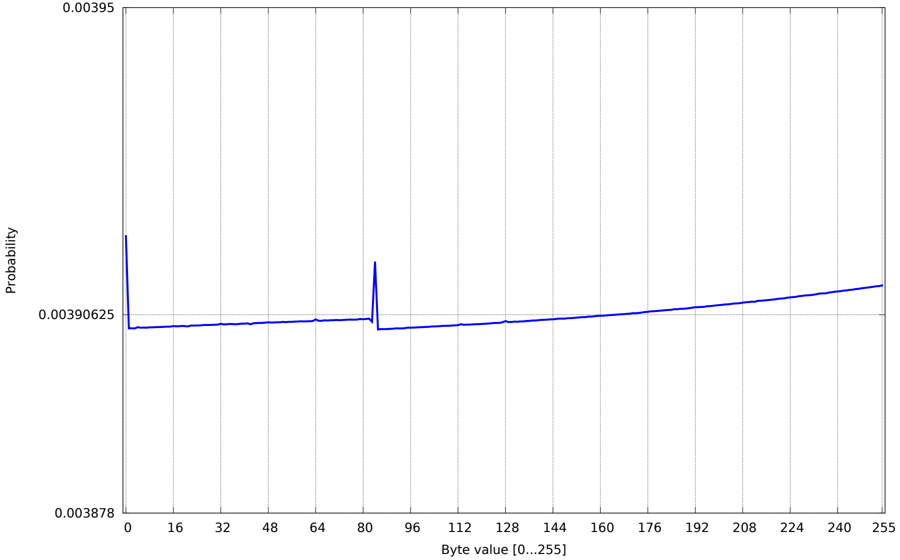
Keystream distribution at position 82



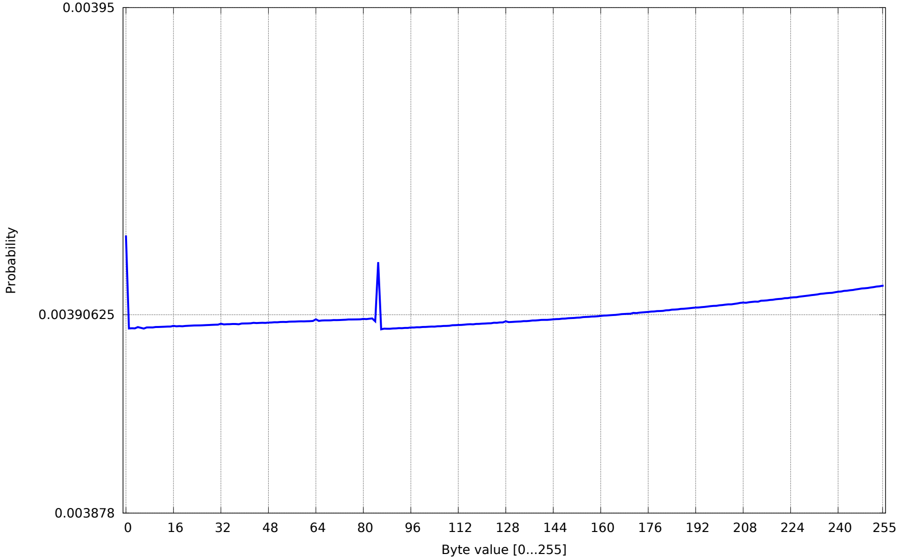
Keystream distribution at position 83



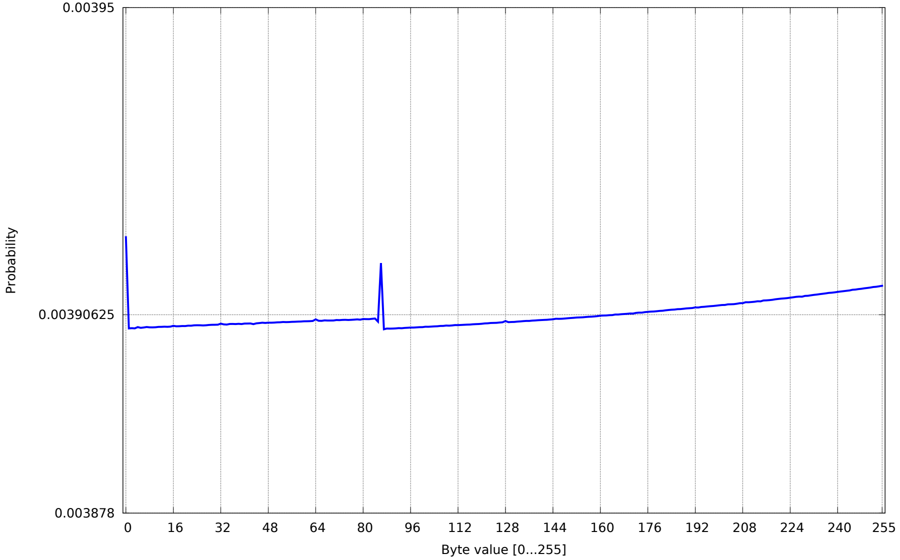
Keystream distribution at position 84



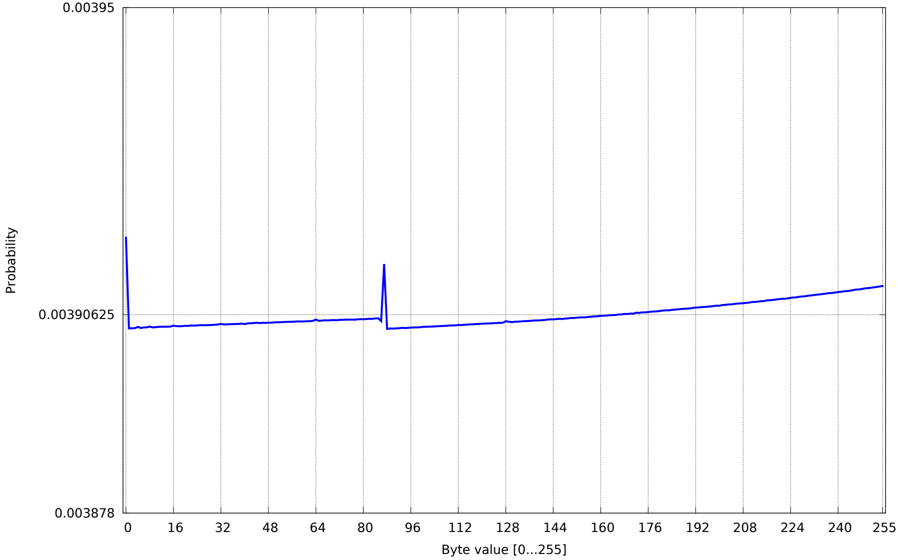
Keystream distribution at position 85



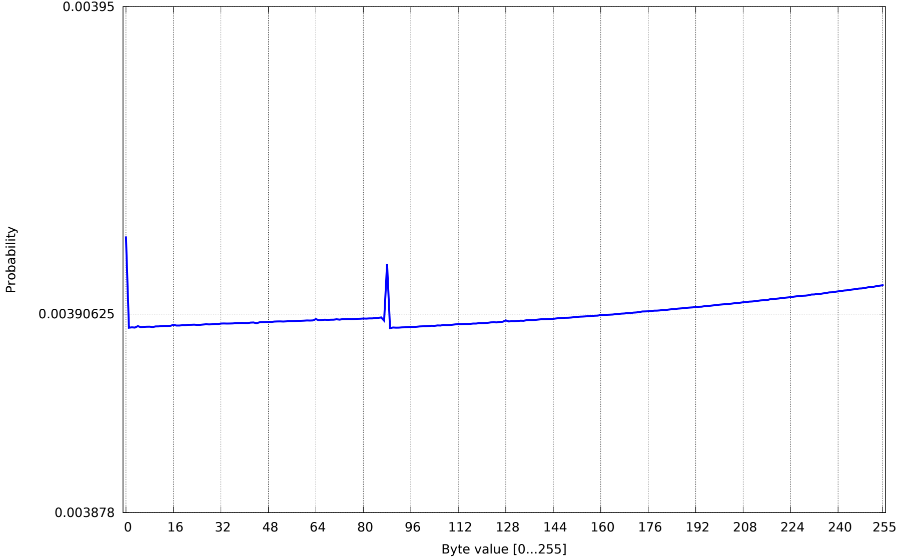
Keystream distribution at position 86



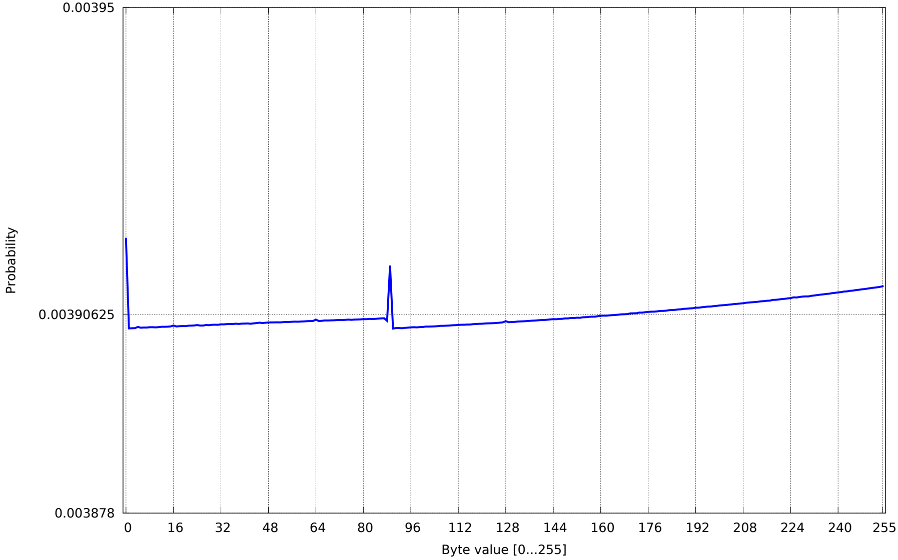
Keystream distribution at position 87



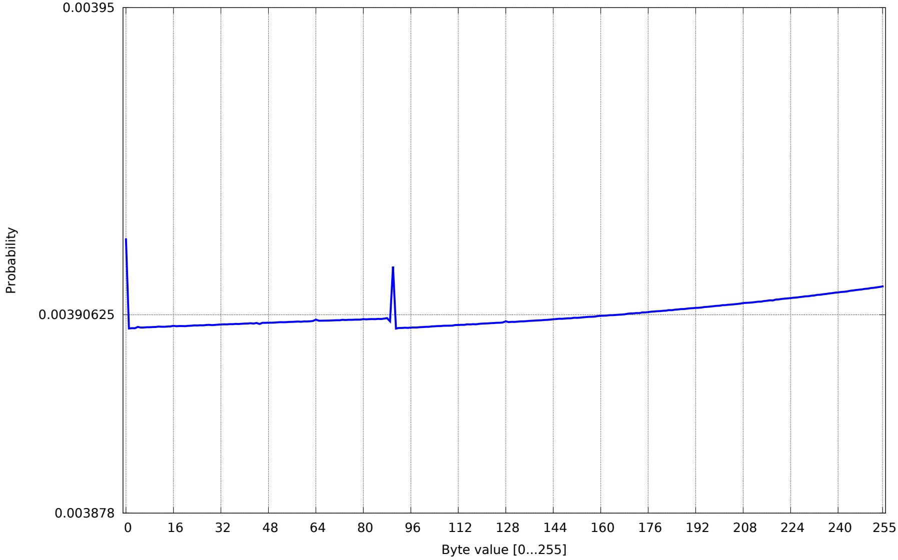
Keystream distribution at position 88



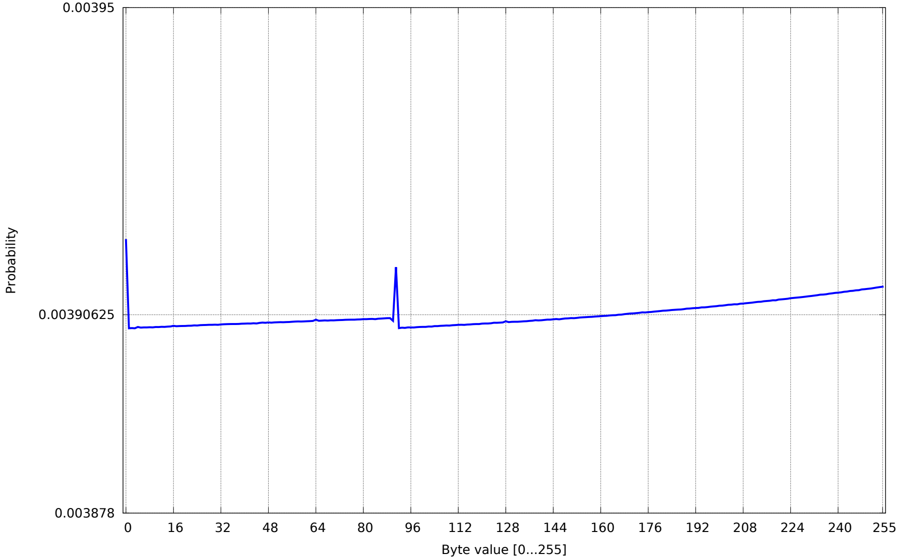
Keystream distribution at position 89



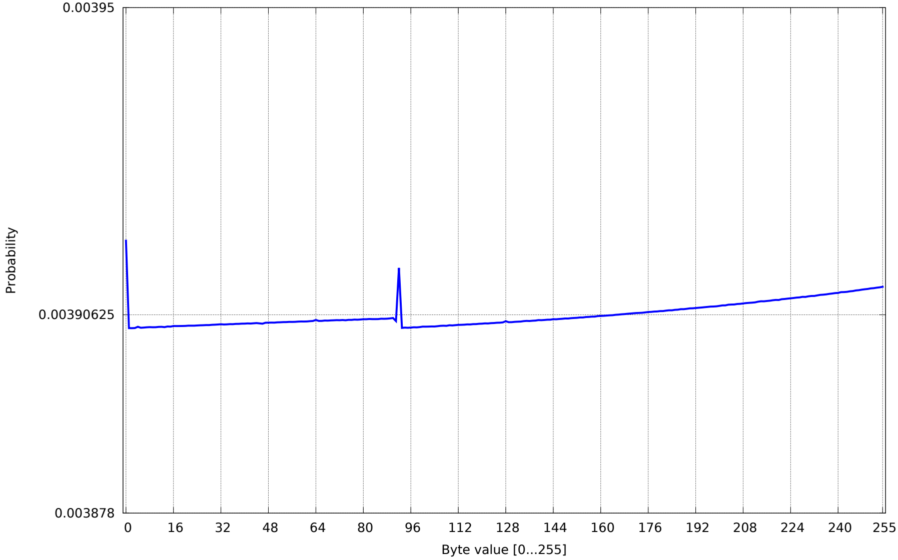
Keystream distribution at position 90



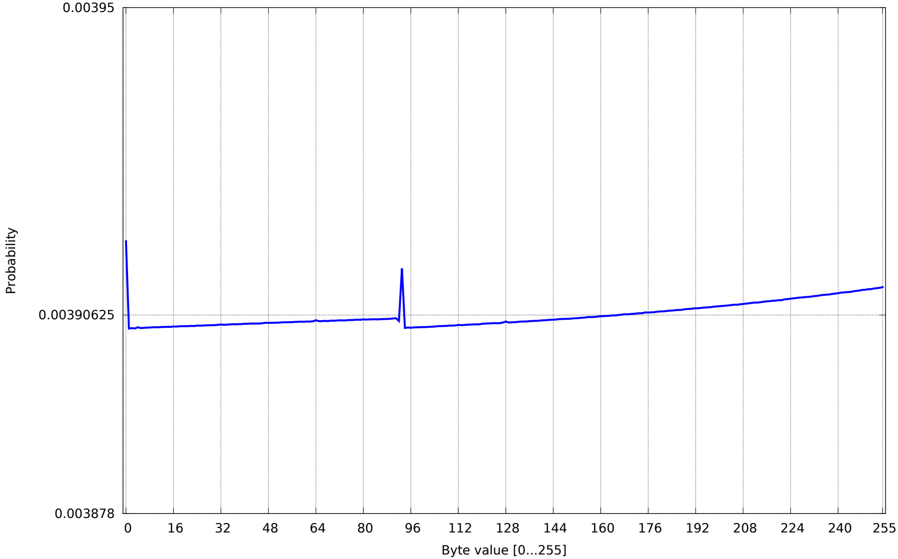
Keystream distribution at position 91



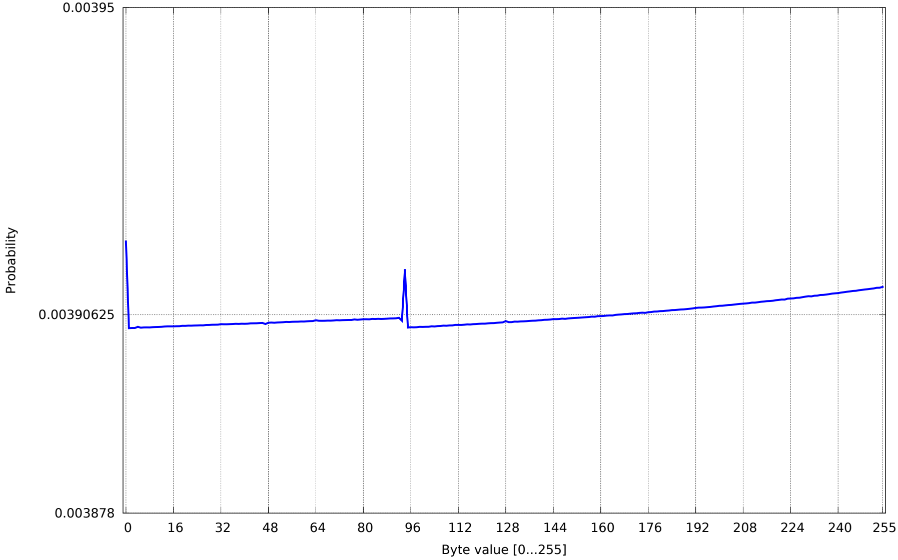
Keystream distribution at position 92



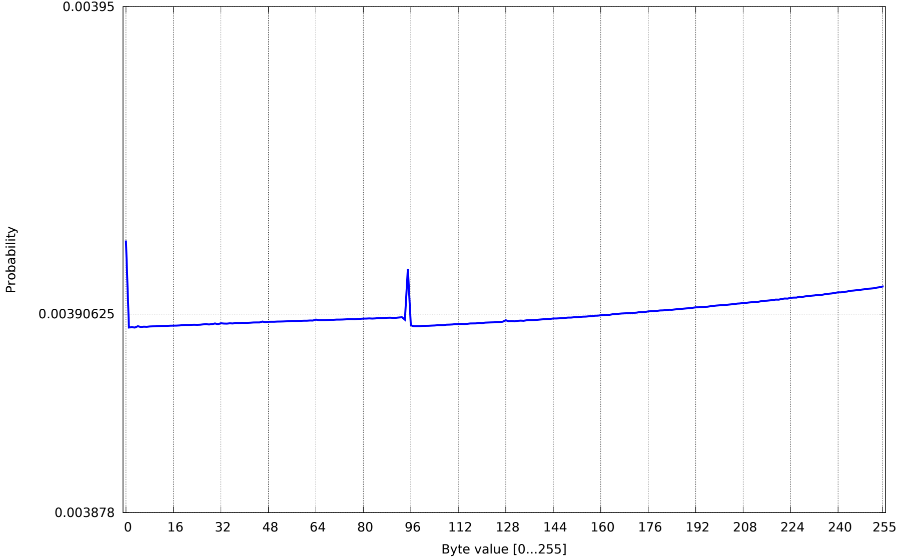
Keystream distribution at position 93



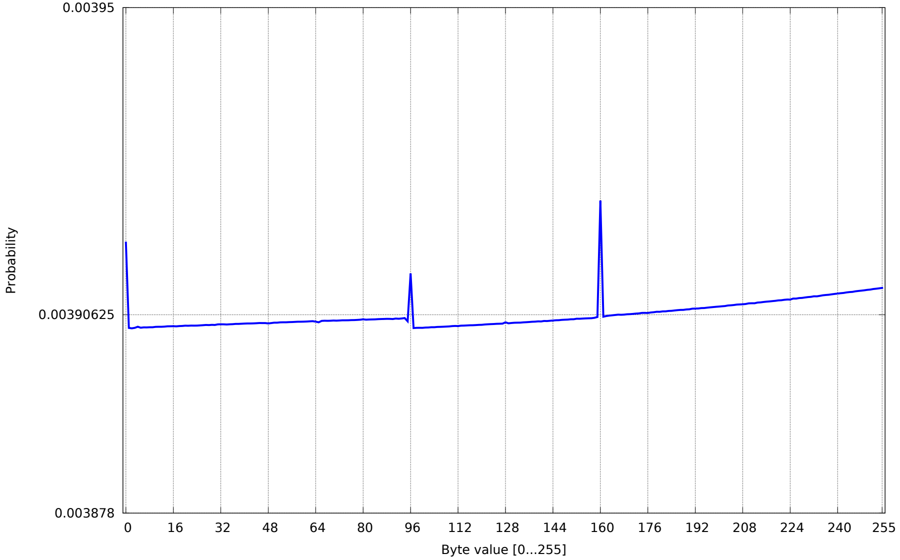
Keystream distribution at position 94



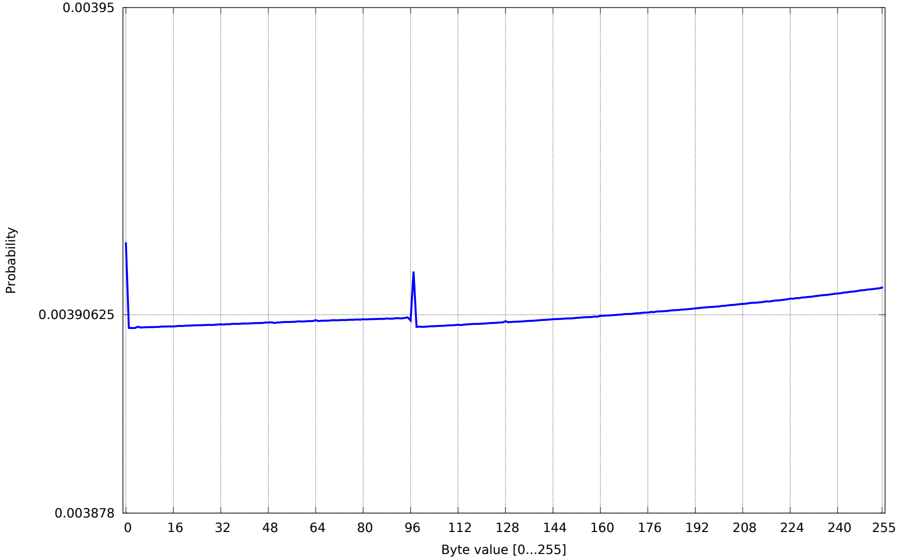
Keystream distribution at position 95



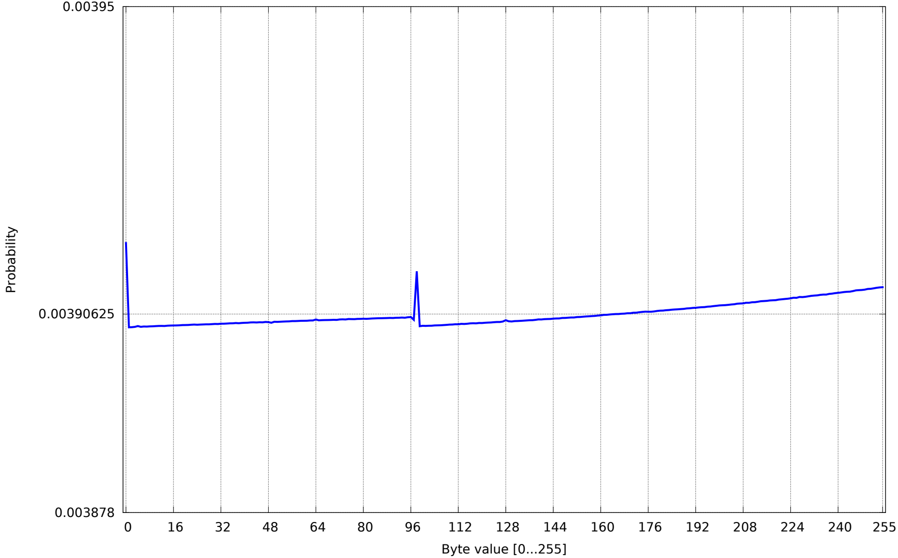
Keystream distribution at position 96



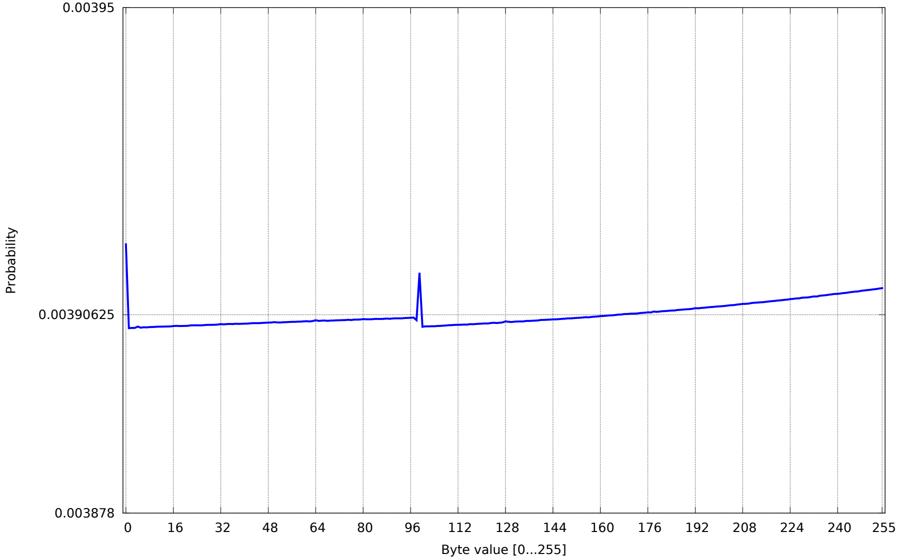
Keystream distribution at position 97



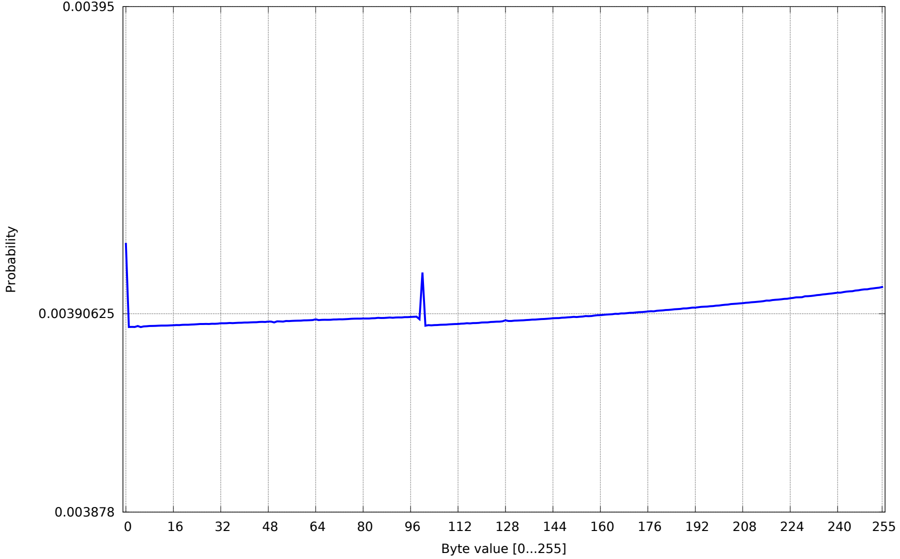
Keystream distribution at position 98



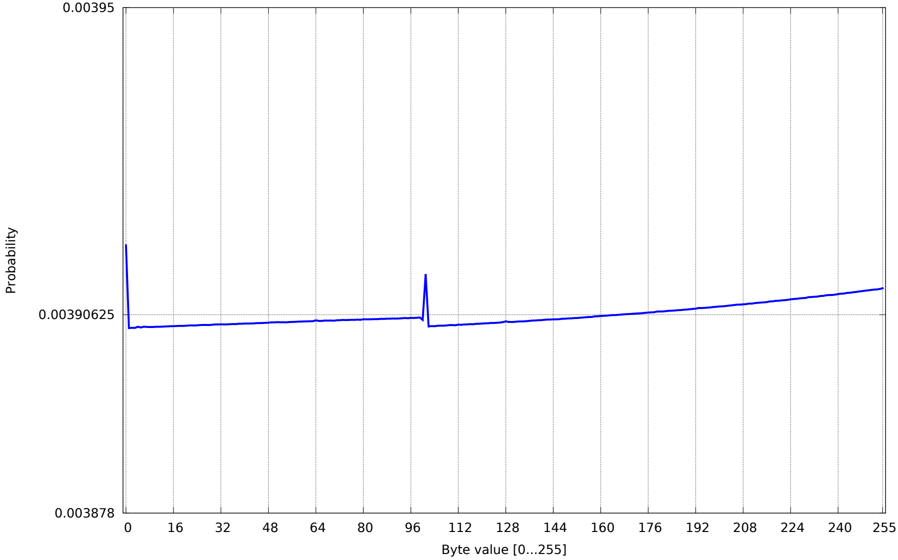
Keystream distribution at position 99



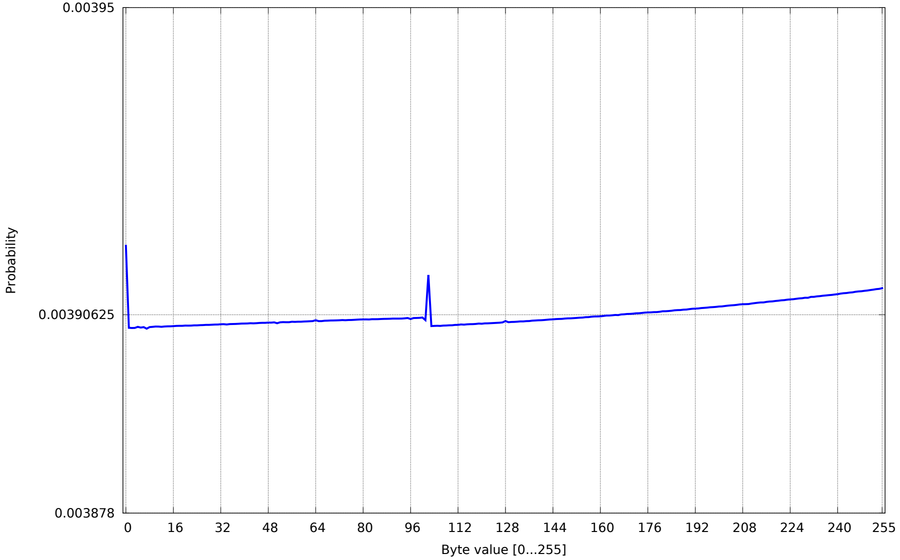
Keystream distribution at position 100



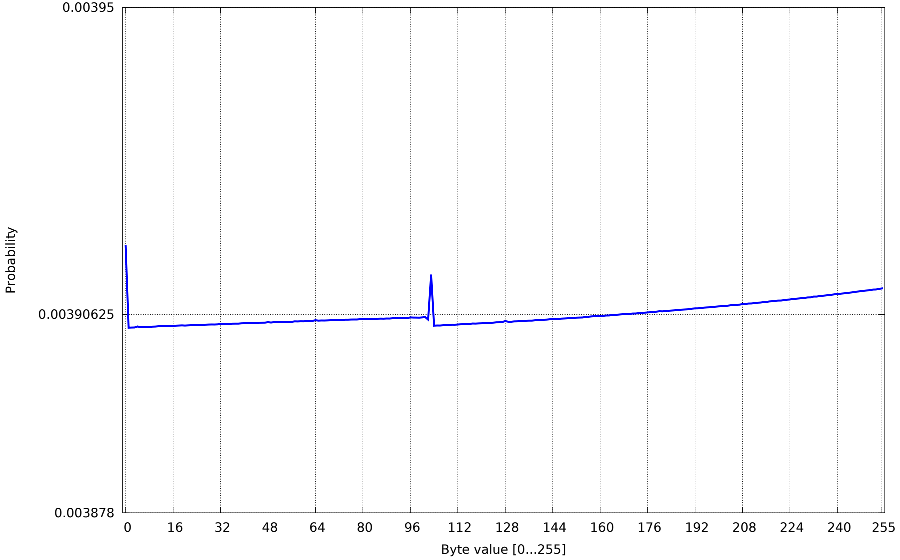
Keystream distribution at position 101



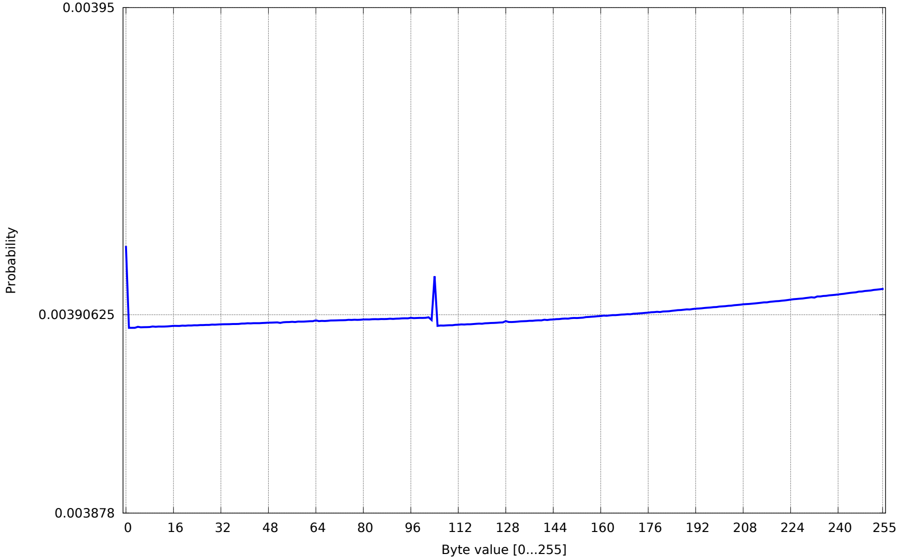
Keystream distribution at position 102



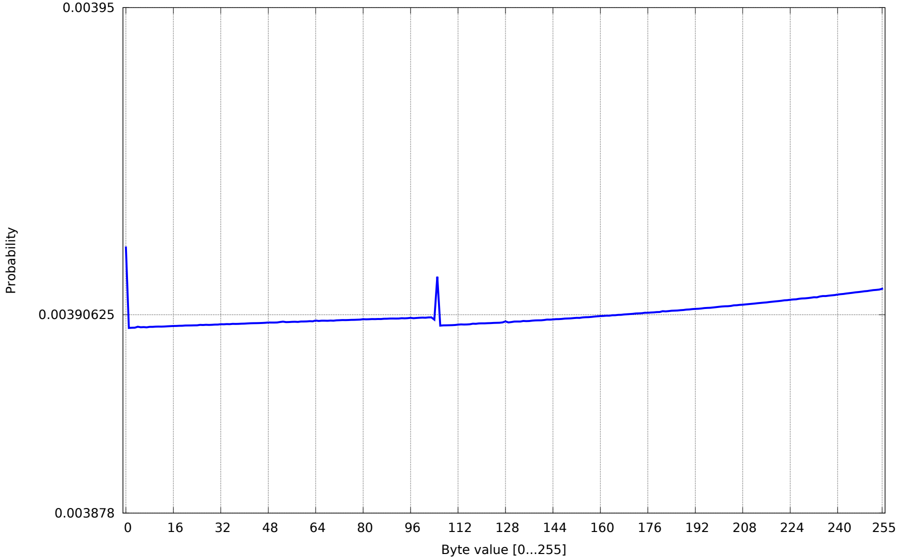
Keystream distribution at position 103



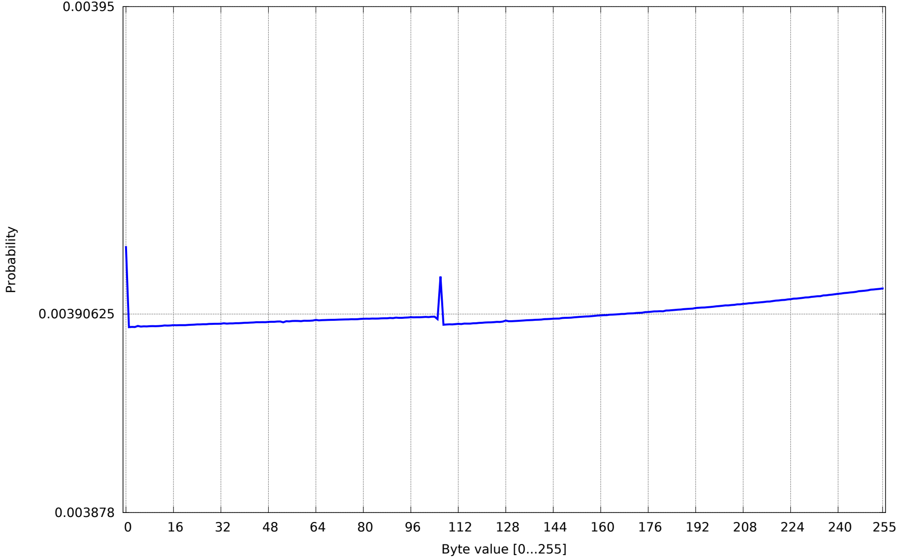
Keystream distribution at position 104



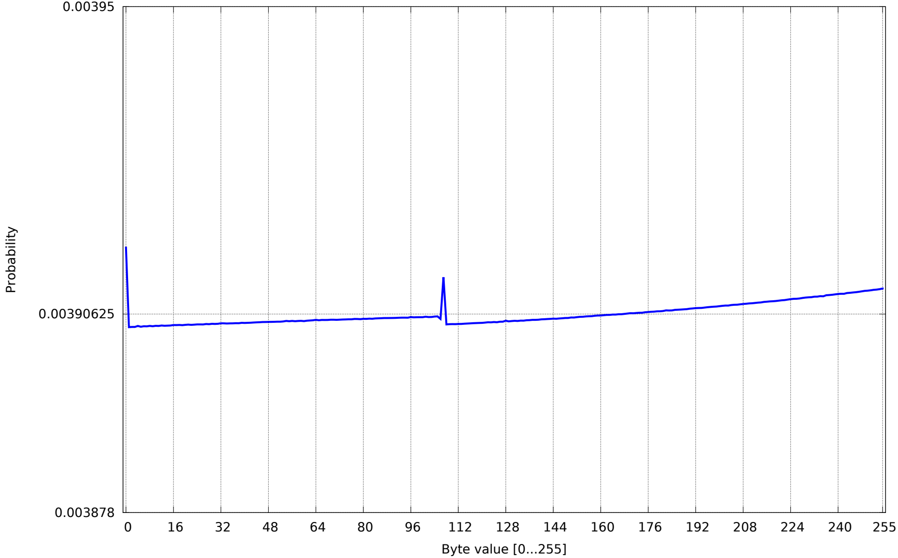
Keystream distribution at position 105



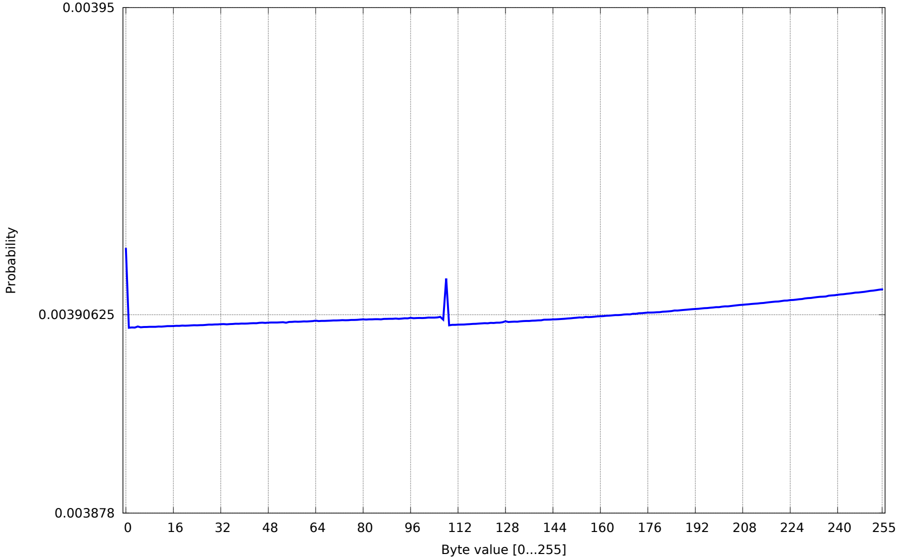
Keystream distribution at position 106



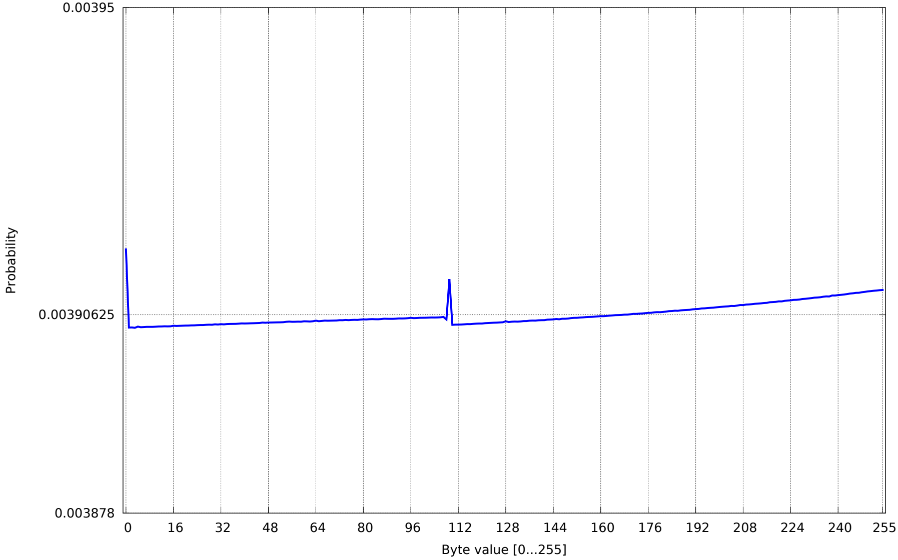
Keystream distribution at position 107



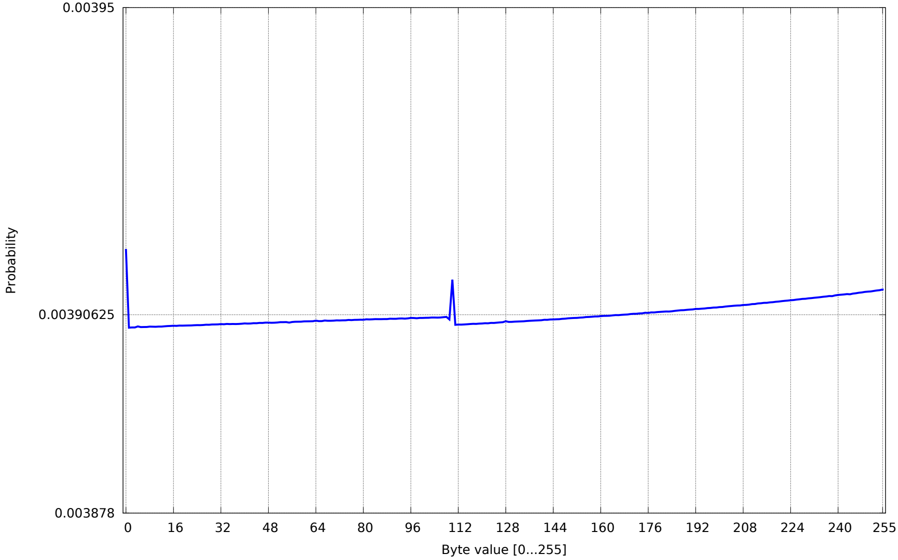
Keystream distribution at position 108



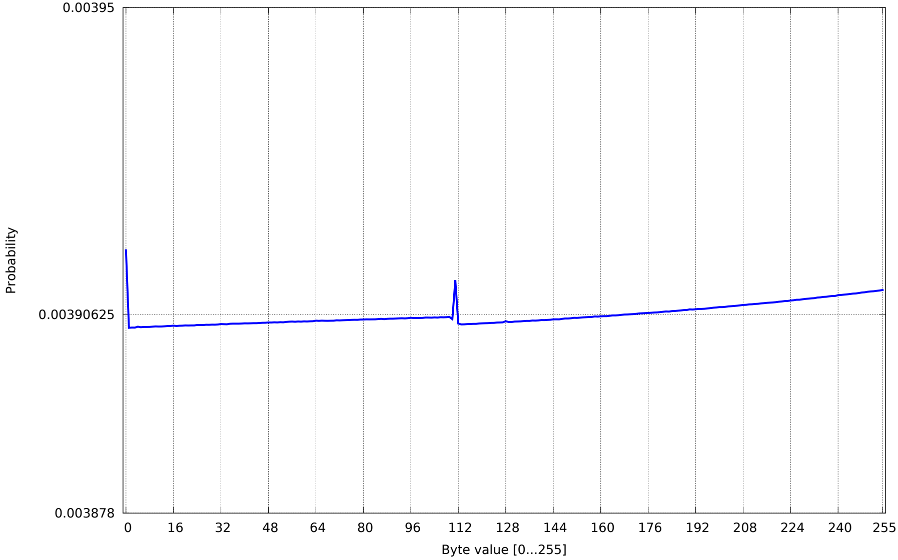
Keystream distribution at position 109



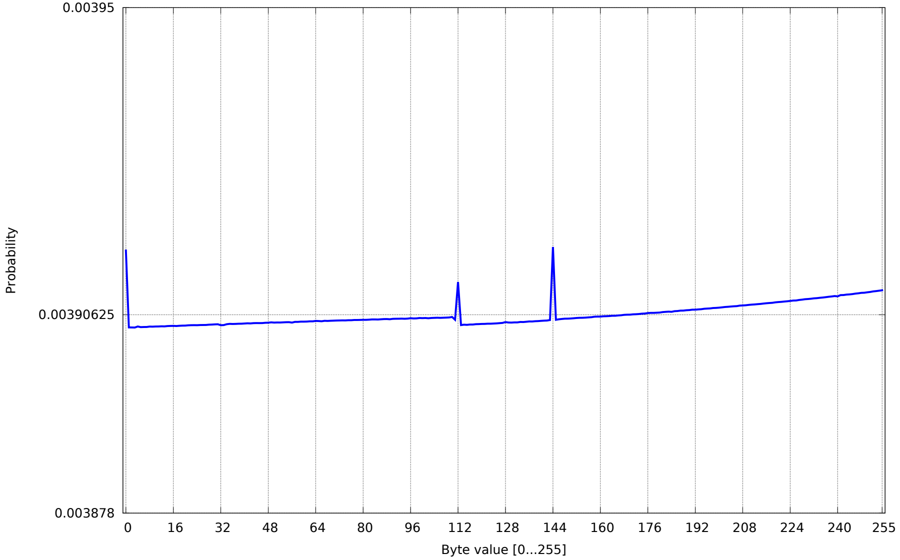
Keystream distribution at position 110



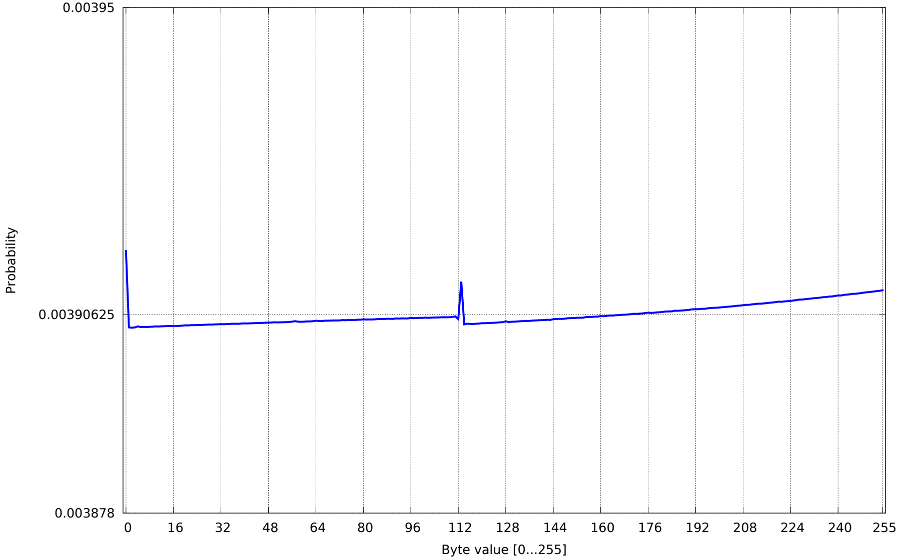
Keystream distribution at position 111



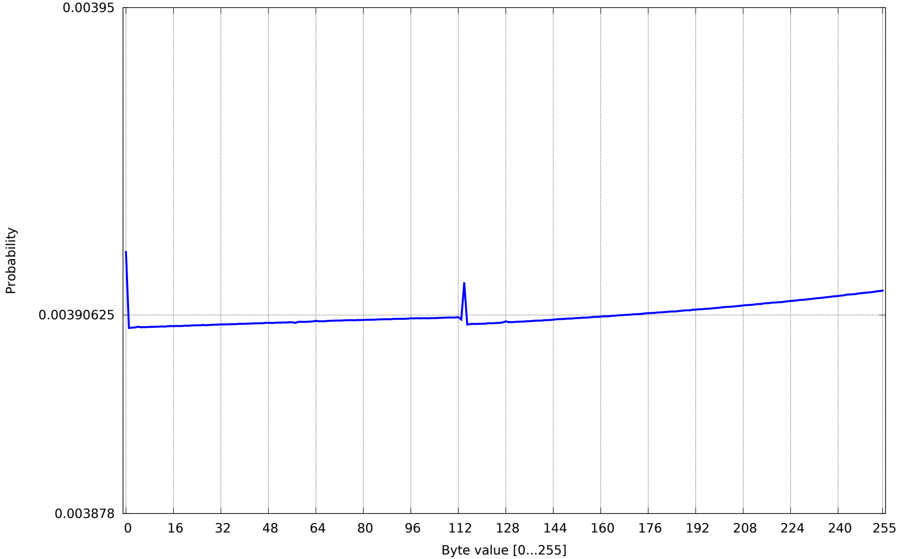
Keystream distribution at position 112



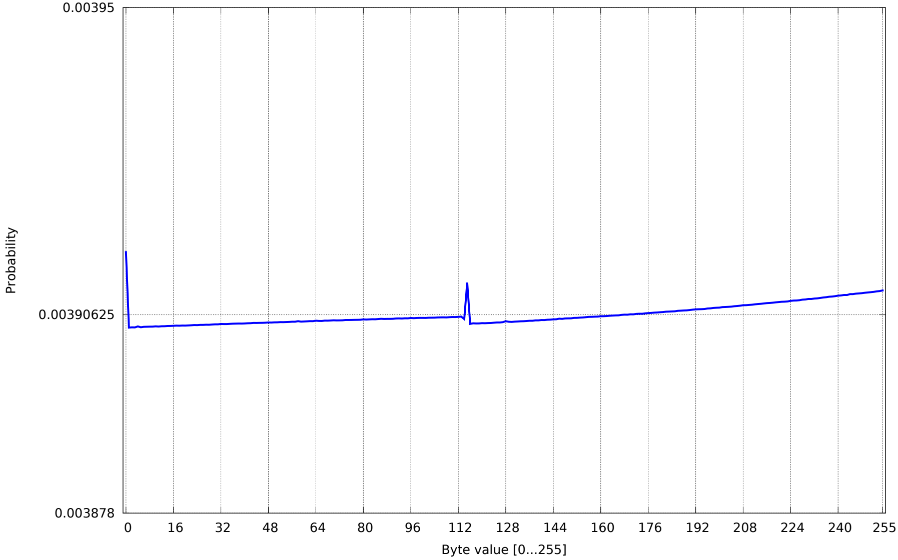
Keystream distribution at position 113



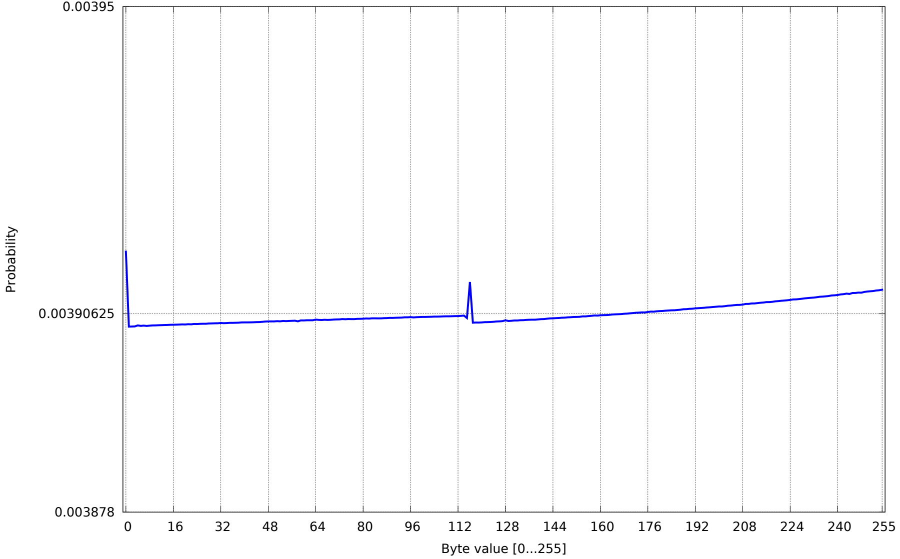
Keystream distribution at position 114



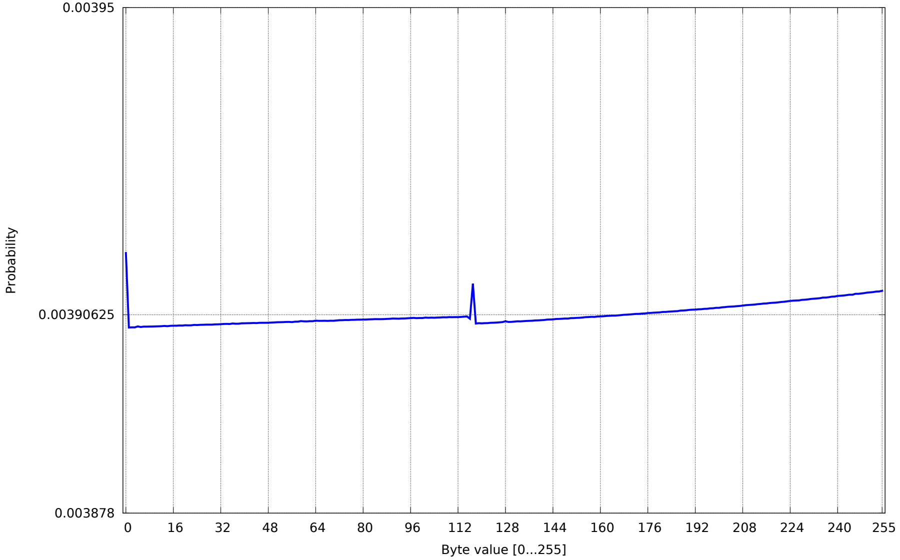
Keystream distribution at position 115



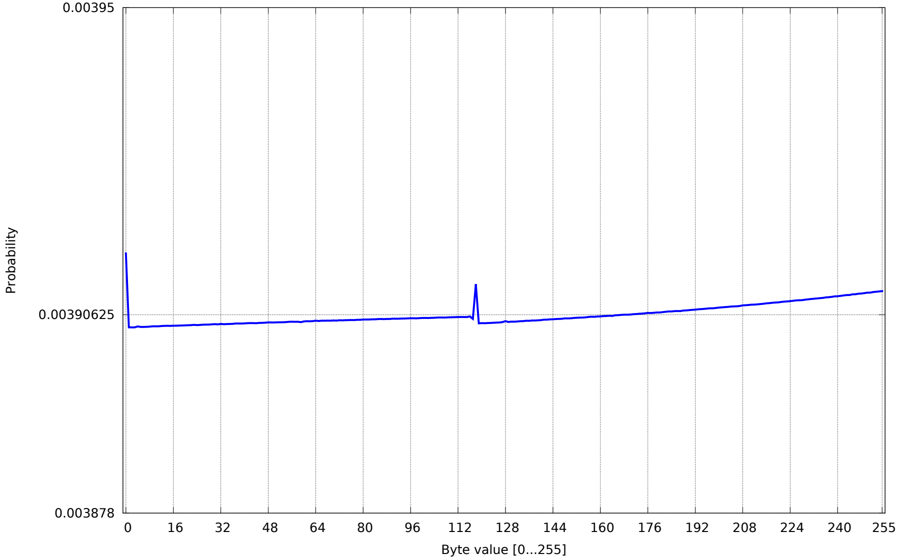
Keystream distribution at position 116



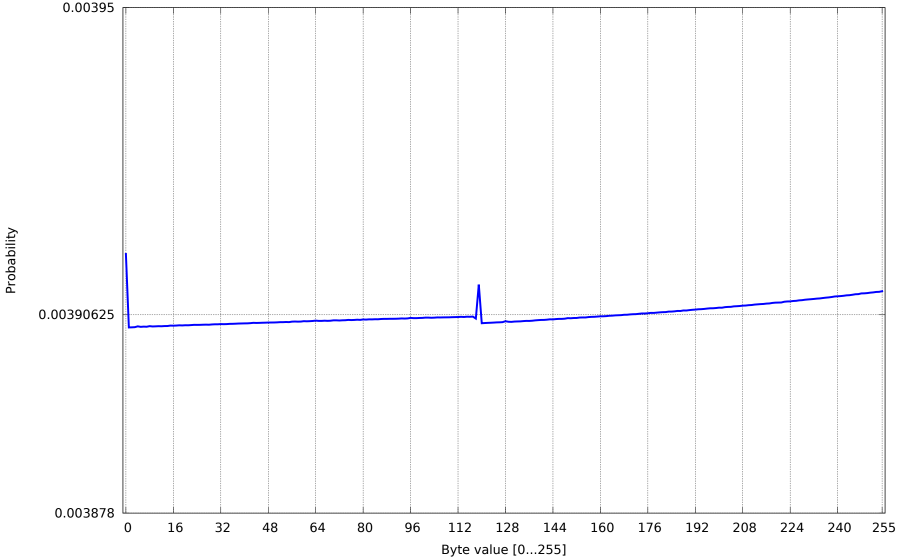
Keystream distribution at position 117



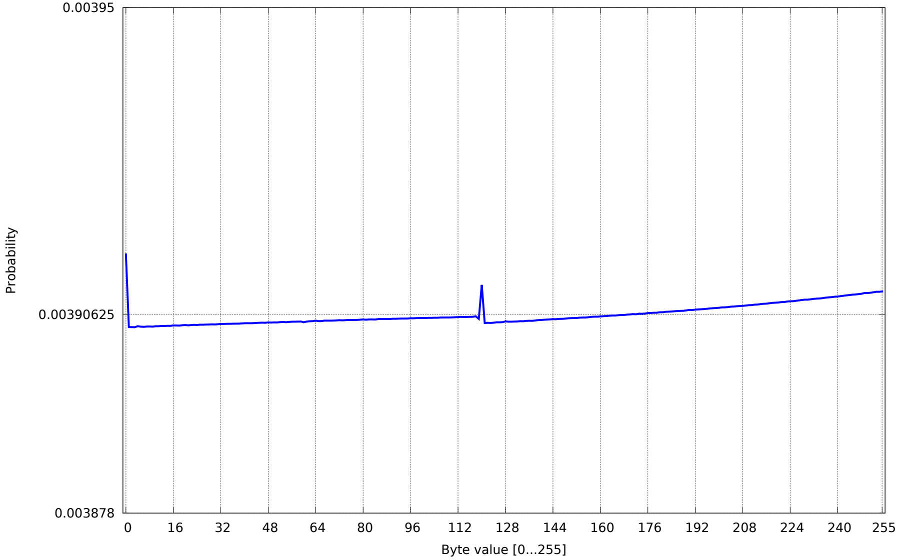
Keystream distribution at position 118



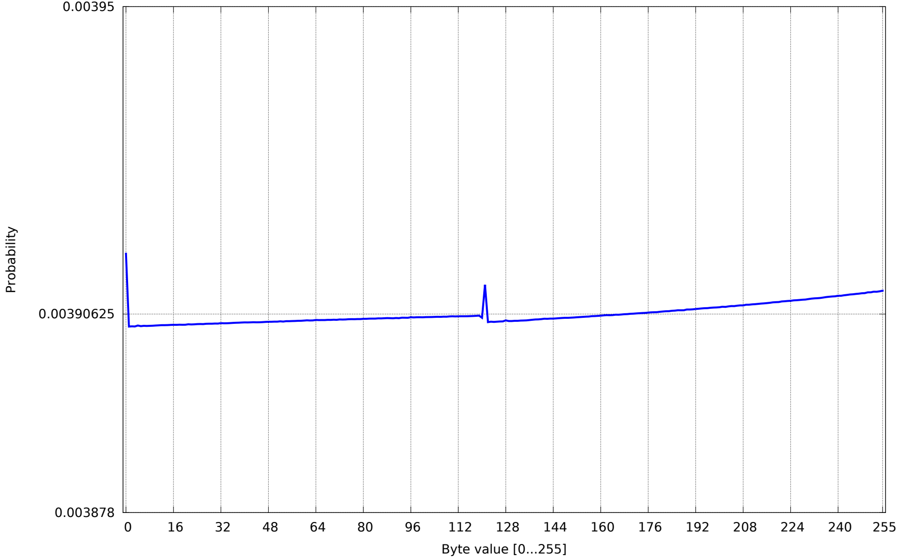
Keystream distribution at position 119



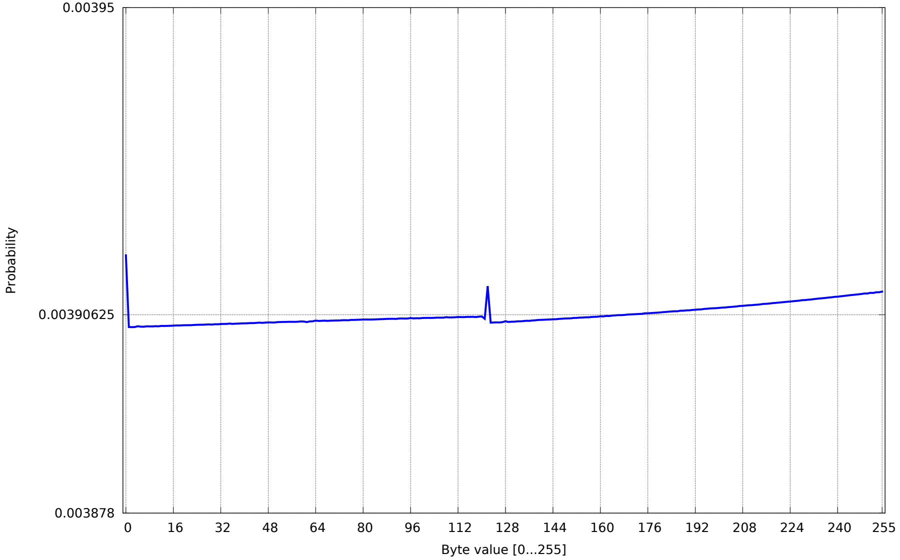
Keystream distribution at position 120



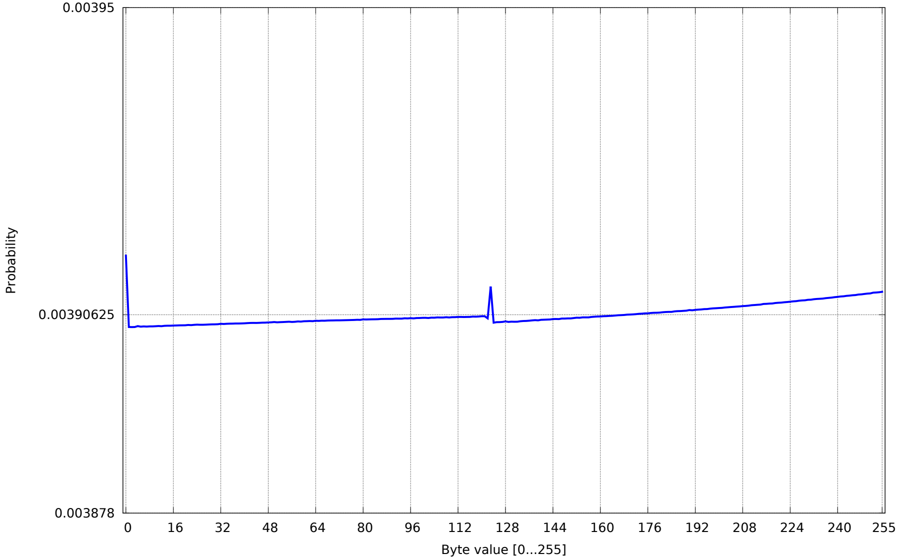
Keystream distribution at position 121



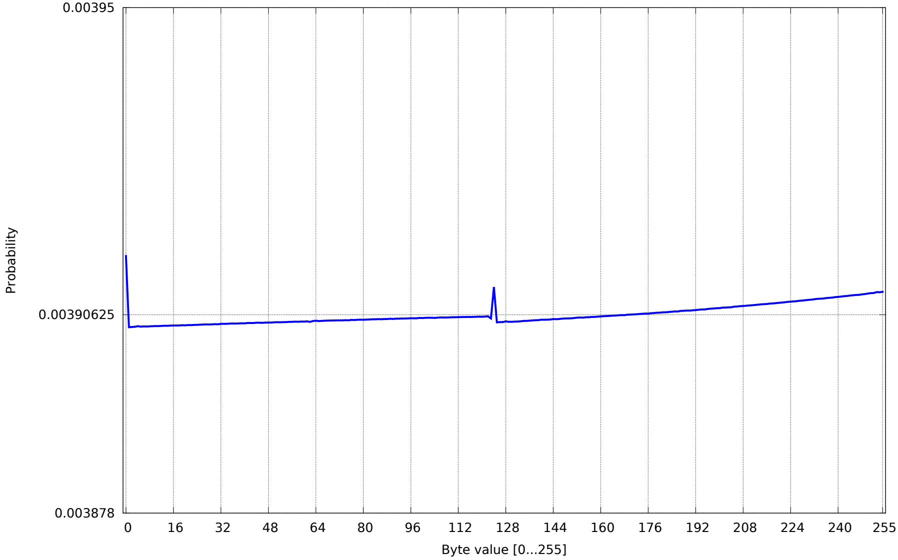
Keystream distribution at position 122



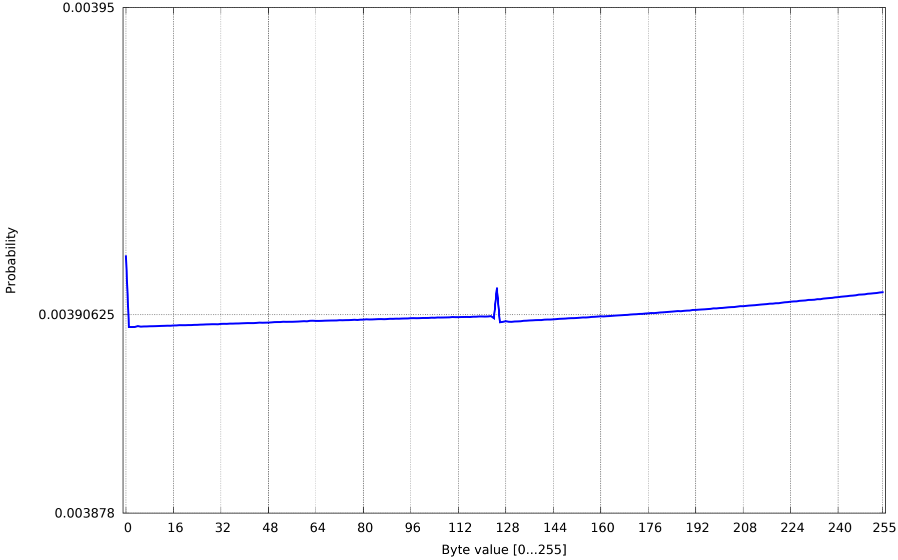
Keystream distribution at position 123



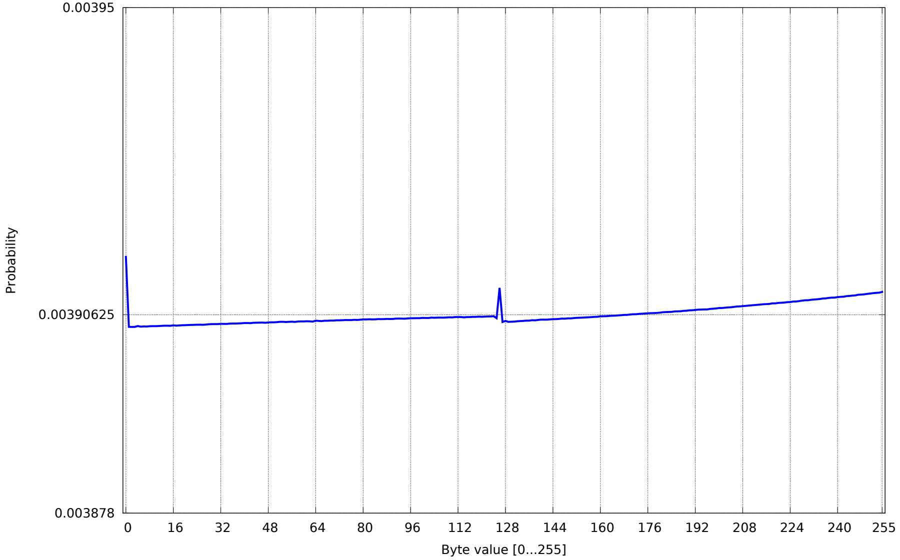
Keystream distribution at position 124



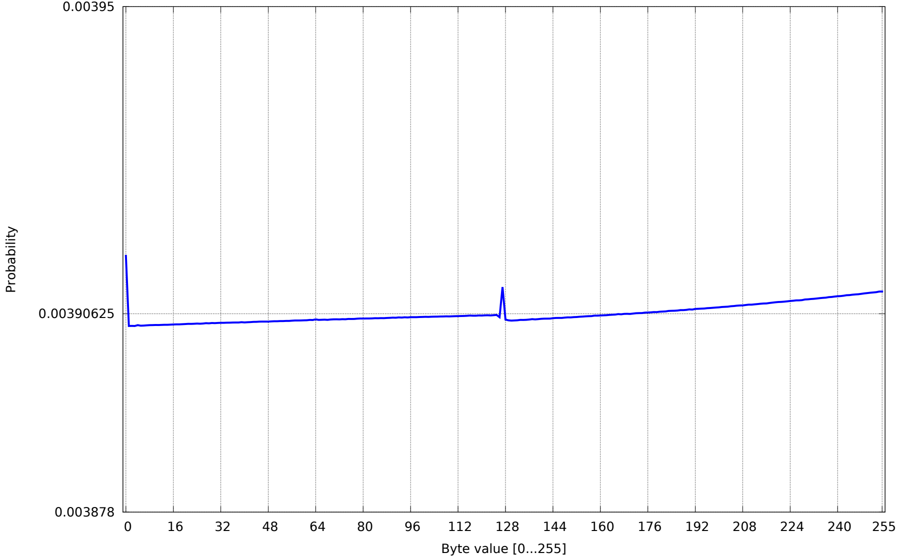
Keystream distribution at position 125



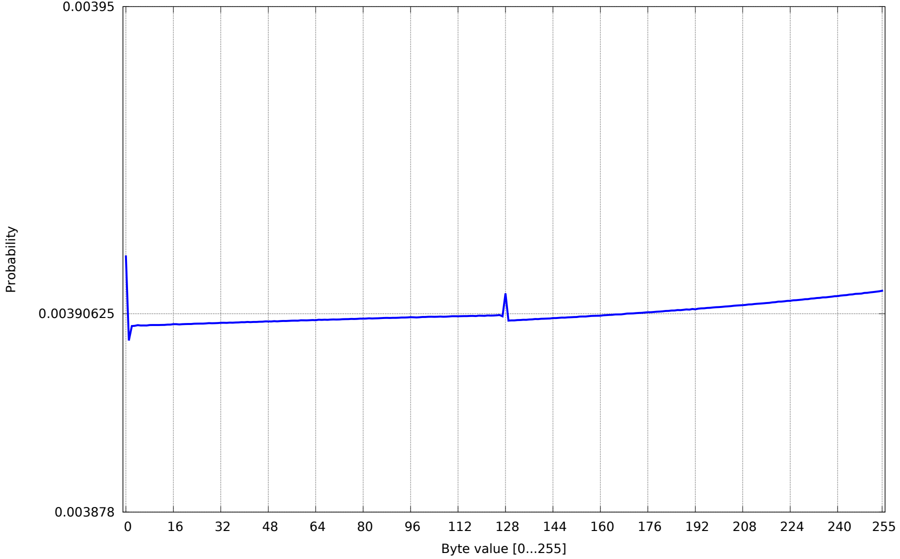
Keystream distribution at position 126



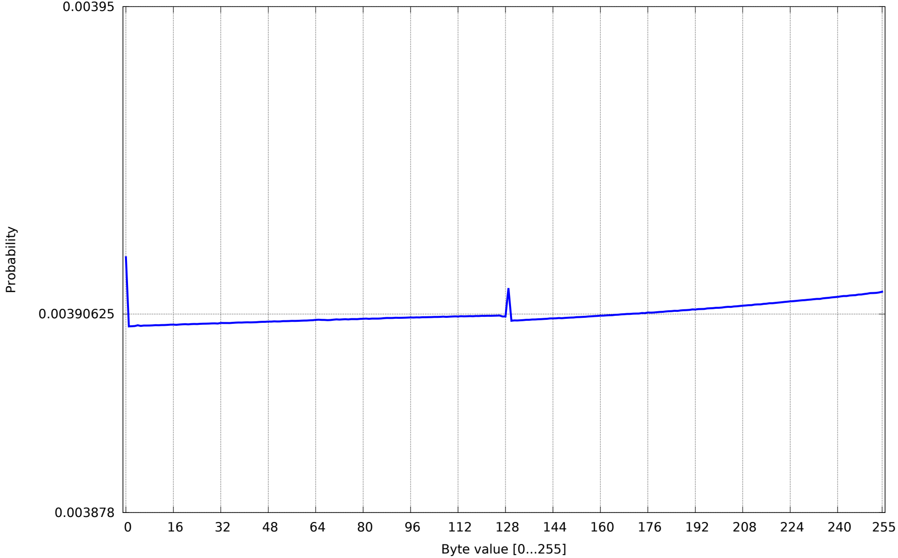
Keystream distribution at position 127



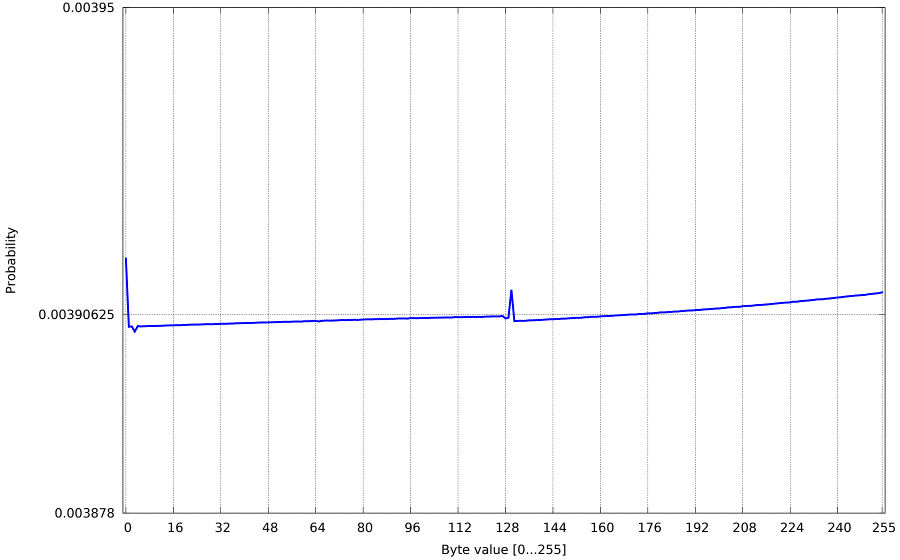
Keystream distribution at position 128



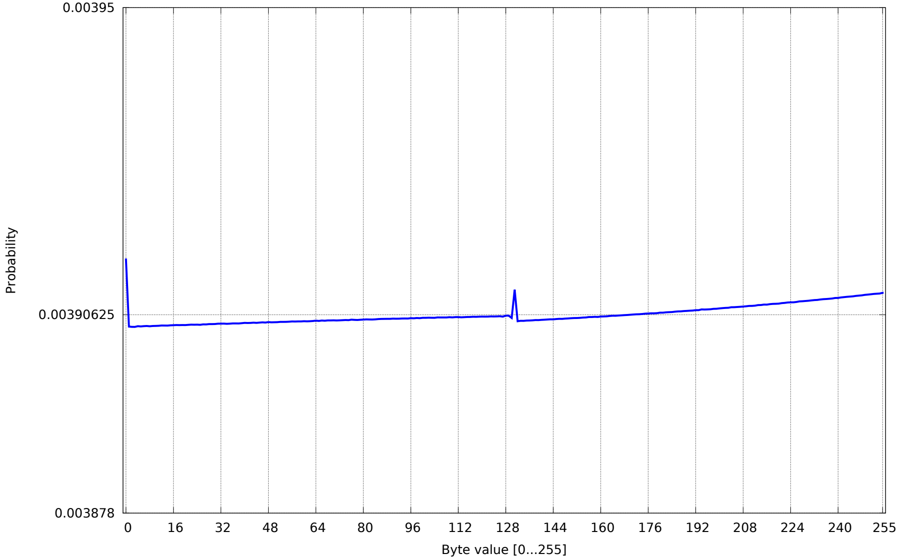
Keystream distribution at position 129



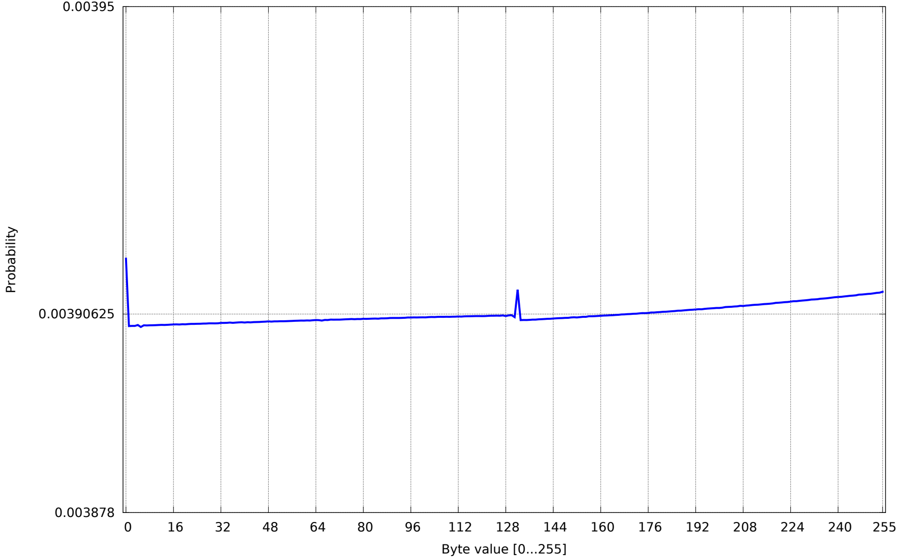
Keystream distribution at position 130



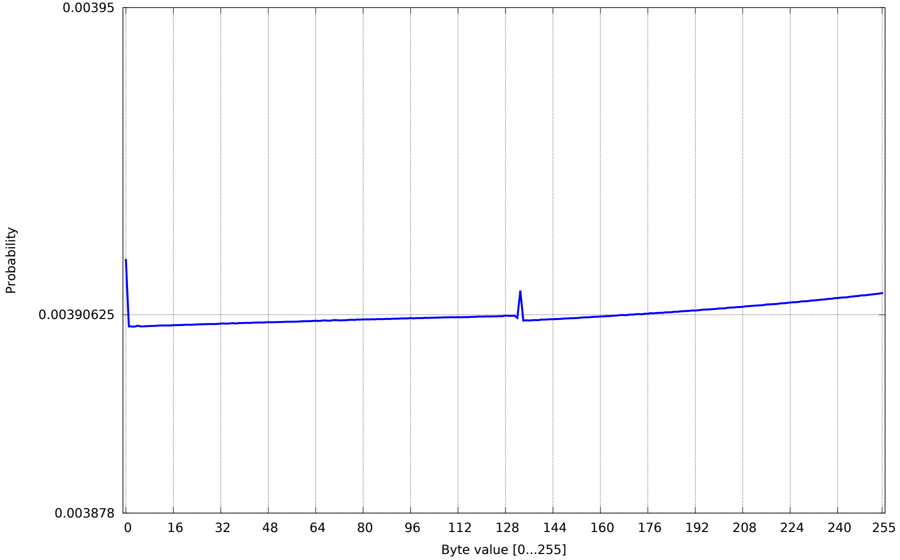
Keystream distribution at position 131



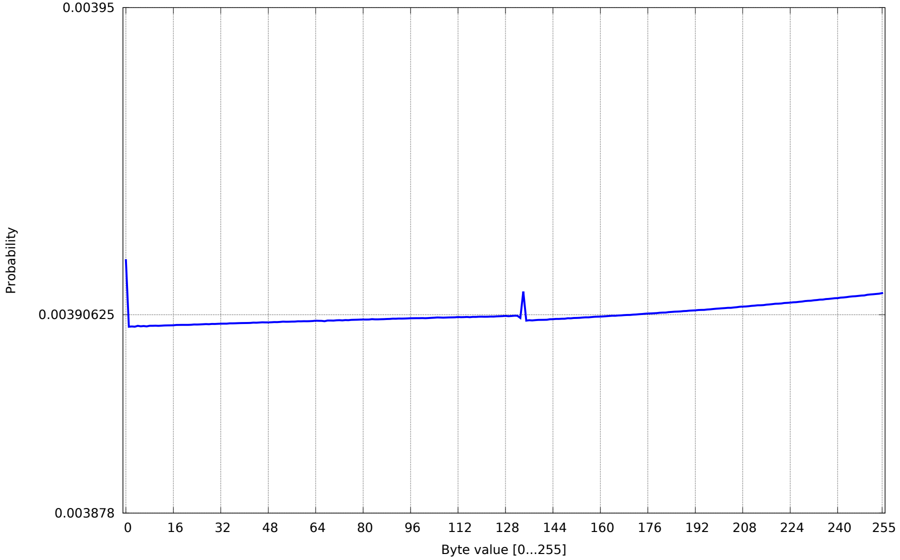
Keystream distribution at position 132



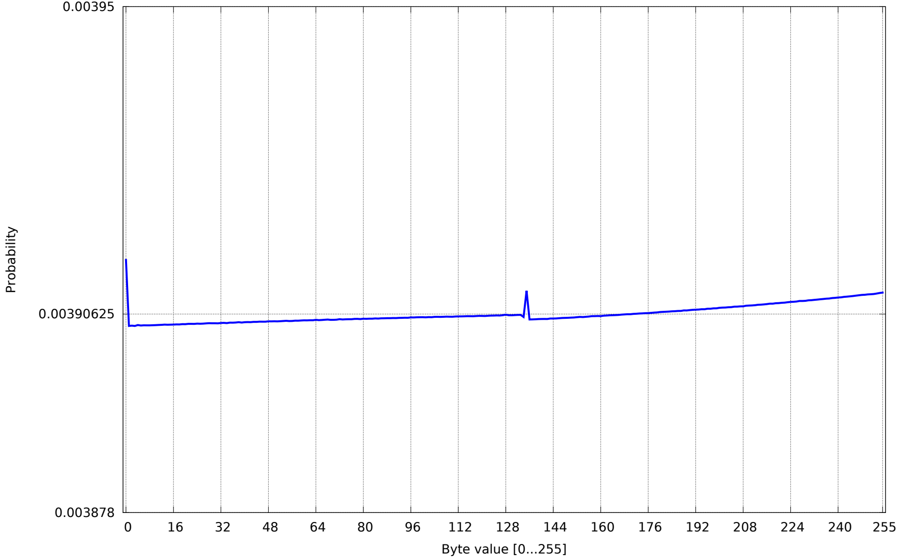
Keystream distribution at position 133



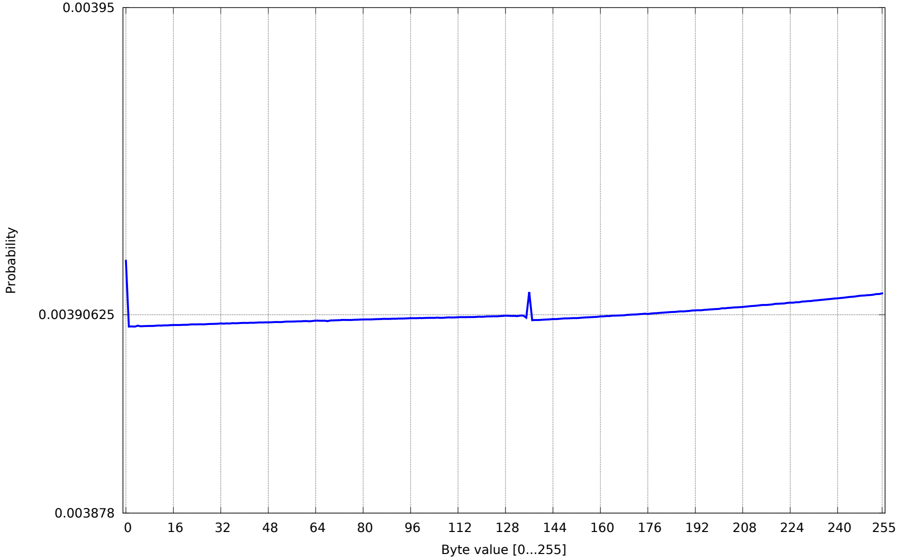
Keystream distribution at position 134



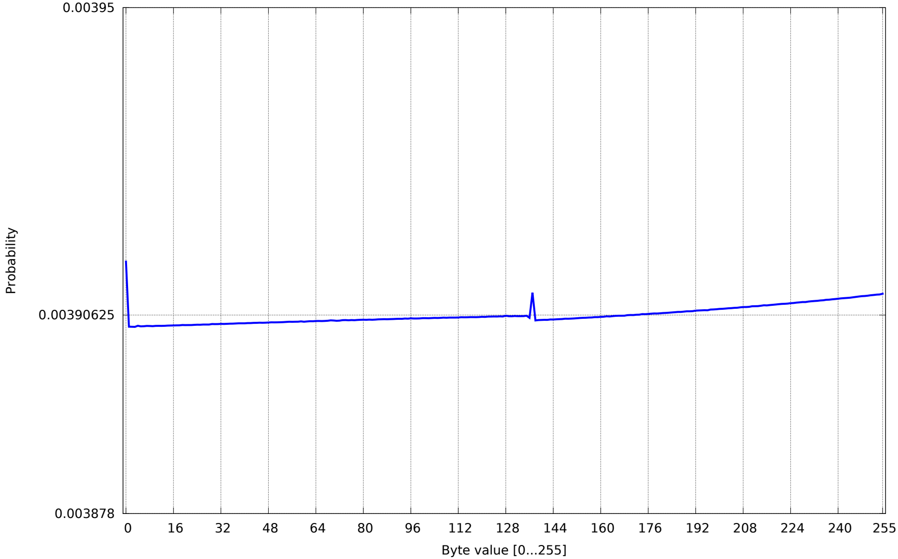
Keystream distribution at position 135



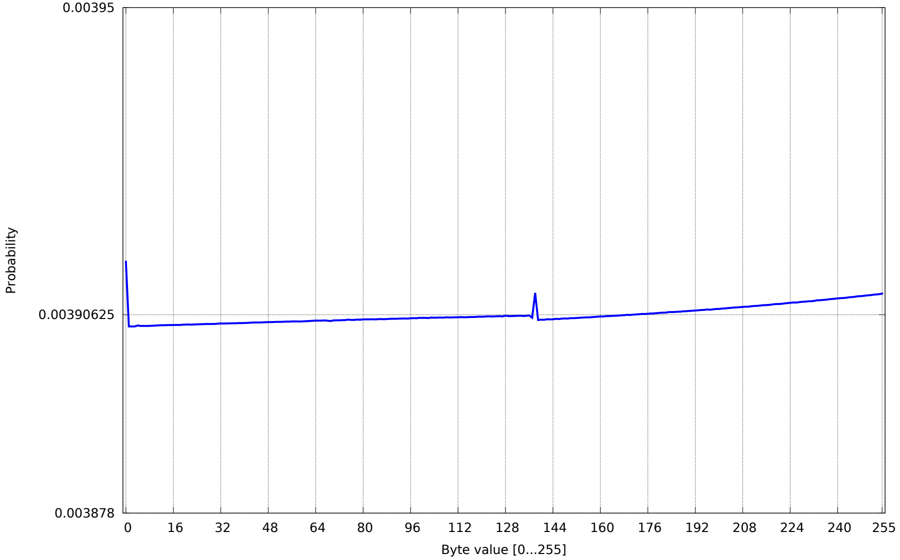
Keystream distribution at position 136



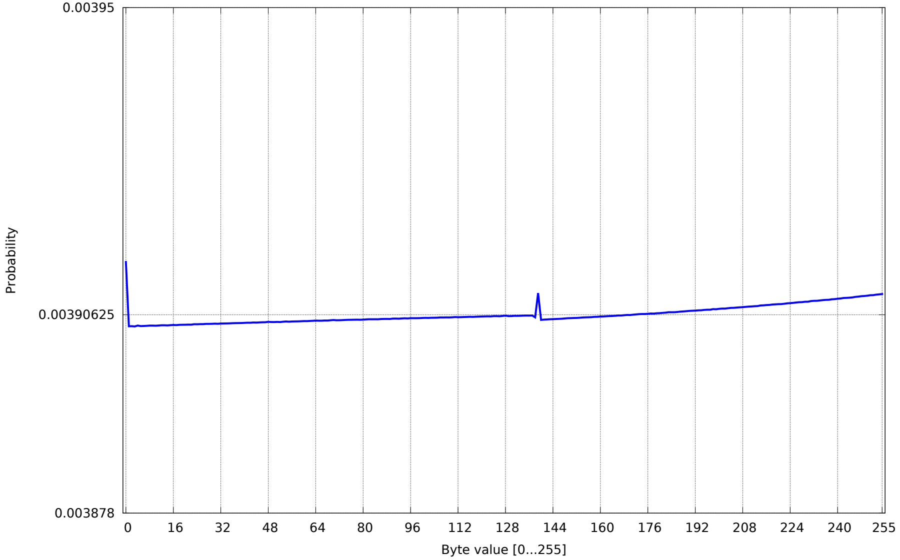
Keystream distribution at position 137



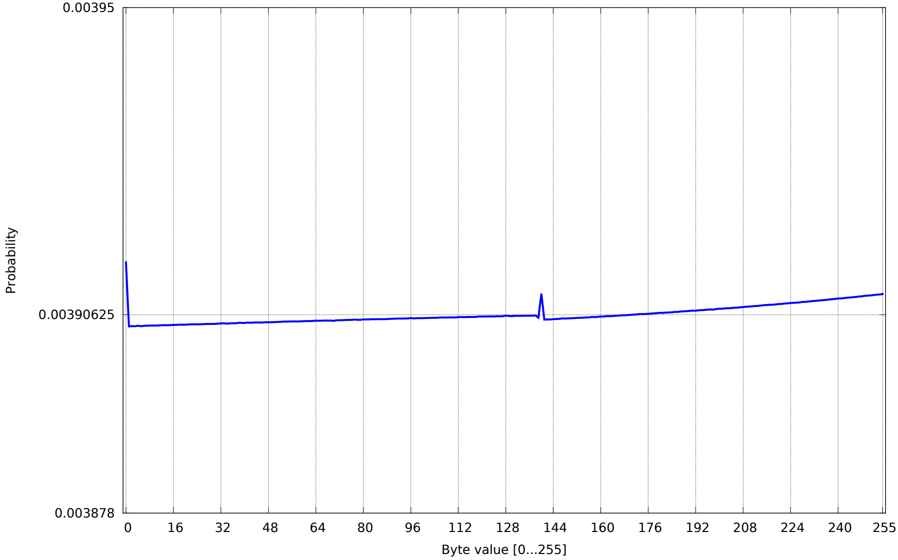
Keystream distribution at position 138



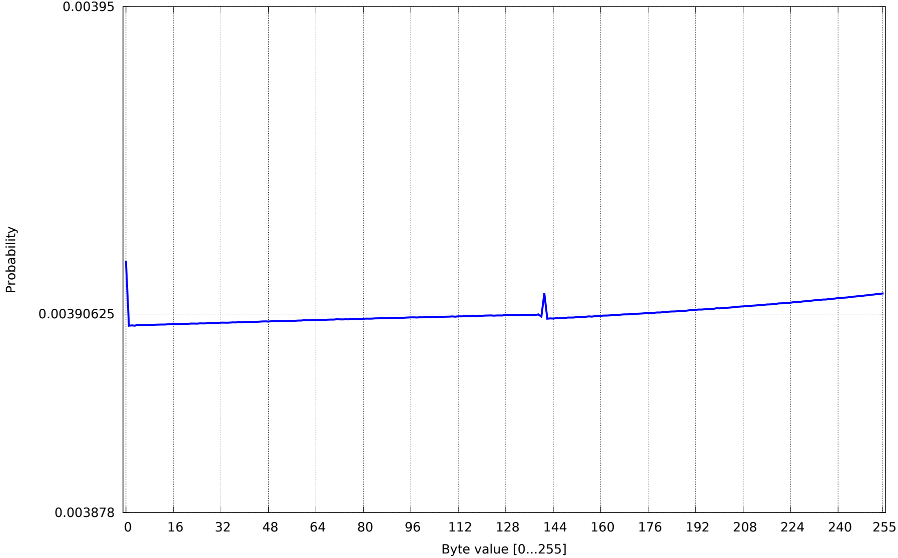
Keystream distribution at position 139



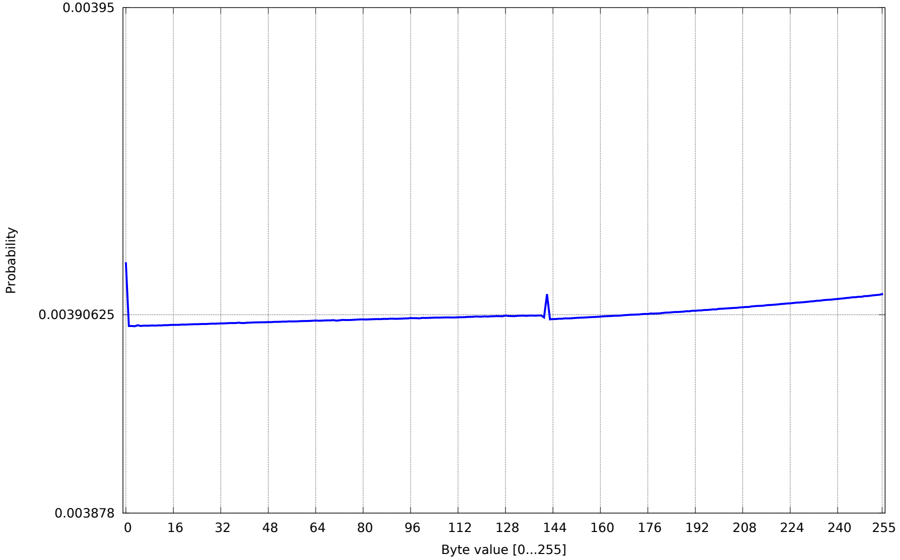
Keystream distribution at position 140



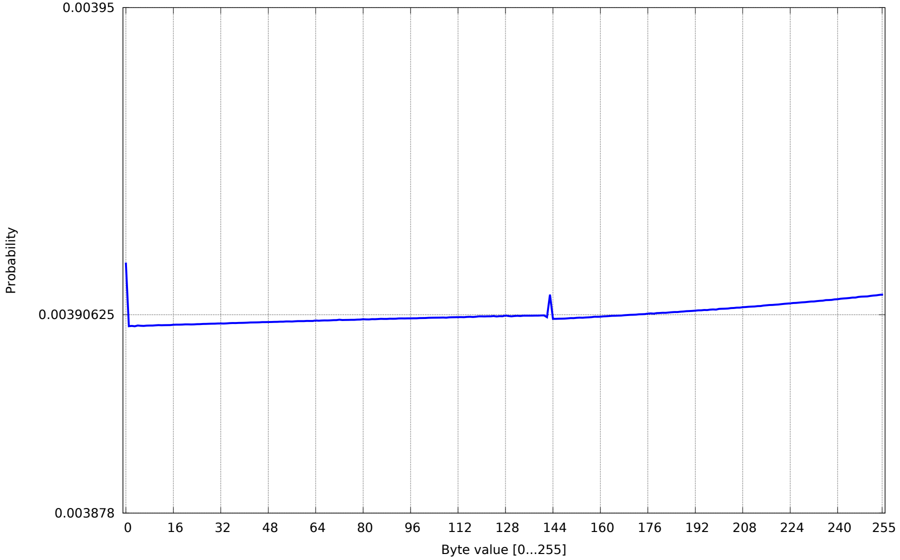
Keystream distribution at position 141



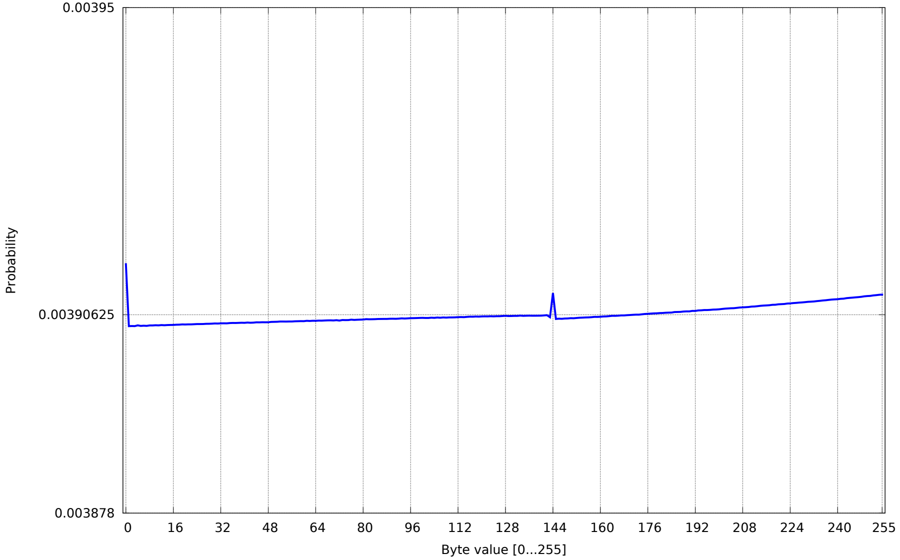
Keystream distribution at position 142



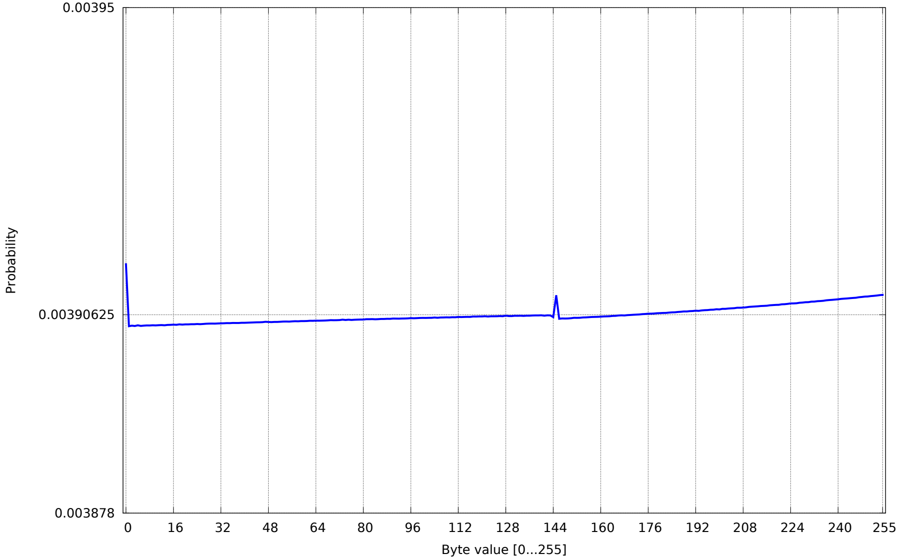
Keystream distribution at position 143



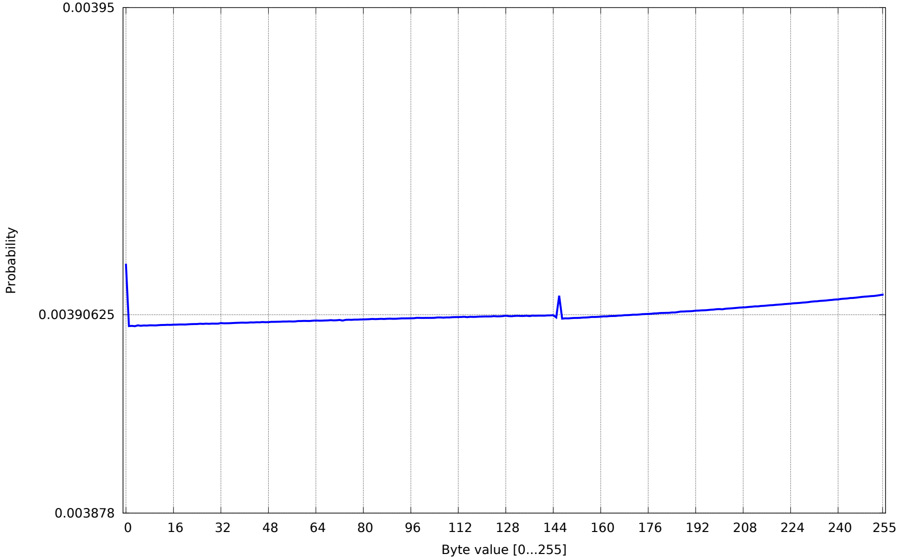
Keystream distribution at position 144



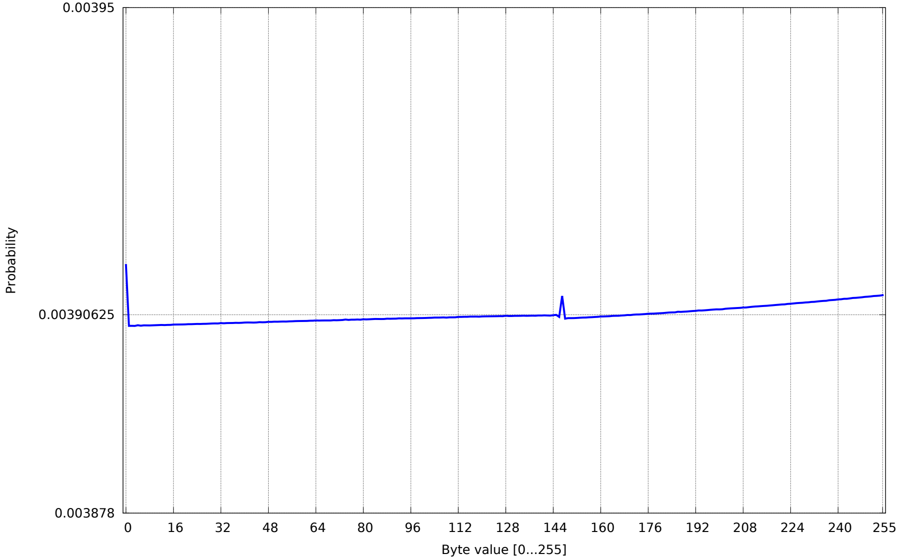
Keystream distribution at position 145



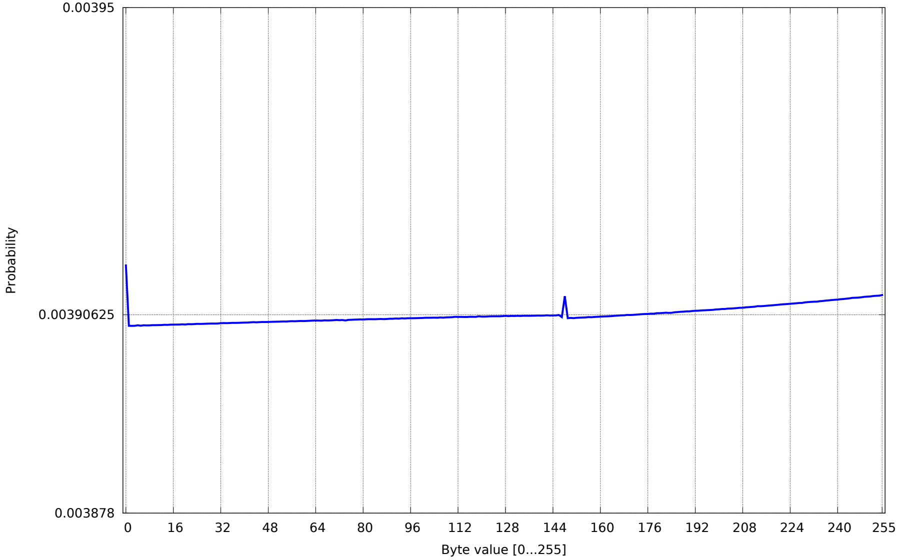
Keystream distribution at position 146



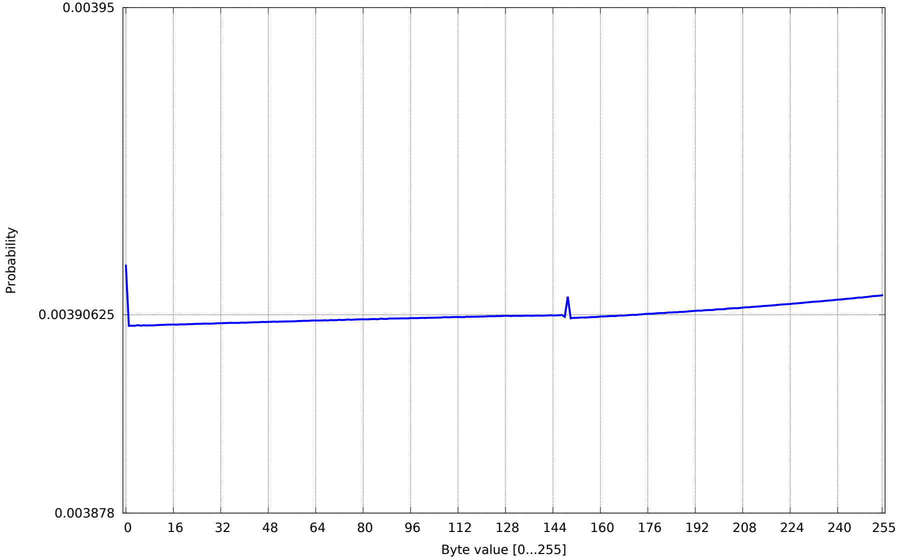
Keystream distribution at position 147



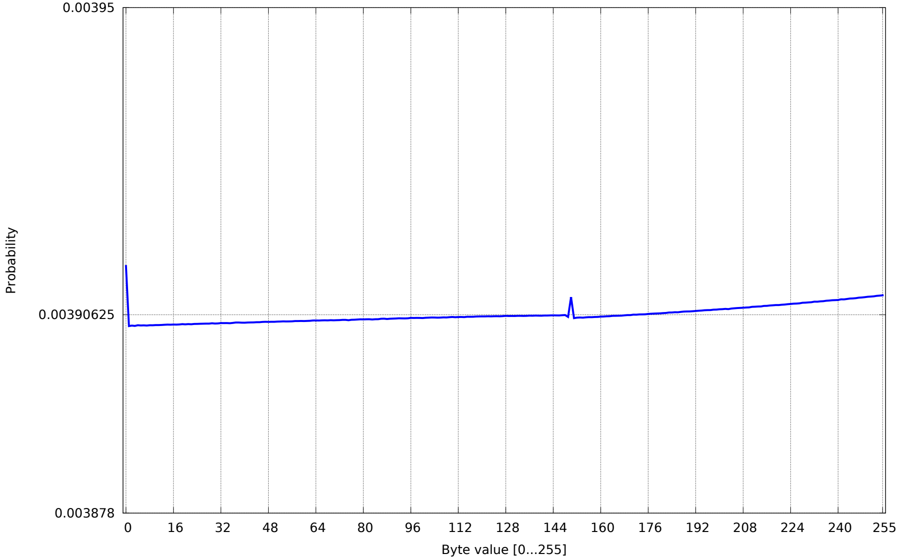
Keystream distribution at position 148



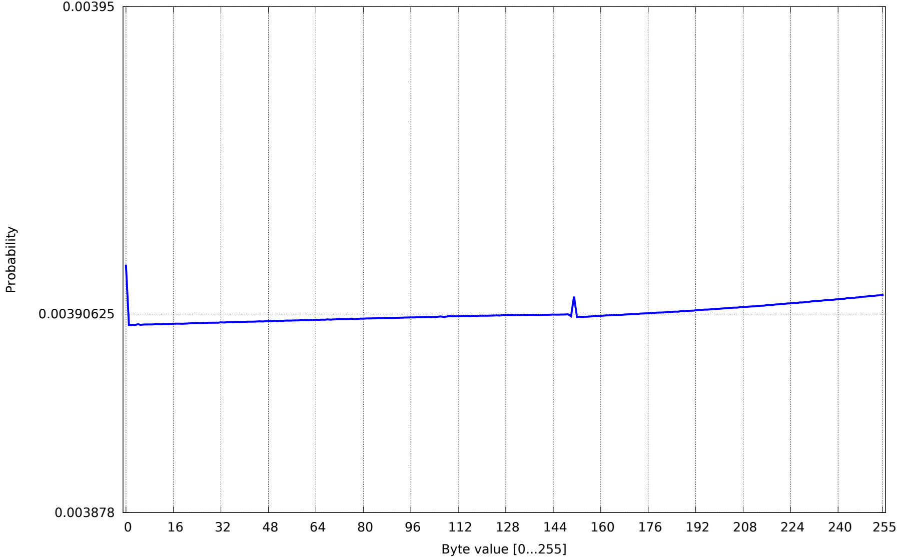
Keystream distribution at position 149



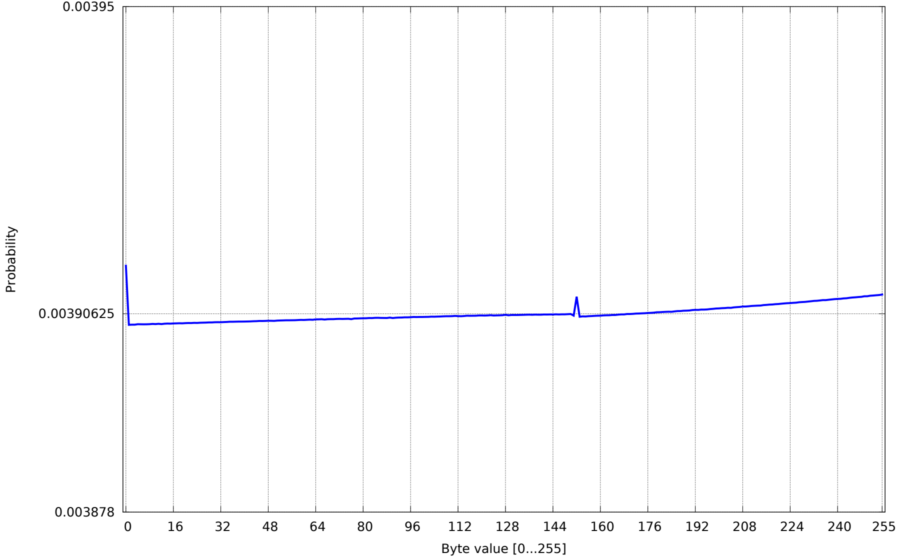
Keystream distribution at position 150



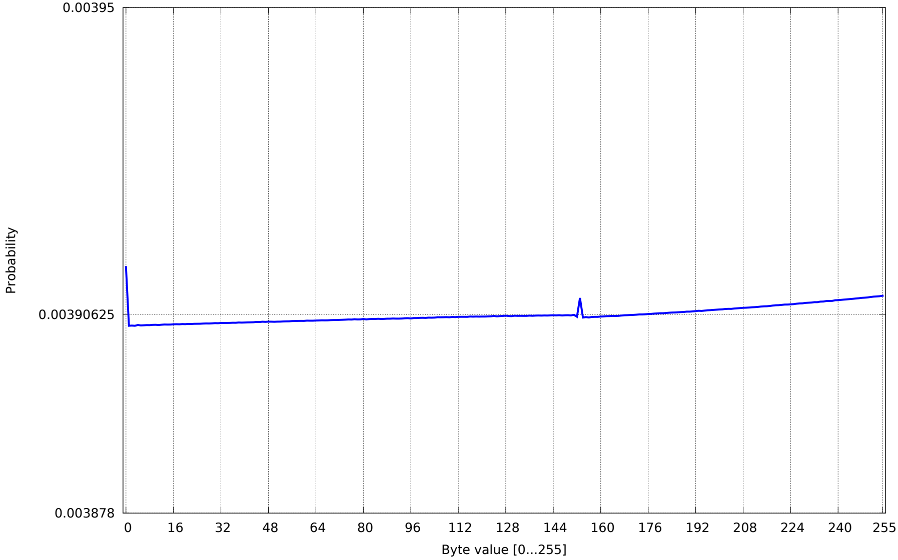
Keystream distribution at position 151



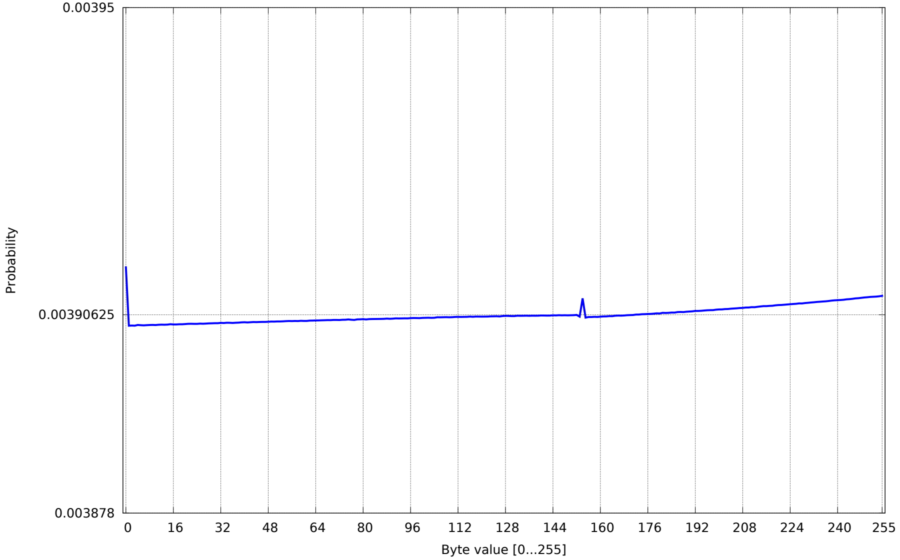
Keystream distribution at position 152



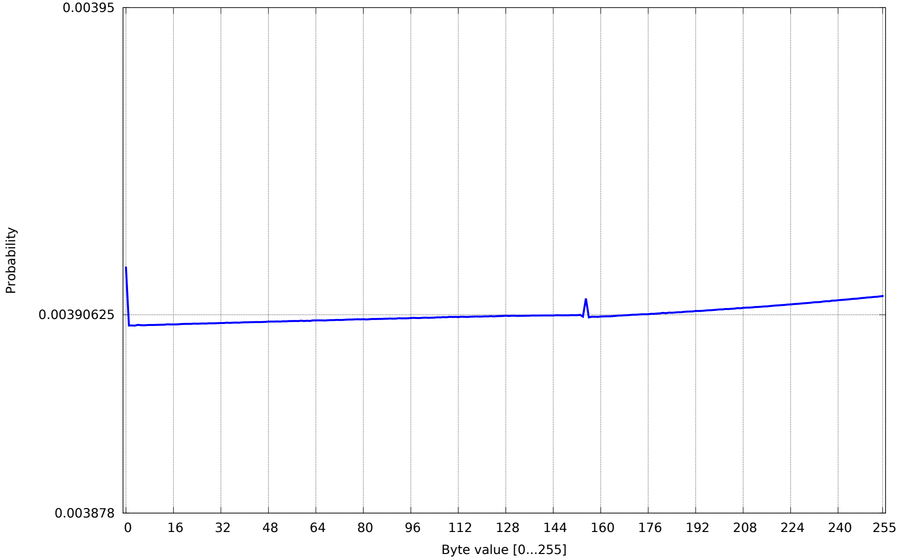
Keystream distribution at position 153



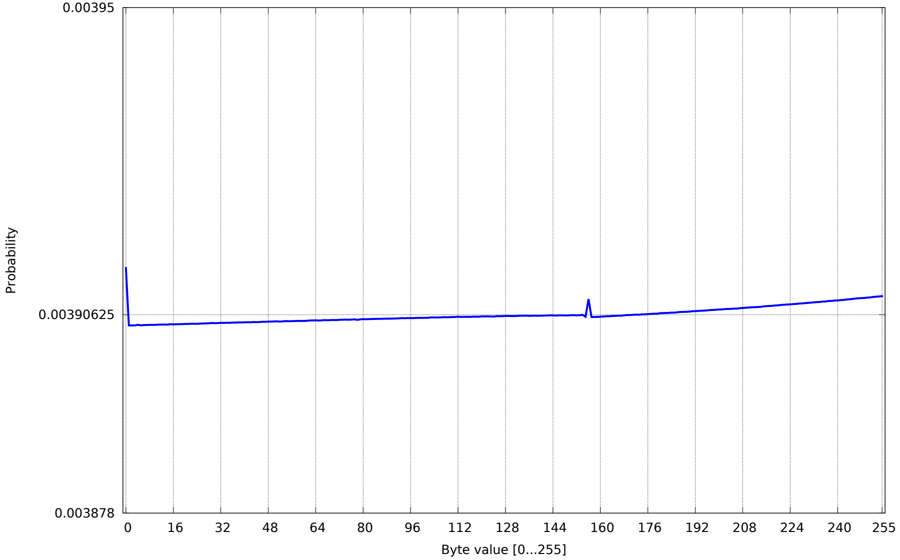
Keystream distribution at position 154



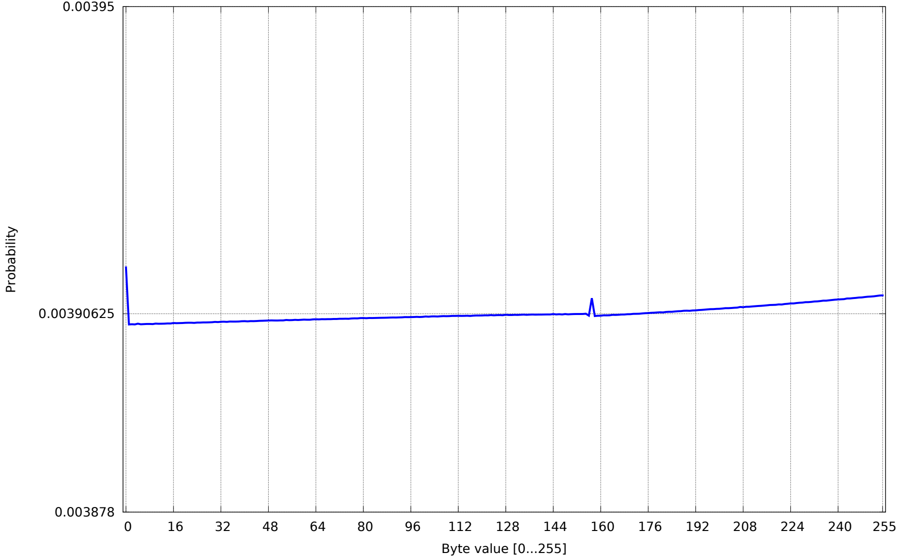
Keystream distribution at position 155



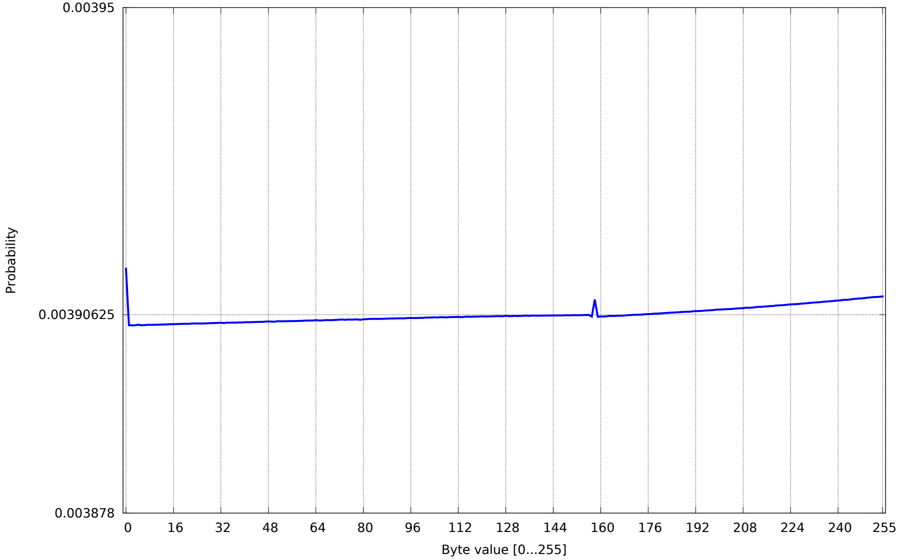
Keystream distribution at position 156



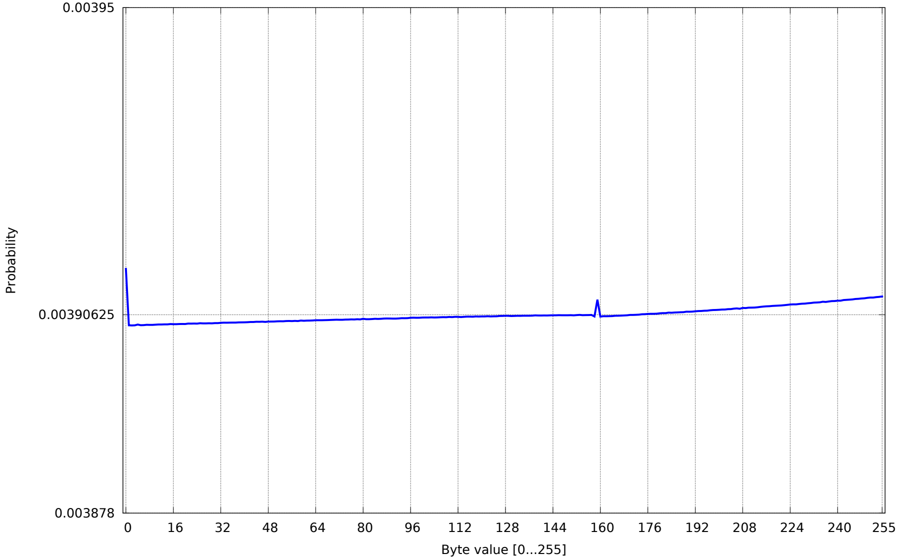
Keystream distribution at position 157



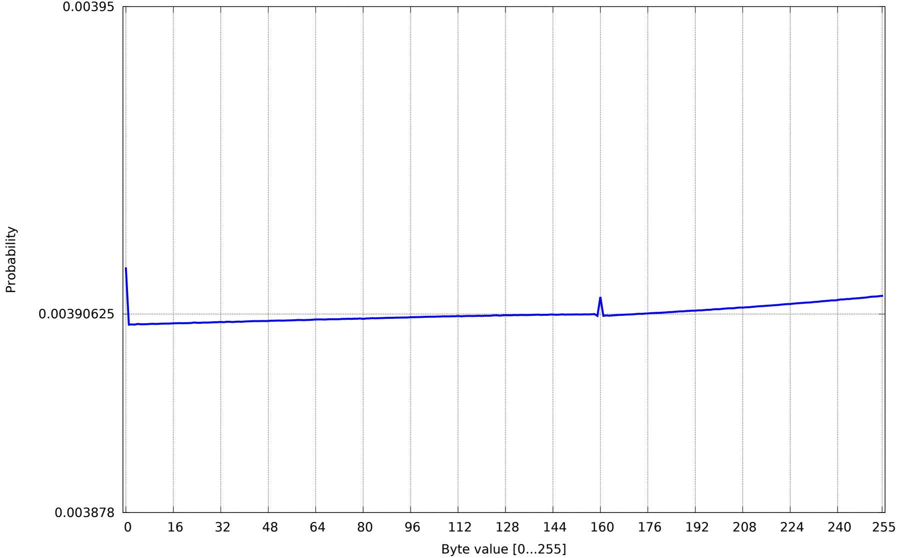
Keystream distribution at position 158



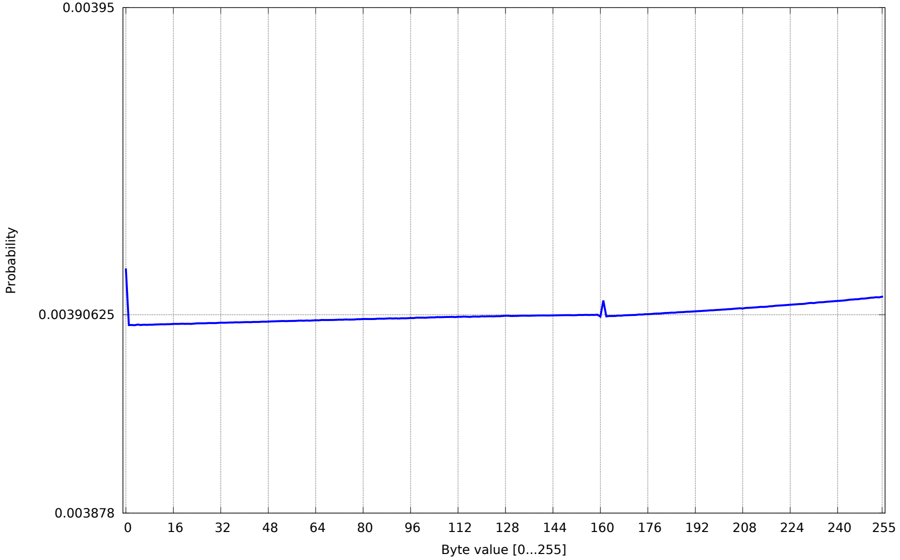
Keystream distribution at position 159



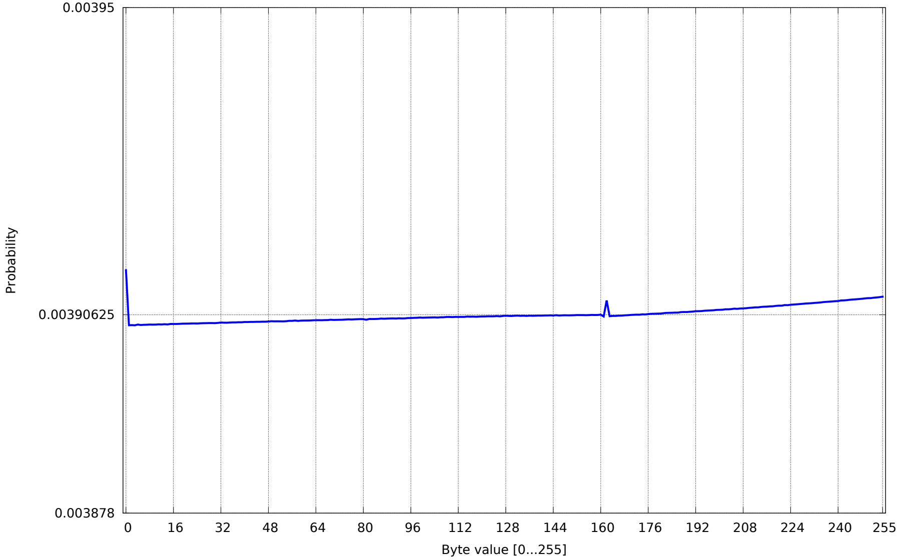
Keystream distribution at position 160



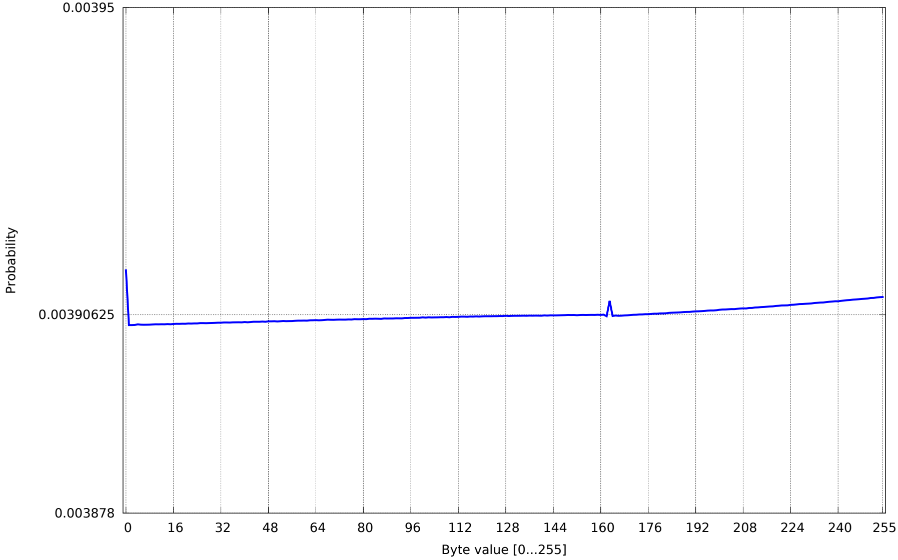
Keystream distribution at position 161



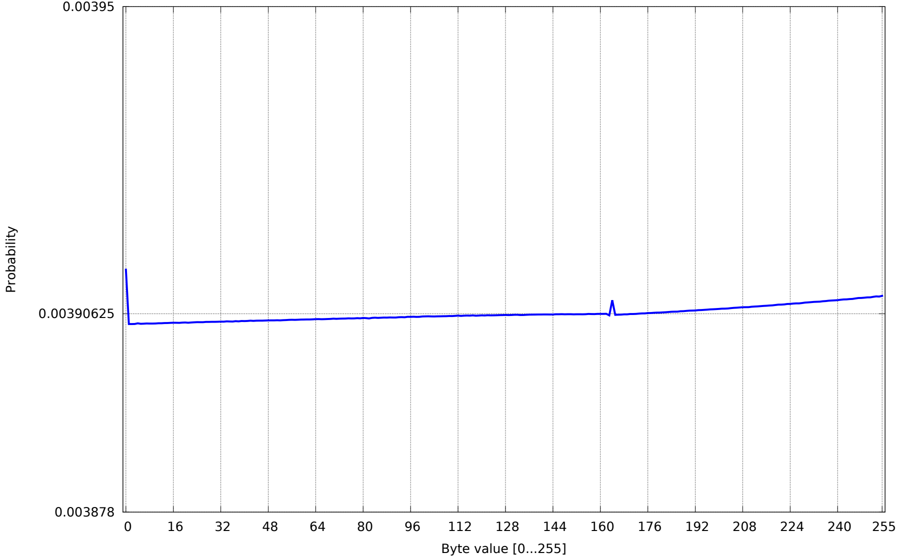
Keystream distribution at position 162



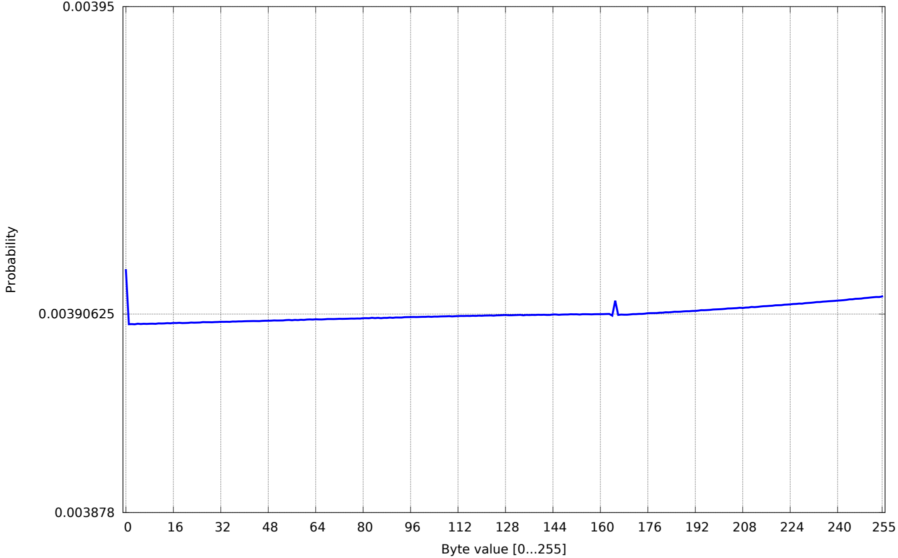
Keystream distribution at position 163



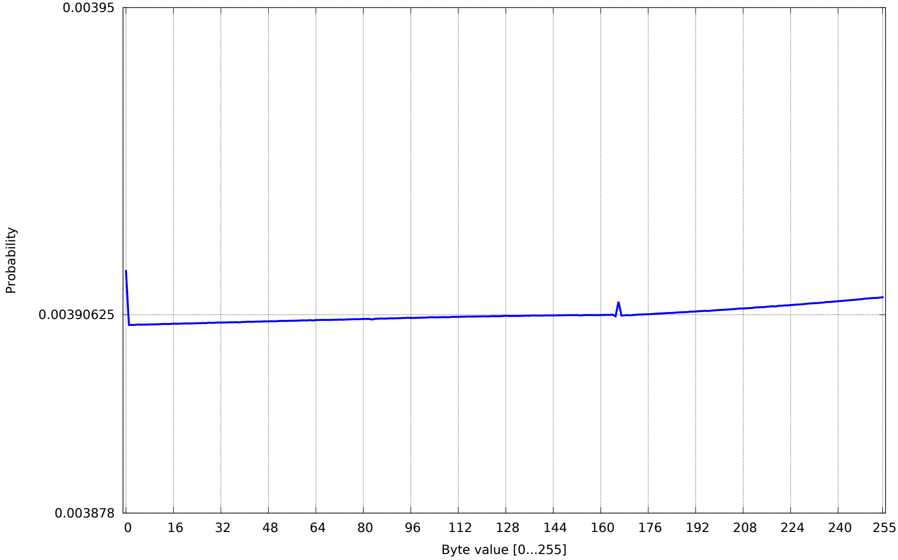
Keystream distribution at position 164



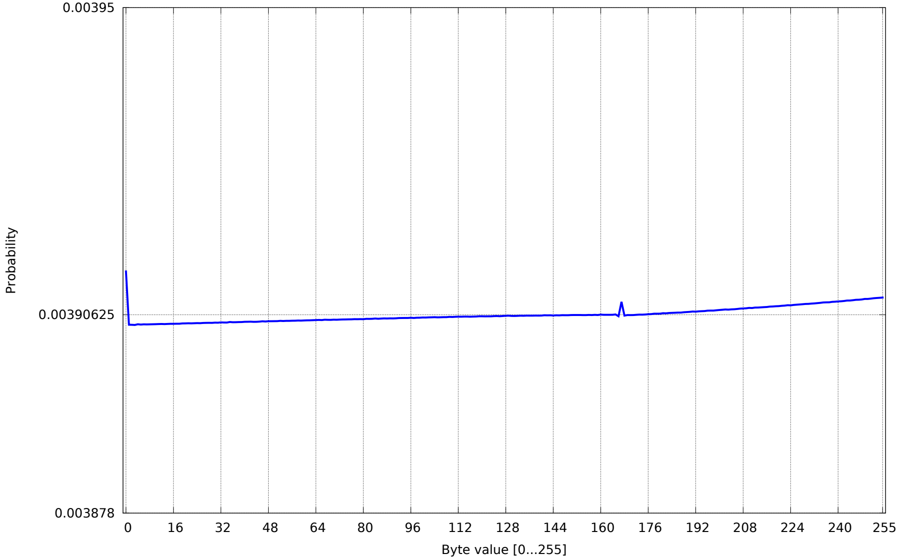
Keystream distribution at position 165



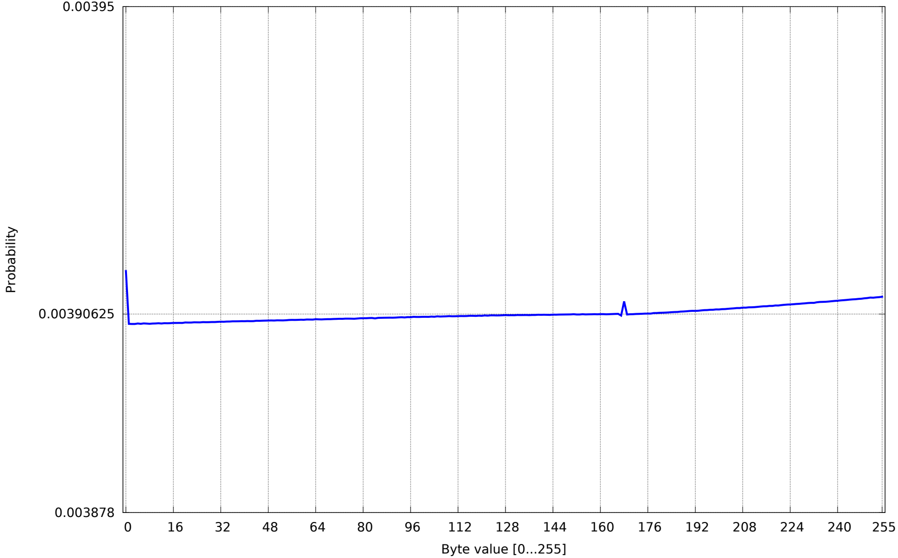
Keystream distribution at position 166



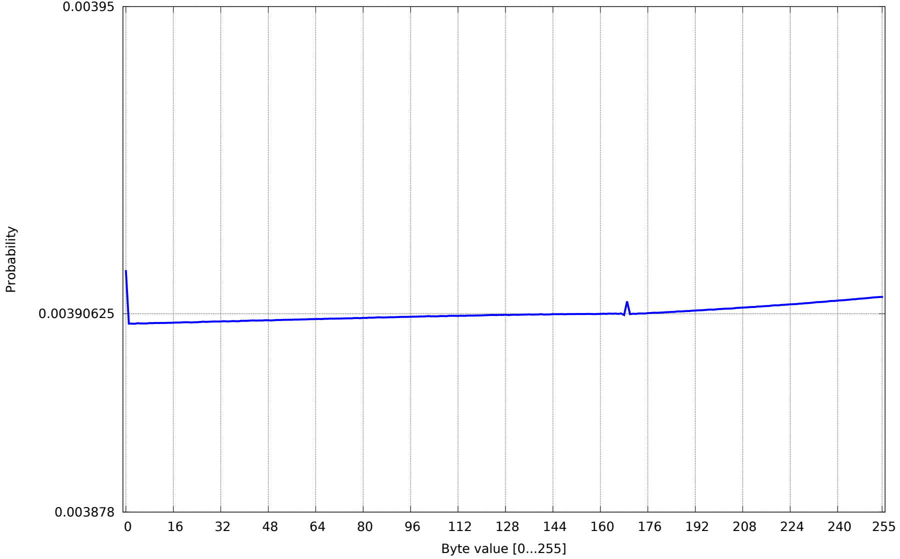
Keystream distribution at position 167



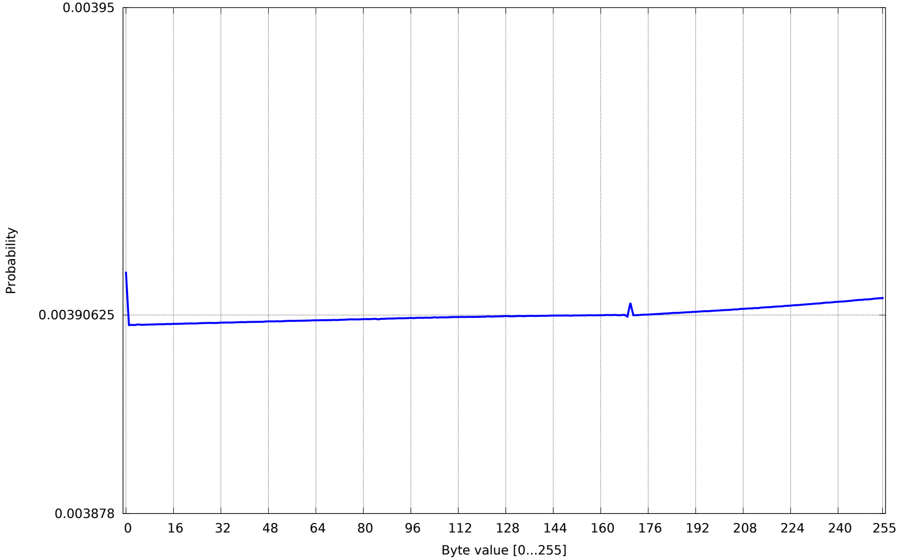
Keystream distribution at position 168



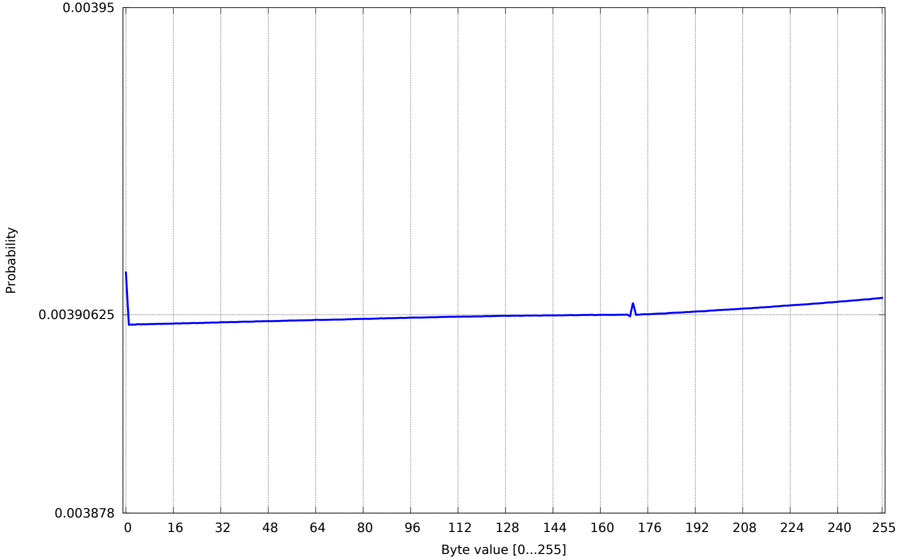
Keystream distribution at position 169



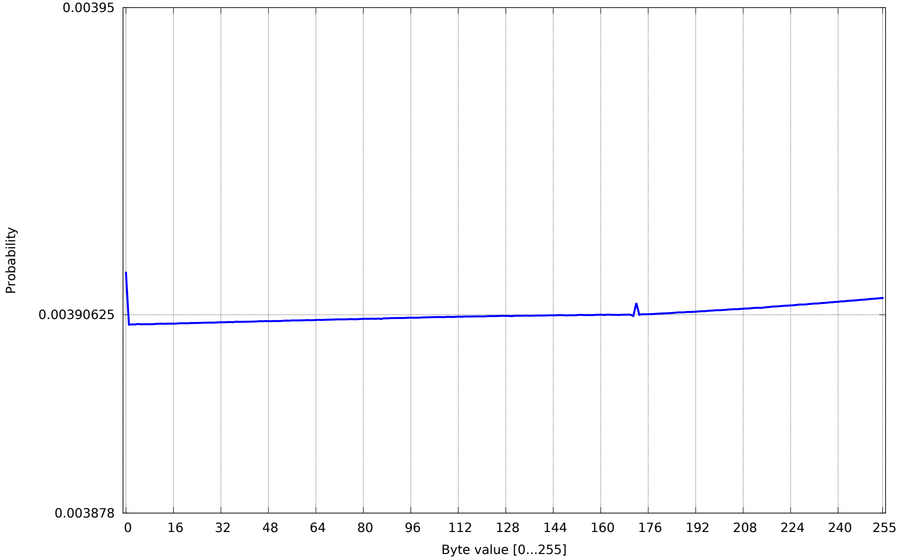
Keystream distribution at position 170



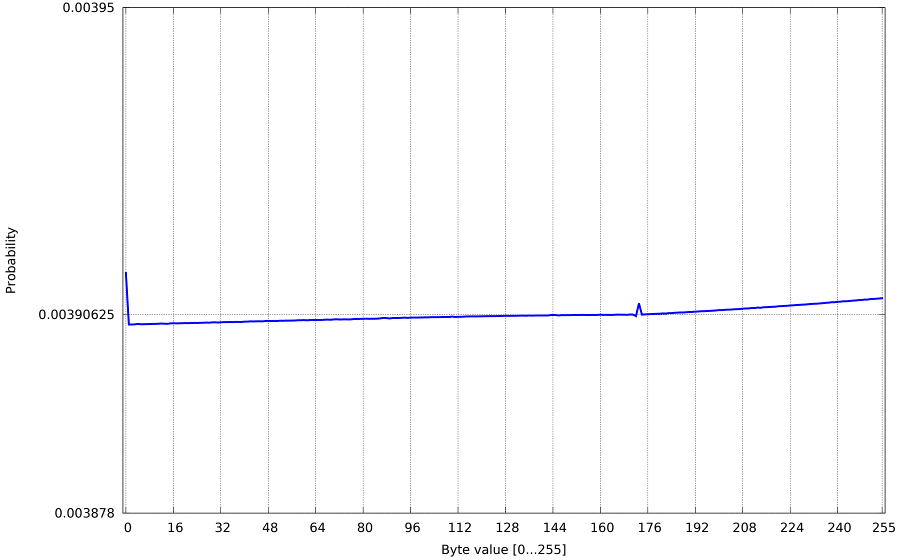
Keystream distribution at position 171



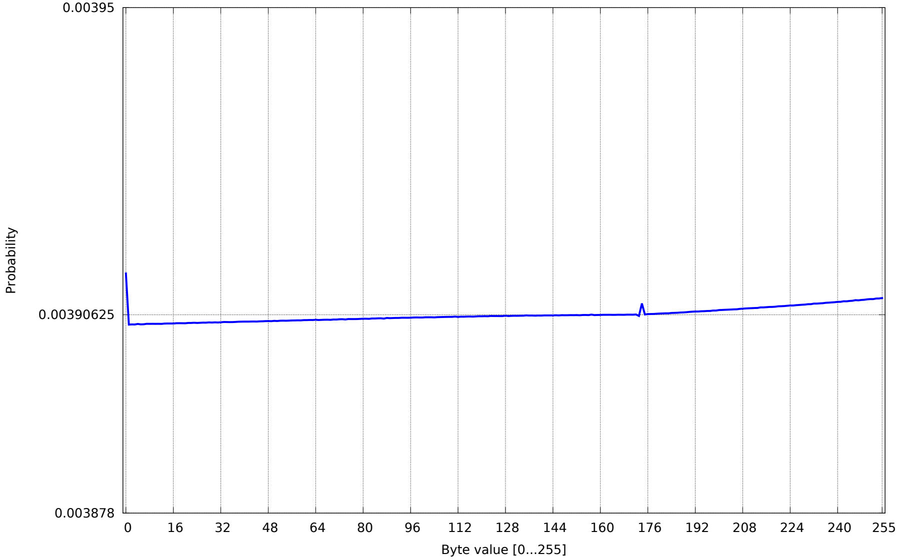
Keystream distribution at position 172



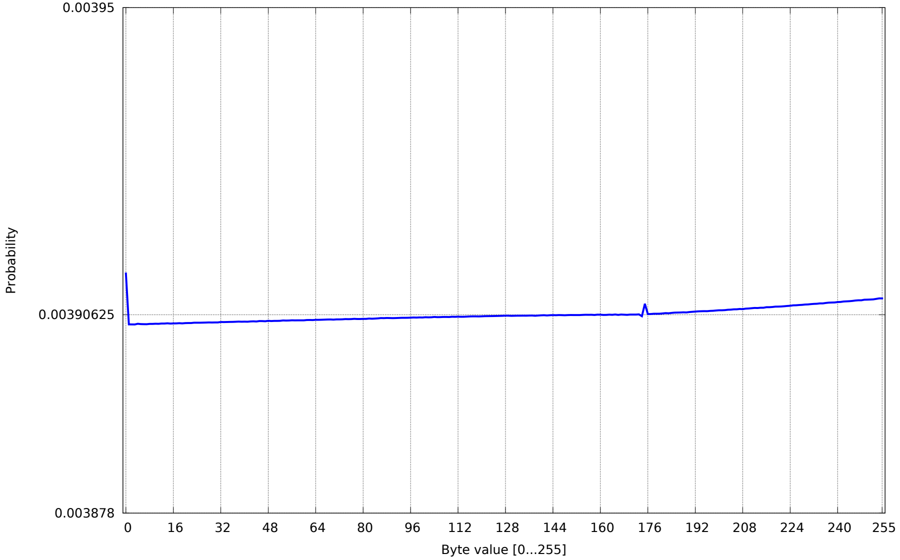
Keystream distribution at position 173



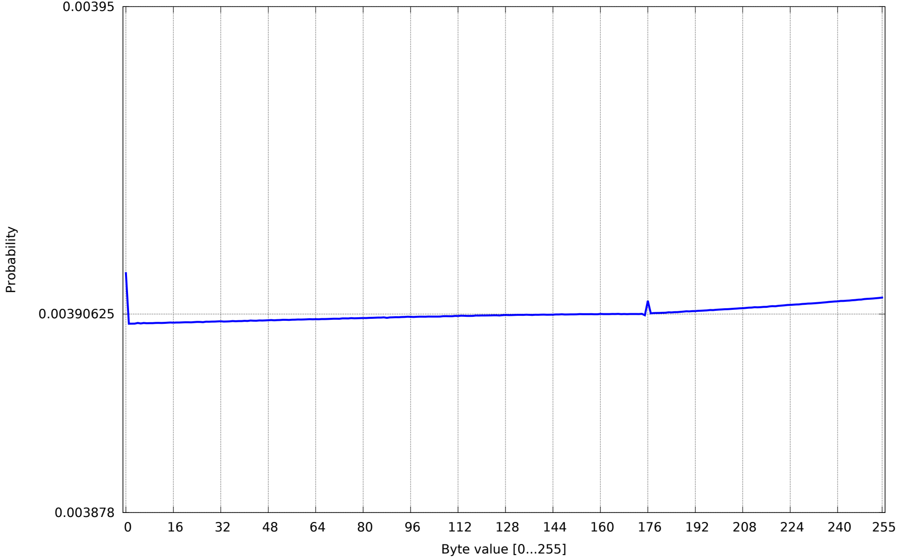
Keystream distribution at position 174



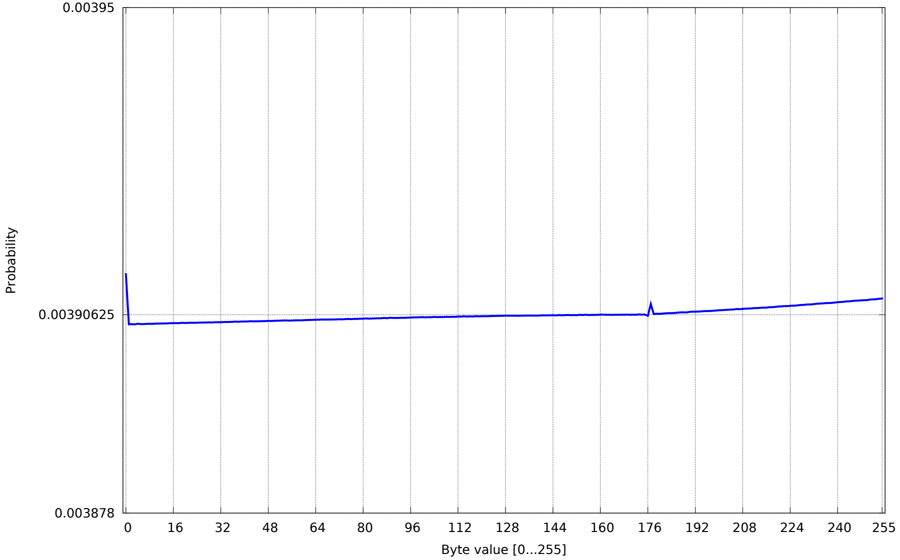
Keystream distribution at position 175



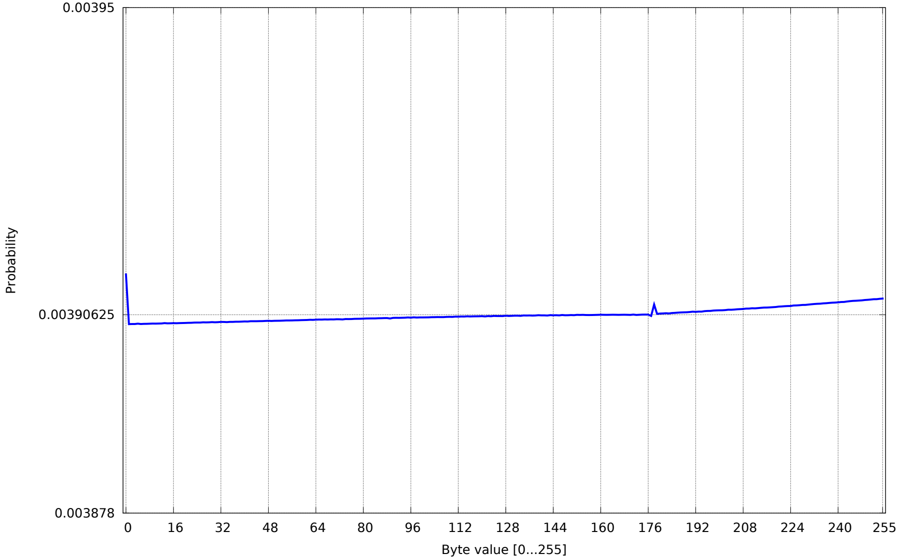
Keystream distribution at position 176



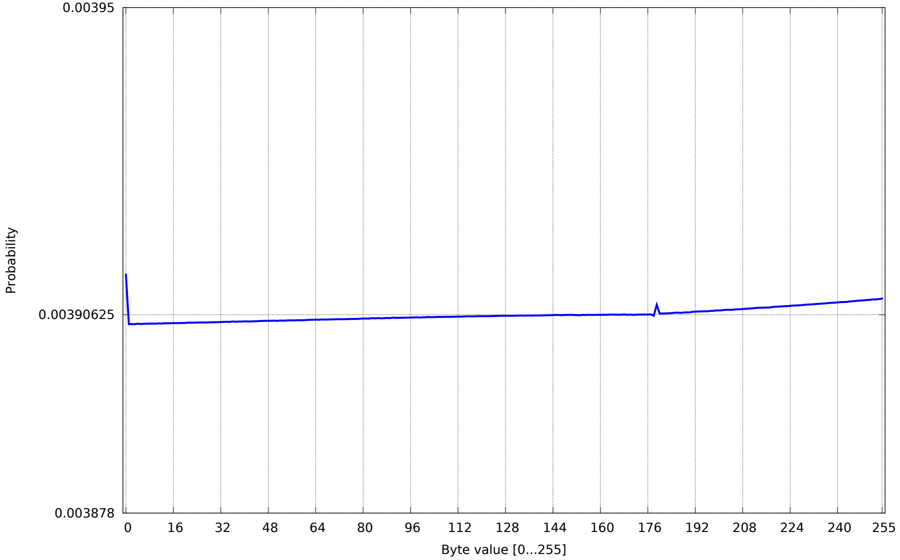
Keystream distribution at position 177



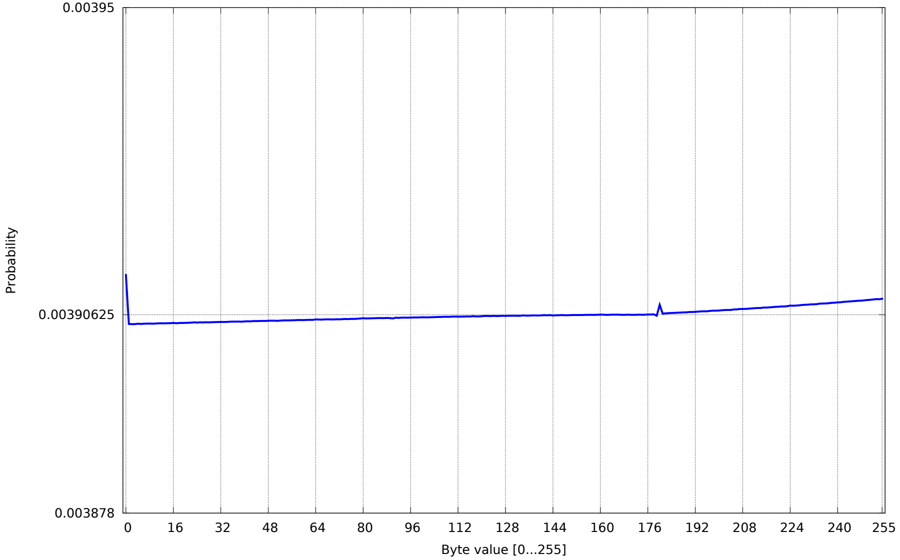
Keystream distribution at position 178



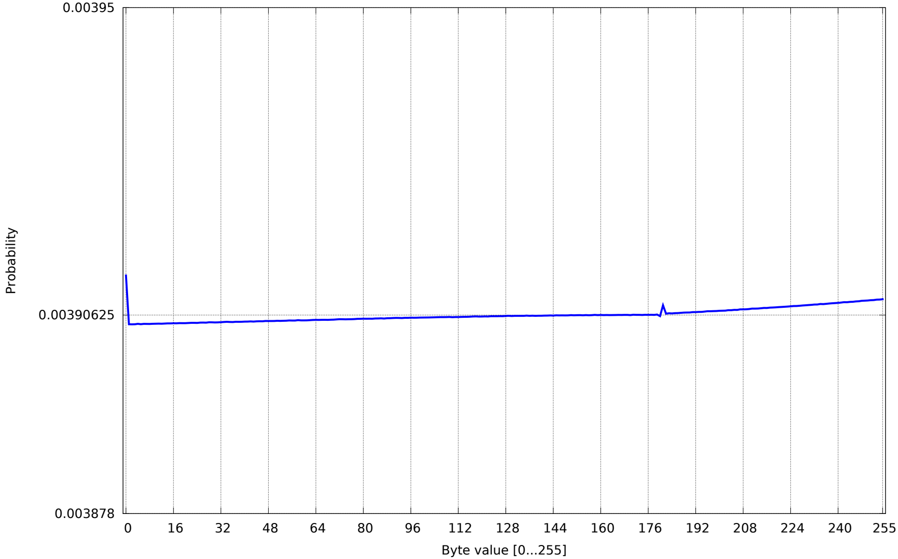
Keystream distribution at position 179



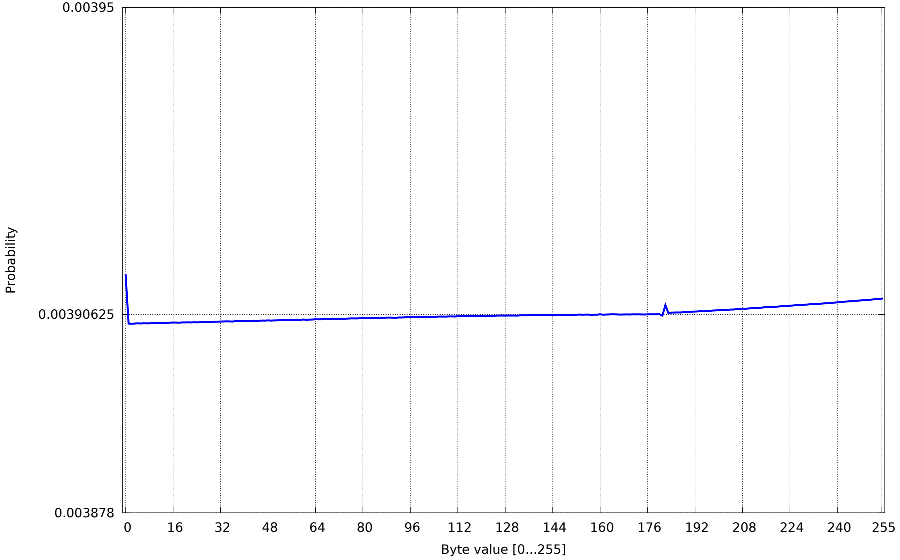
Keystream distribution at position 180



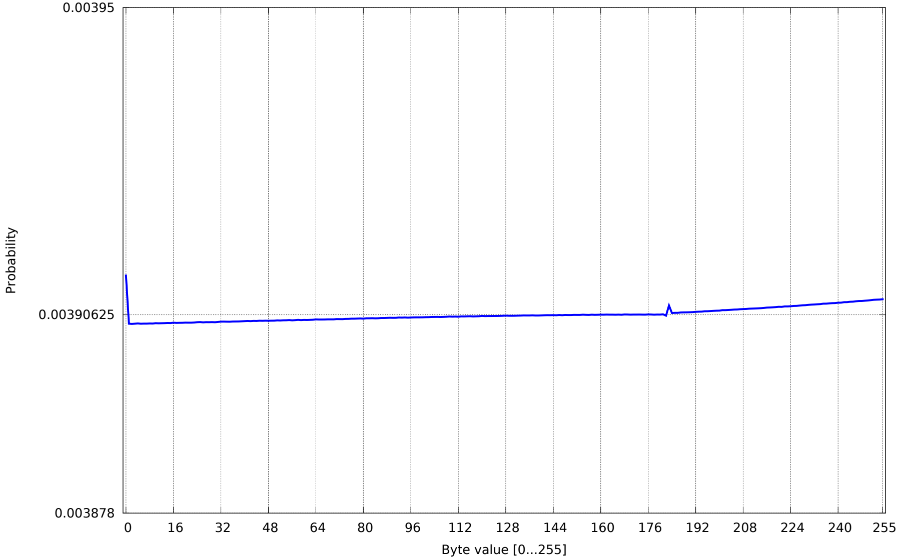
Keystream distribution at position 181



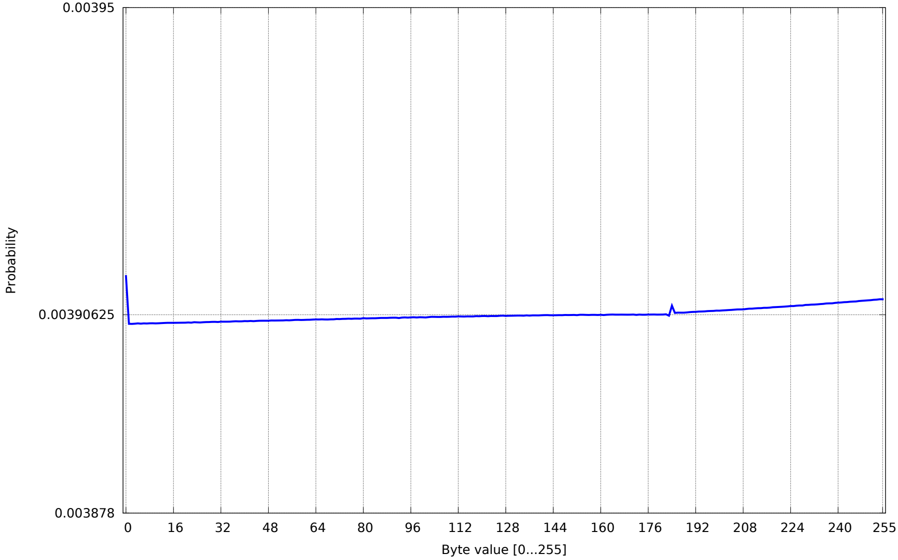
Keystream distribution at position 182



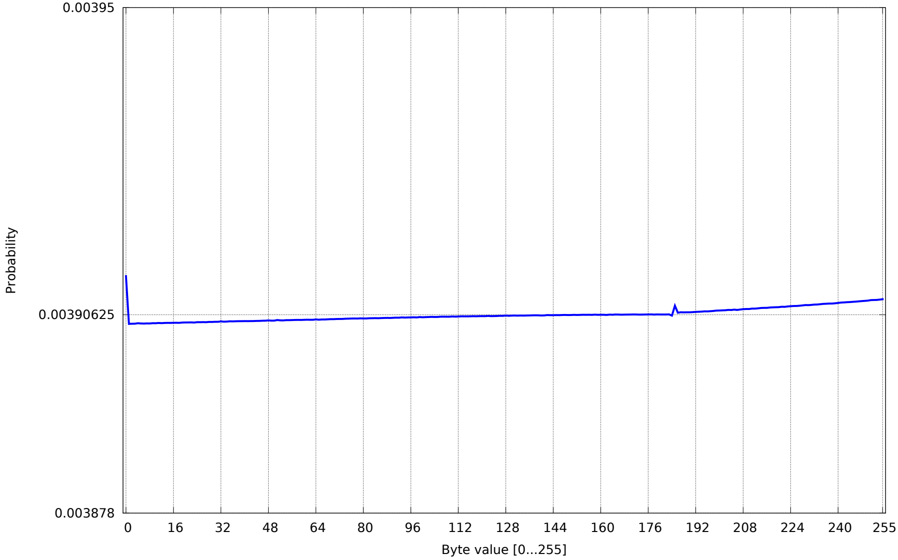
Keystream distribution at position 183



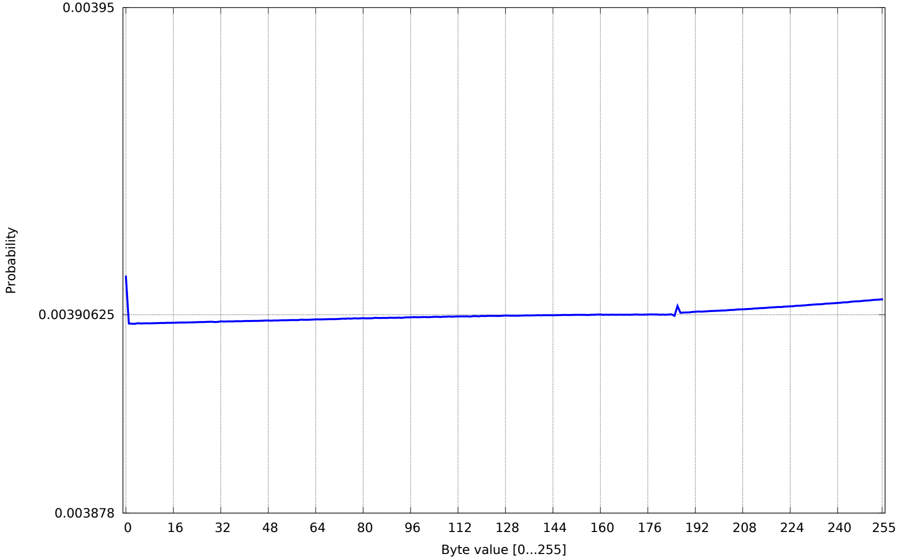
Keystream distribution at position 184



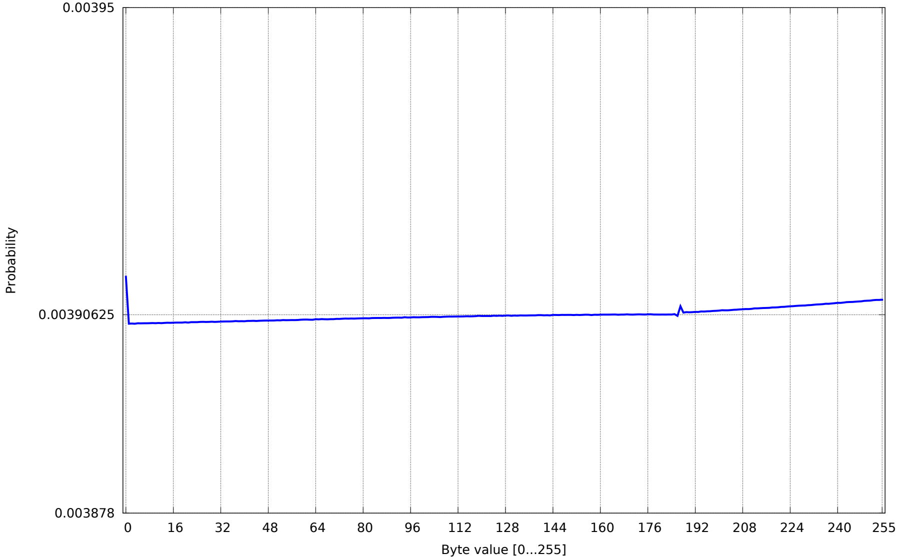
Keystream distribution at position 185



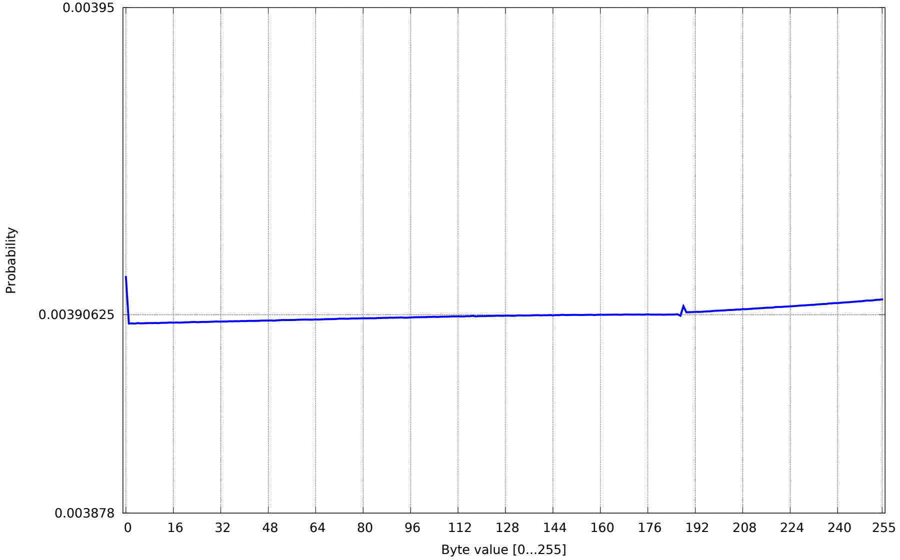
Keystream distribution at position 186



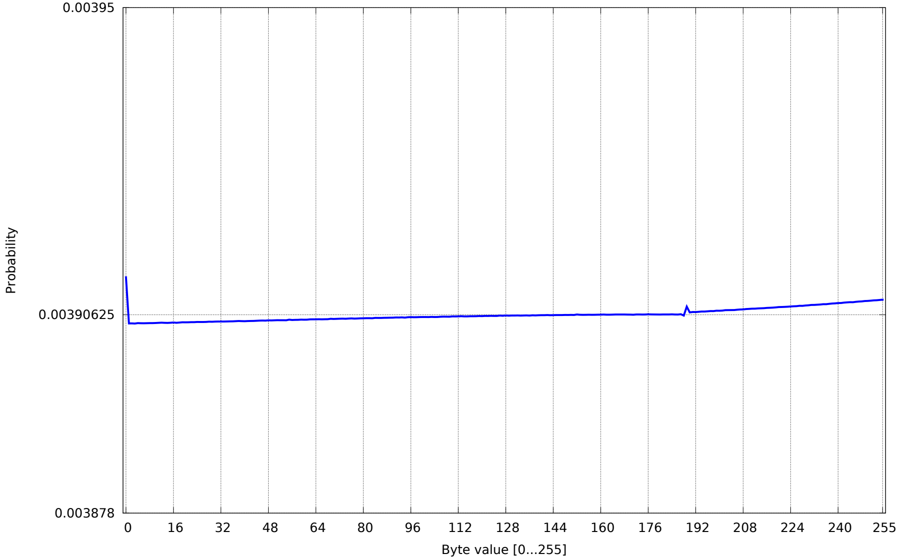
Keystream distribution at position 187



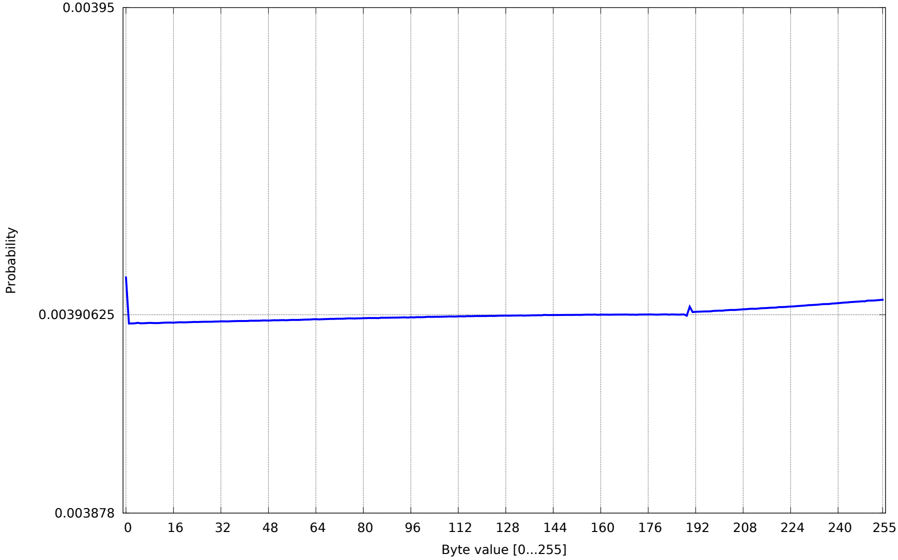
Keystream distribution at position 188



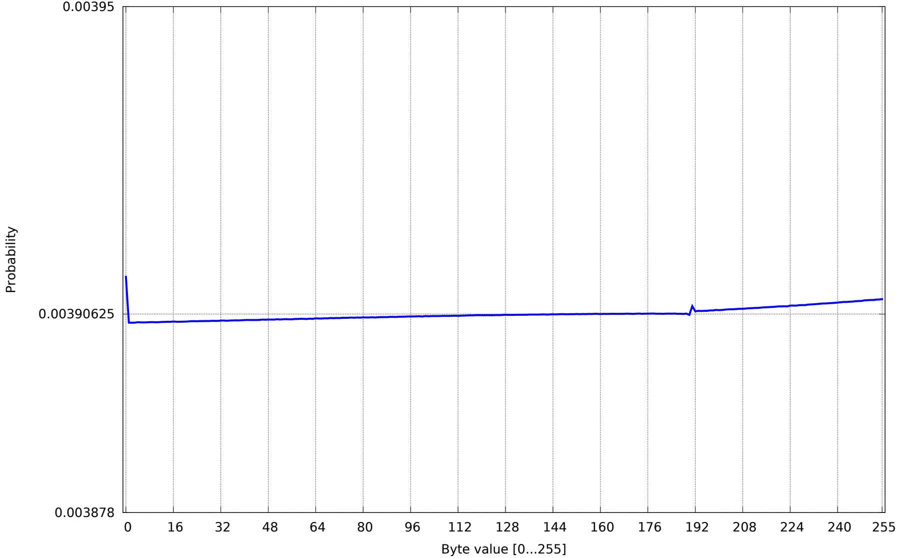
Keystream distribution at position 189



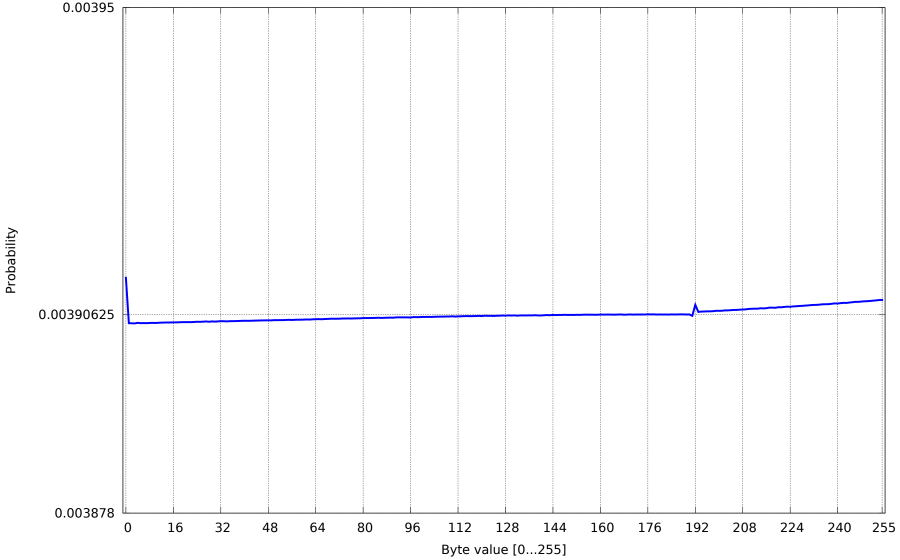
Keystream distribution at position 190



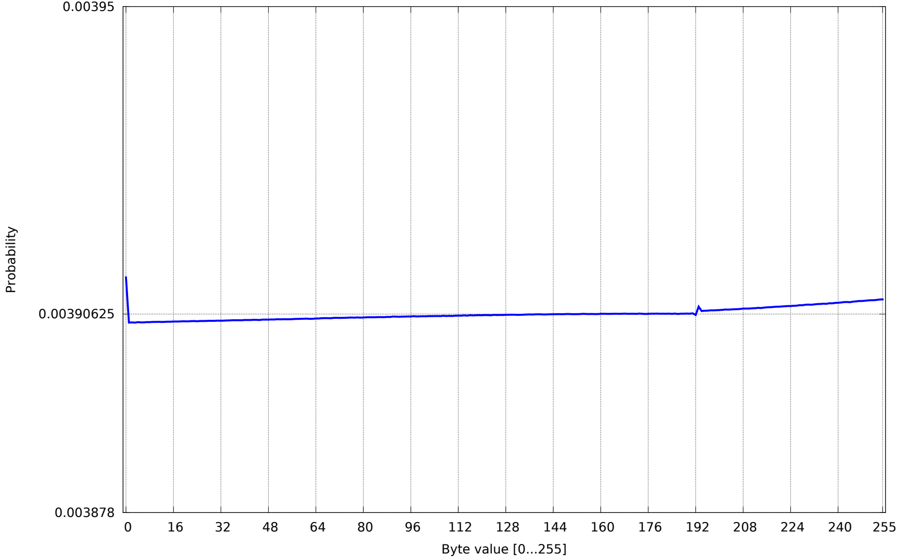
Keystream distribution at position 191



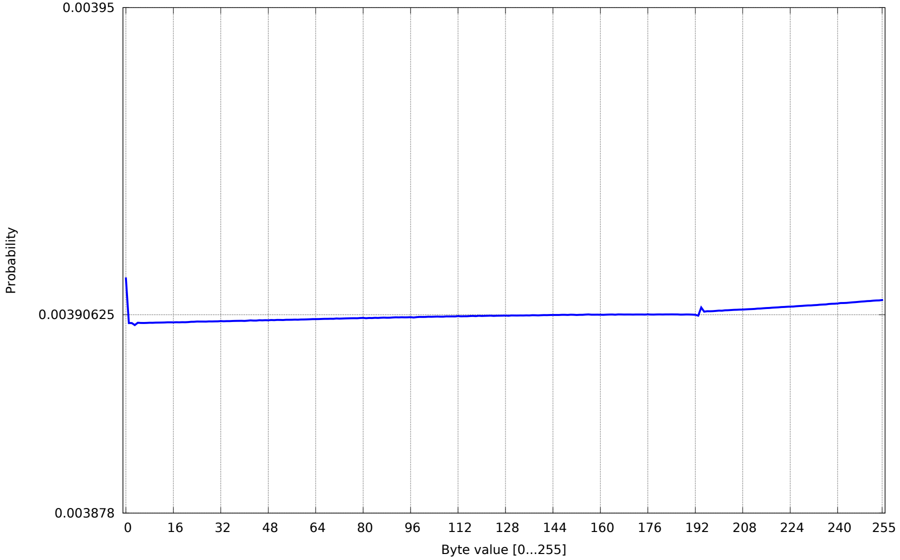
Keystream distribution at position 192



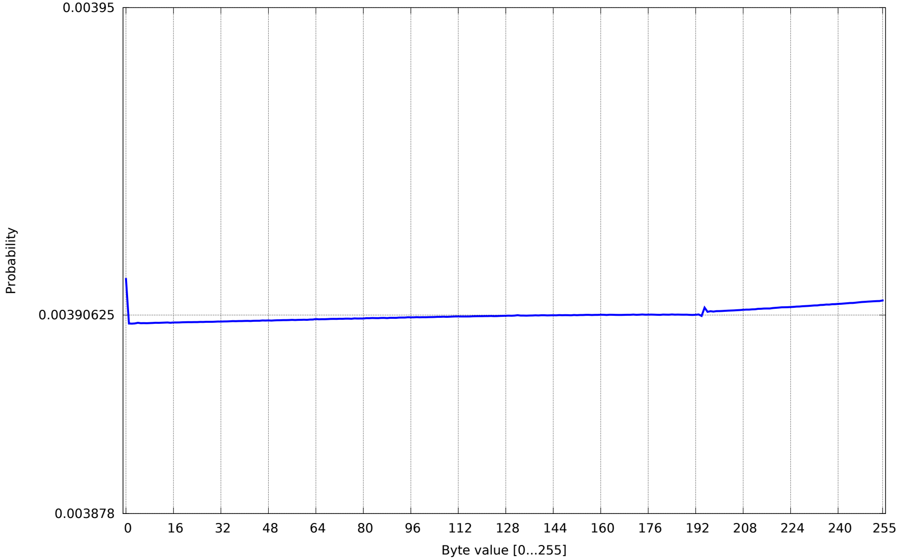
Keystream distribution at position 193



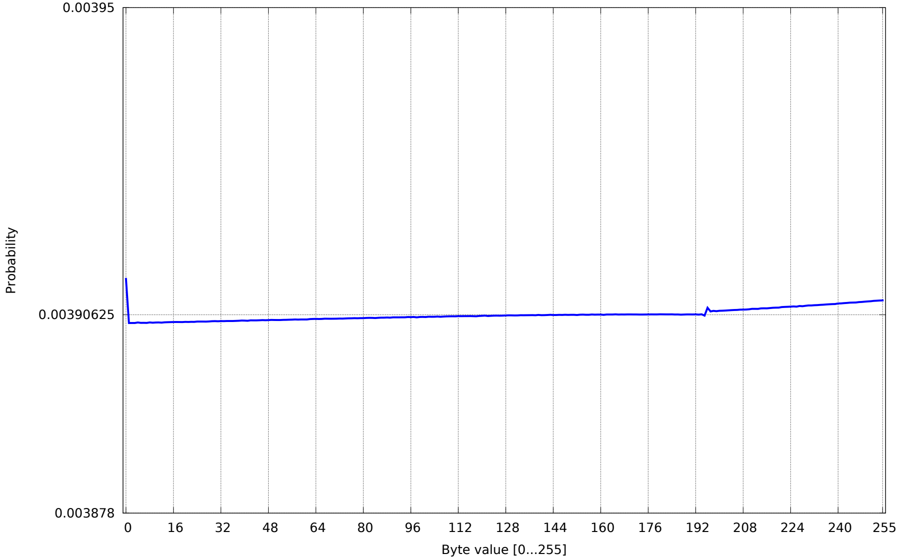
Keystream distribution at position 194



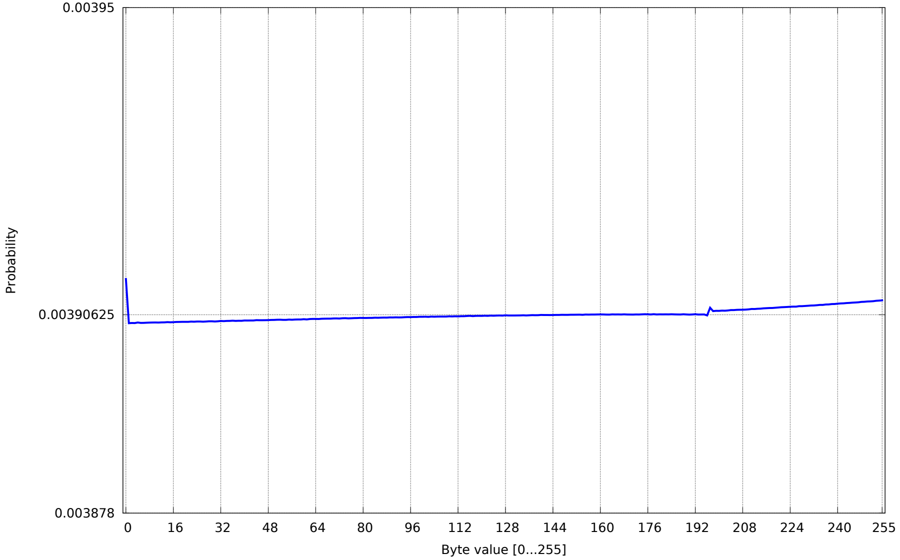
Keystream distribution at position 195



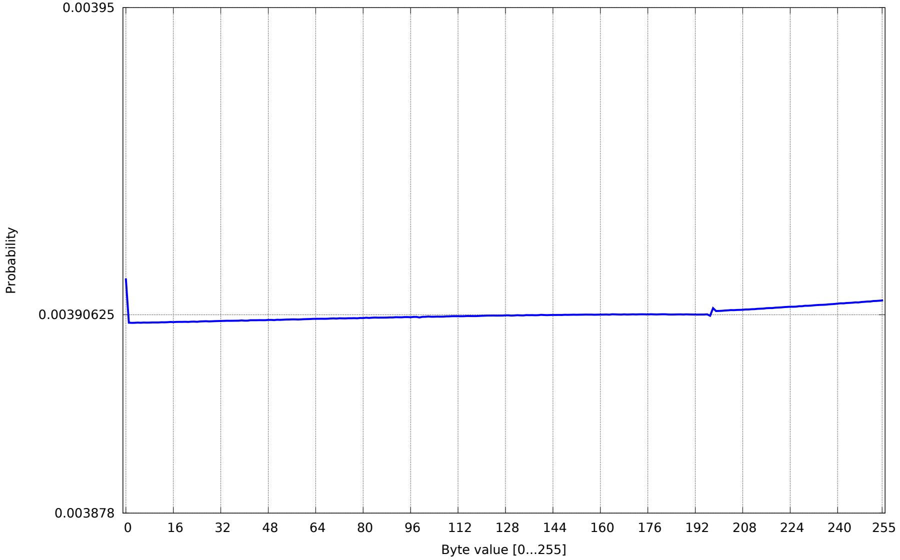
Keystream distribution at position 196



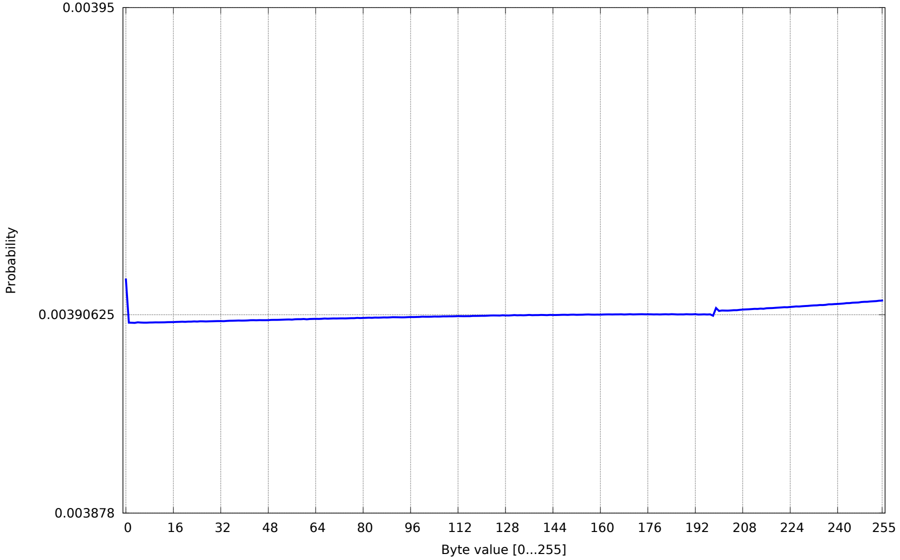
Keystream distribution at position 197



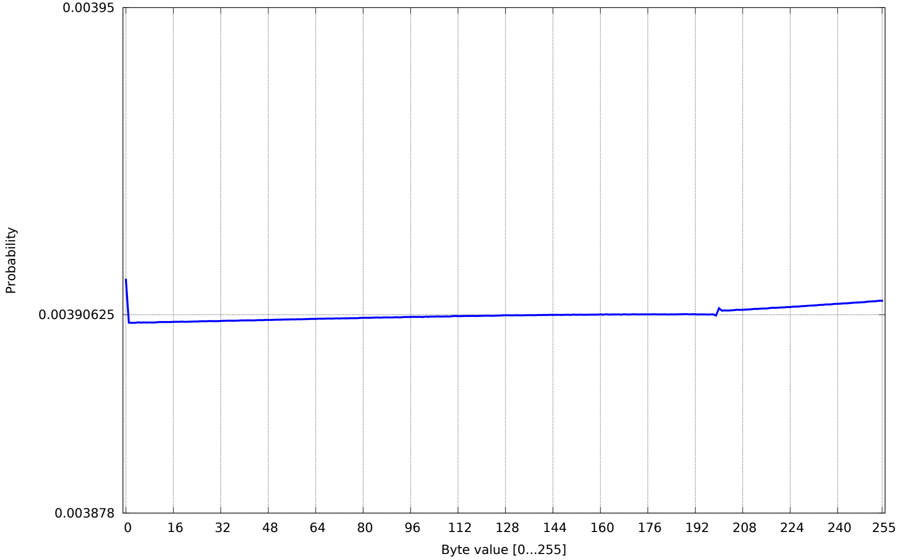
Keystream distribution at position 198



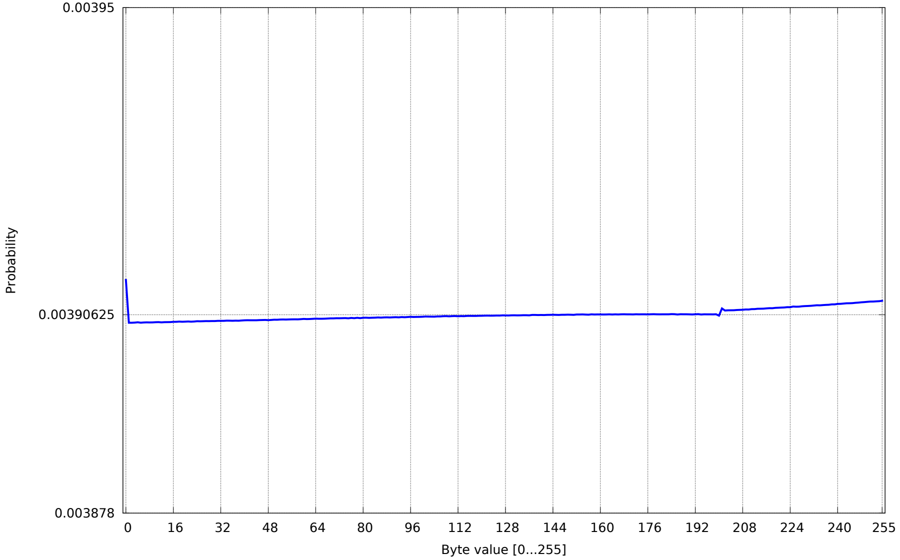
Keystream distribution at position 199



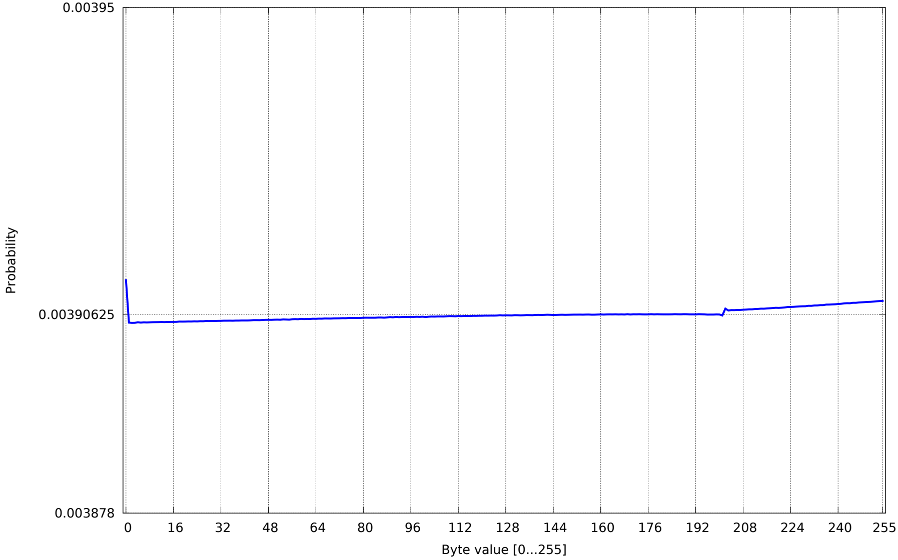
Keystream distribution at position 200



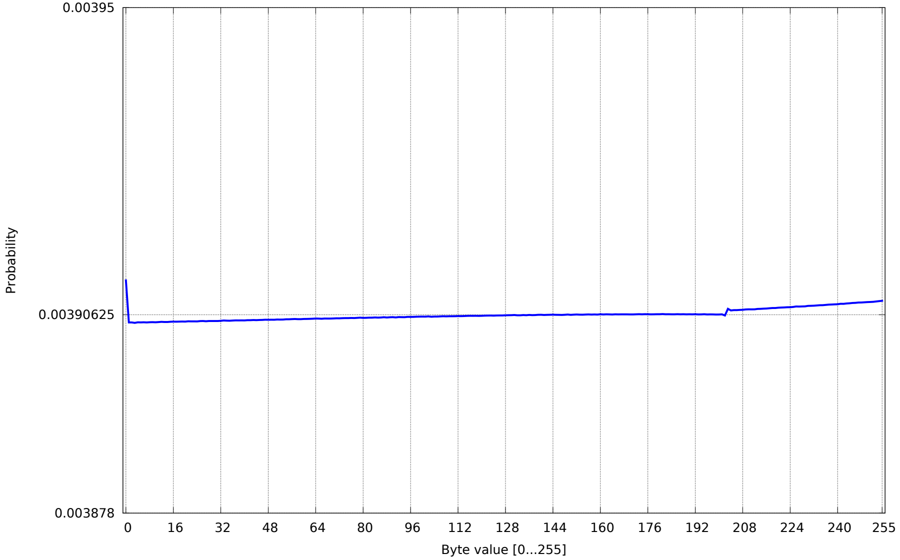
Keystream distribution at position 201



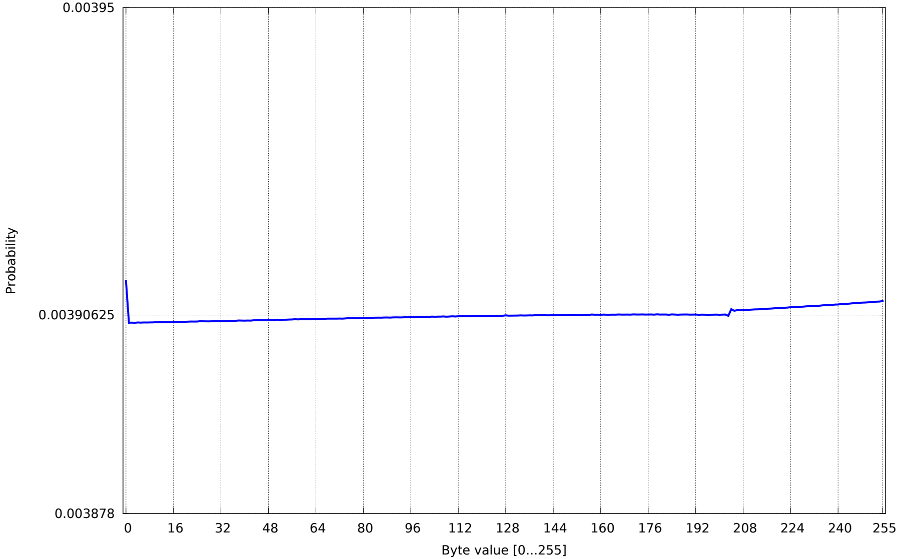
Keystream distribution at position 202



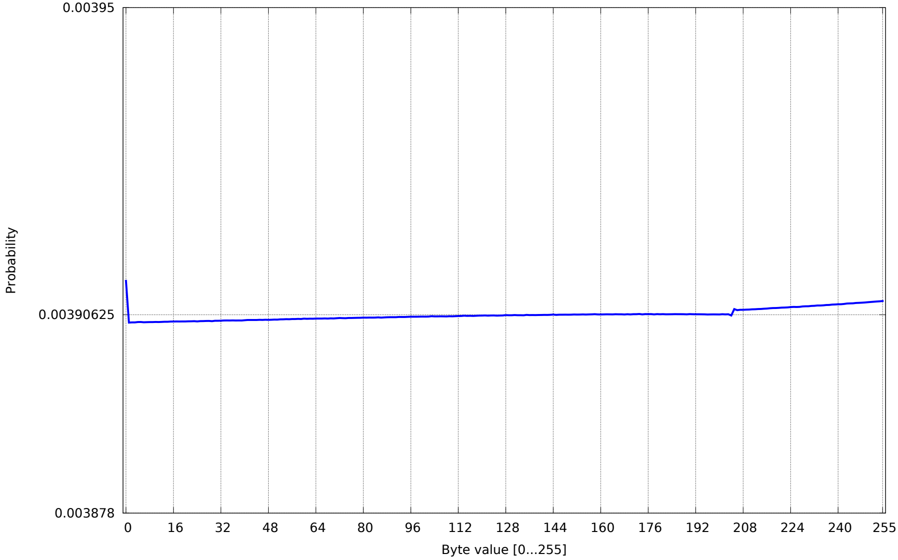
Keystream distribution at position 203



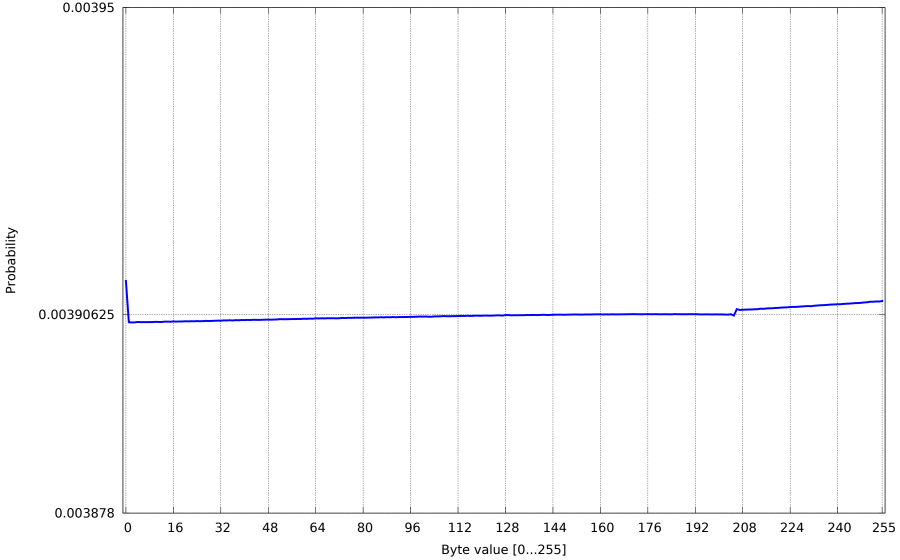
Keystream distribution at position 204



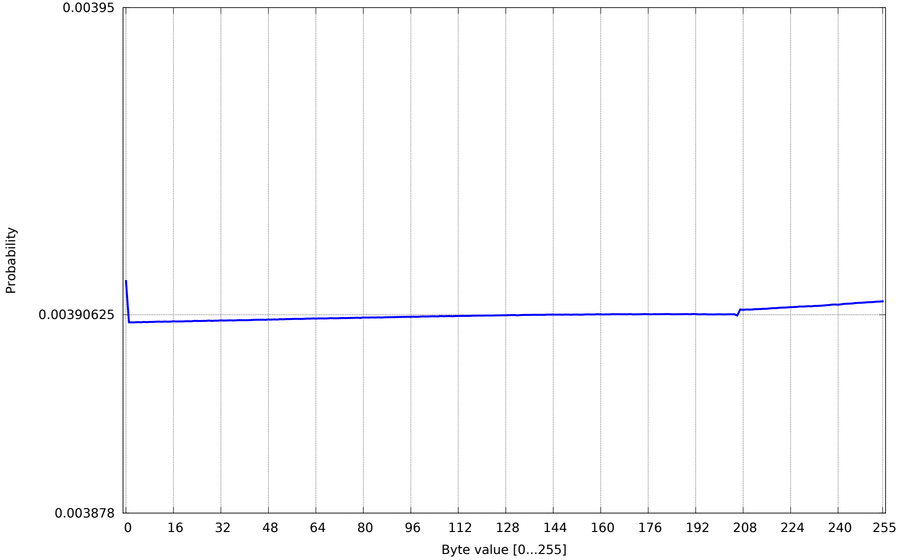
Keystream distribution at position 205



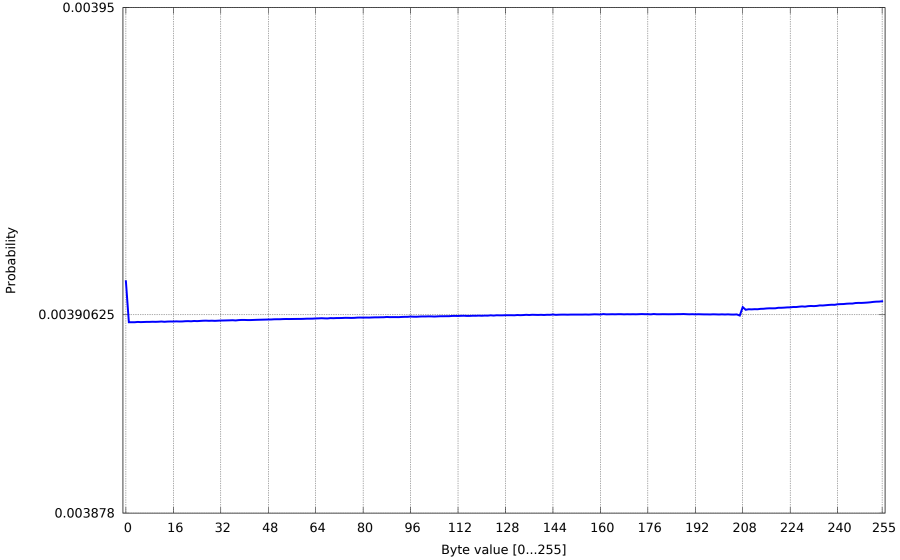
Keystream distribution at position 206



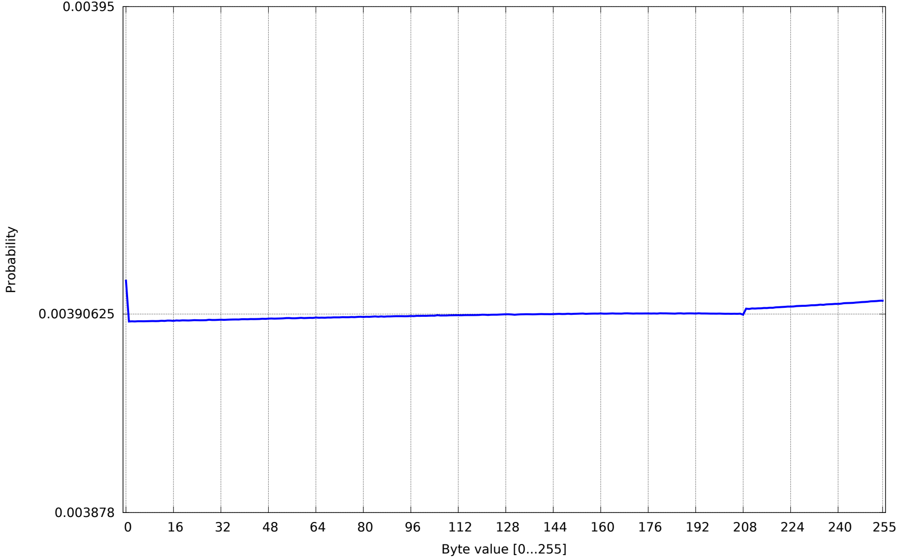
Keystream distribution at position 207



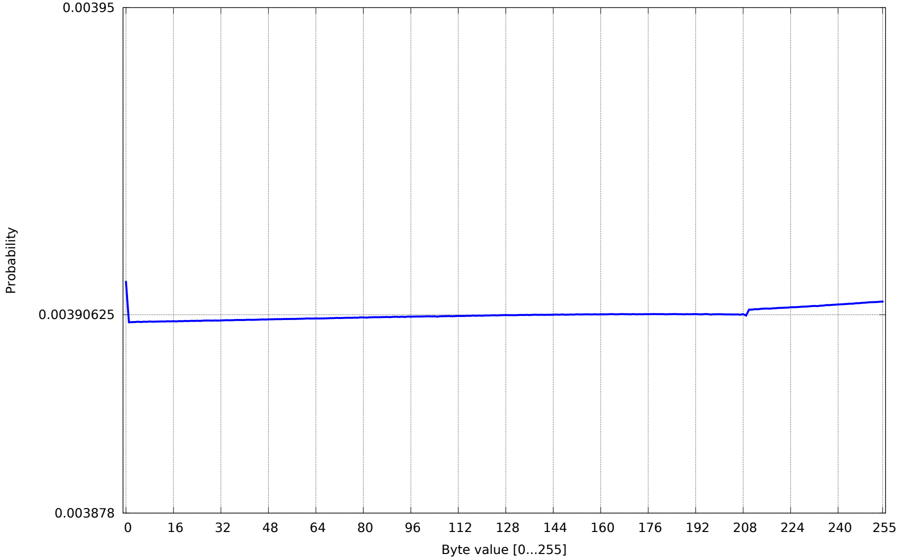
Keystream distribution at position 208



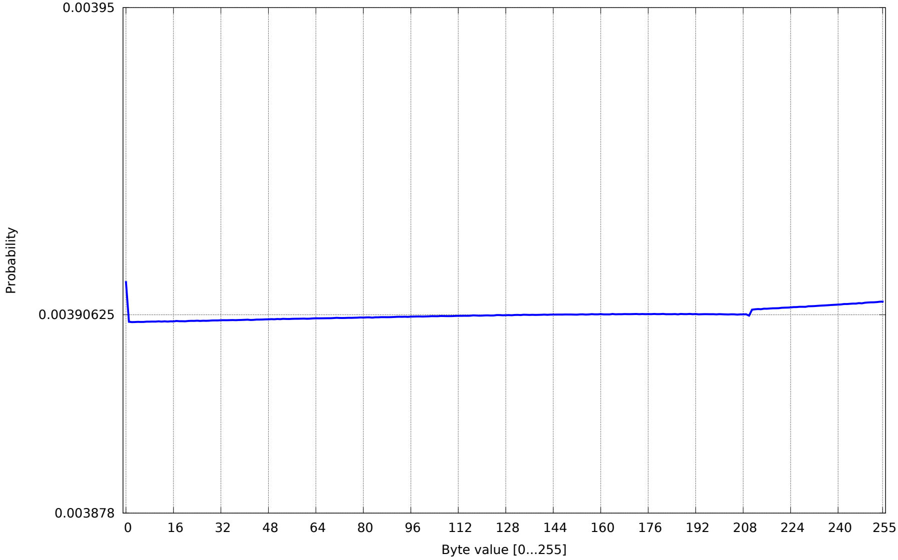
Keystream distribution at position 209



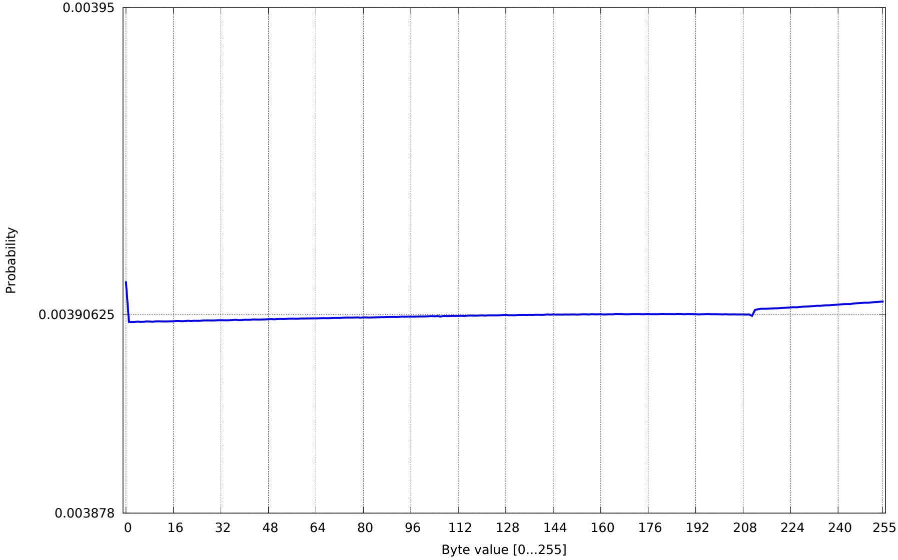
Keystream distribution at position 210



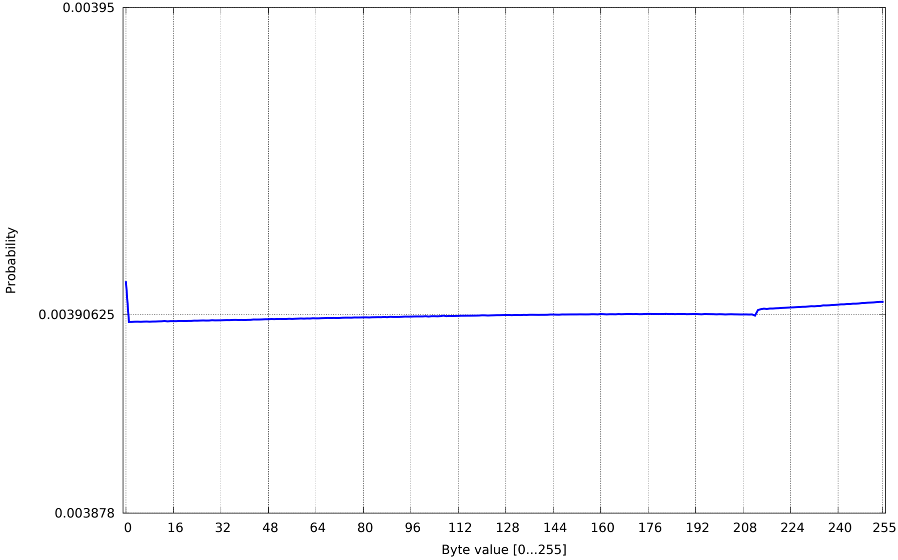
Keystream distribution at position 211



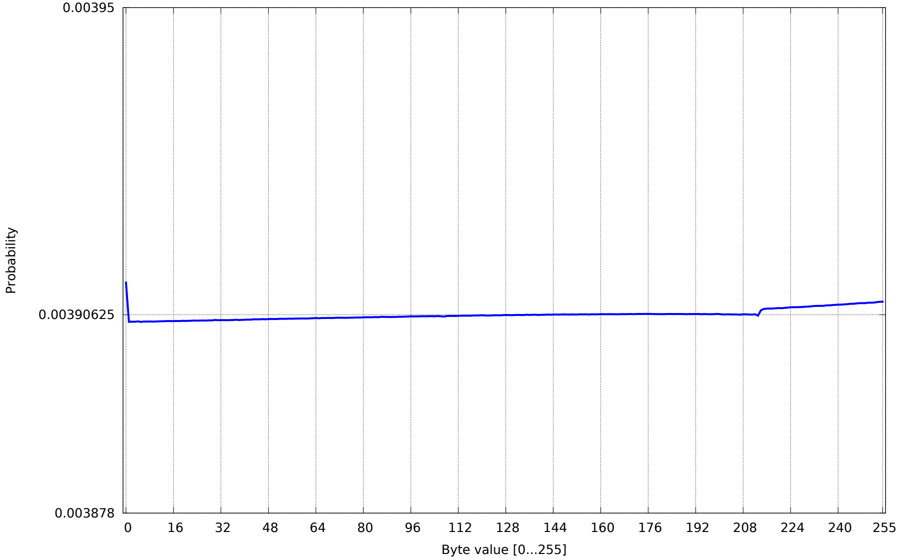
Keystream distribution at position 212



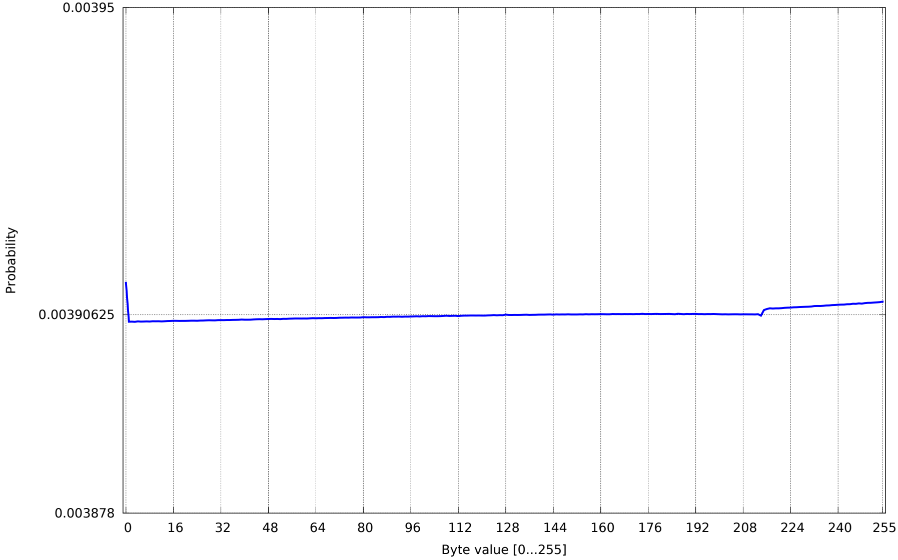
Keystream distribution at position 213



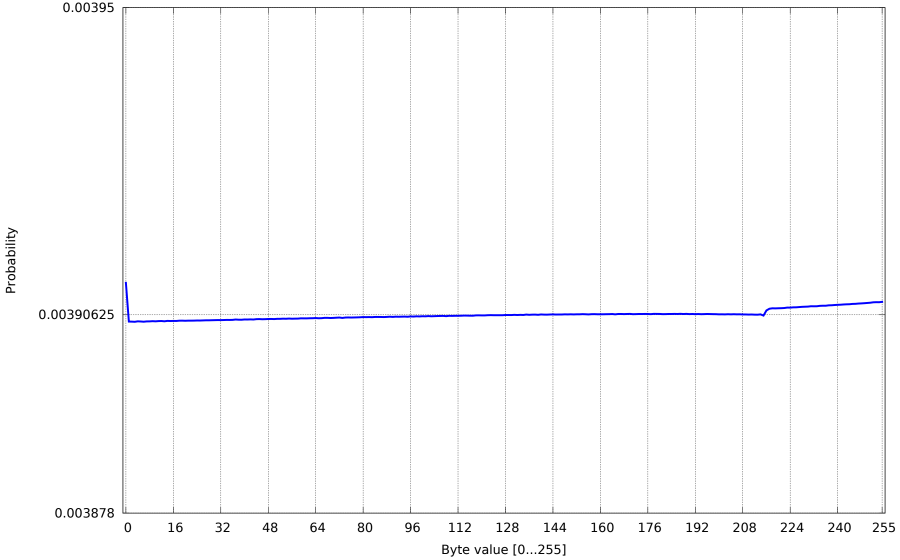
Keystream distribution at position 214



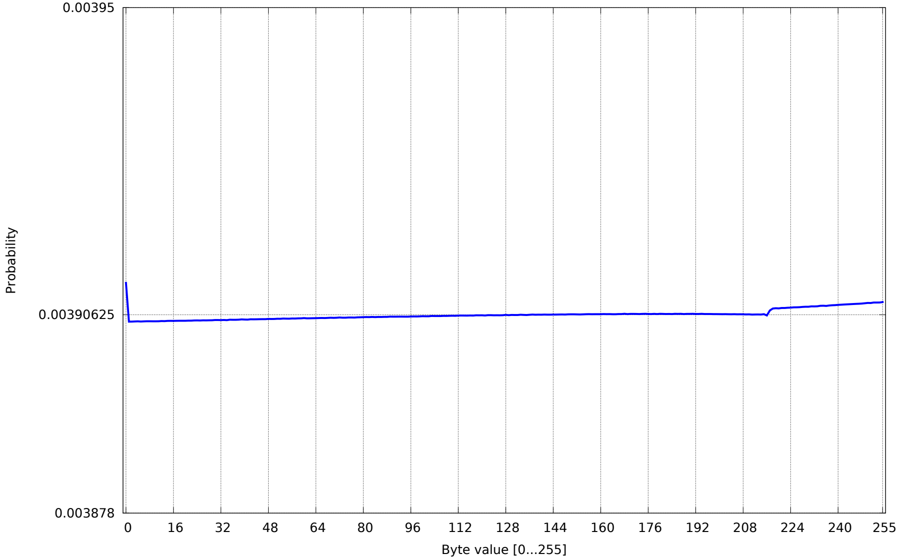
Keystream distribution at position 215



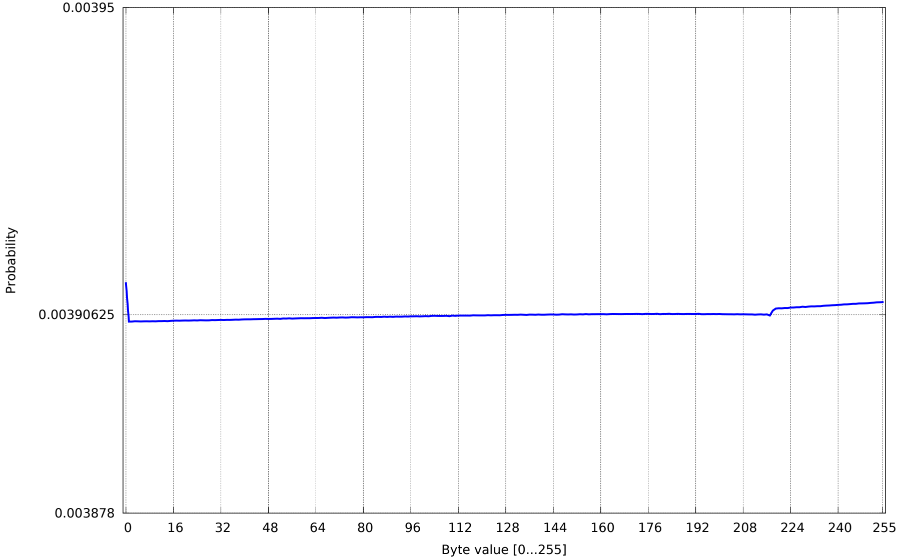
Keystream distribution at position 216



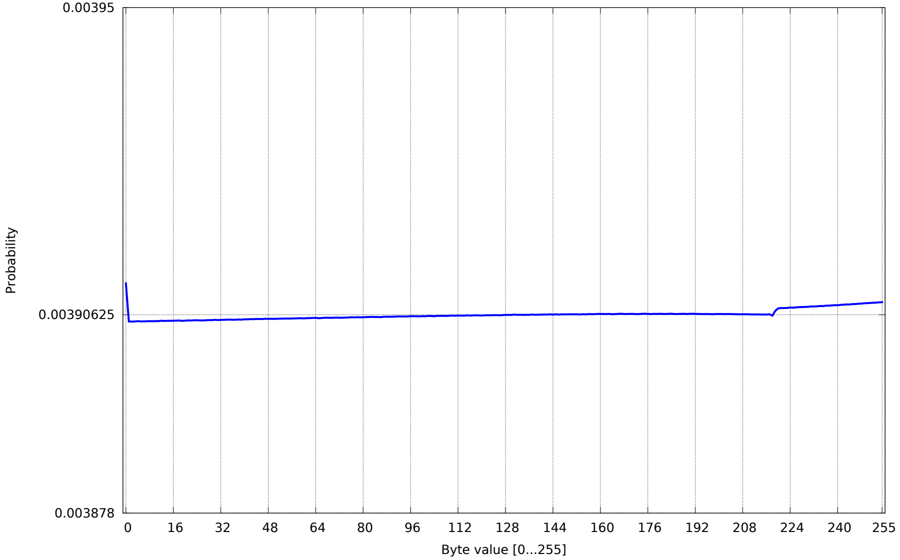
Keystream distribution at position 217



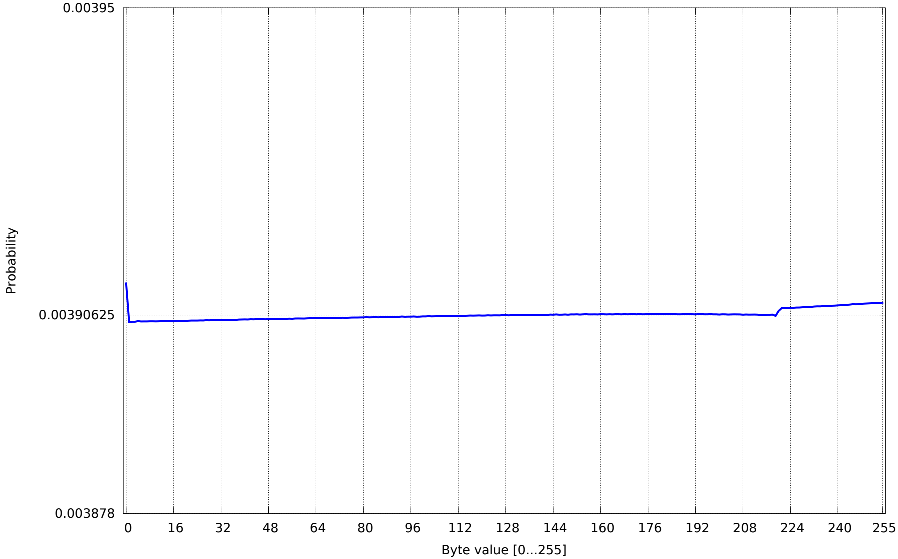
Keystream distribution at position 218



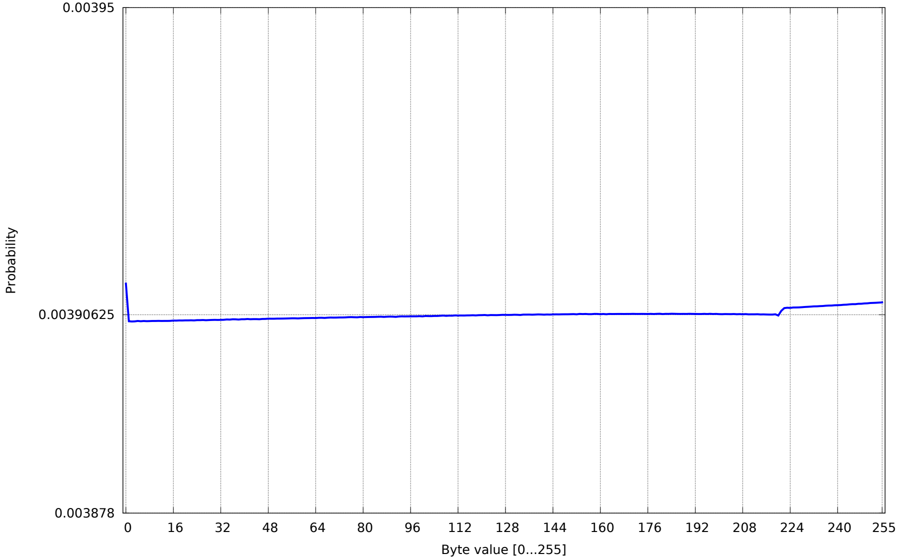
Keystream distribution at position 219



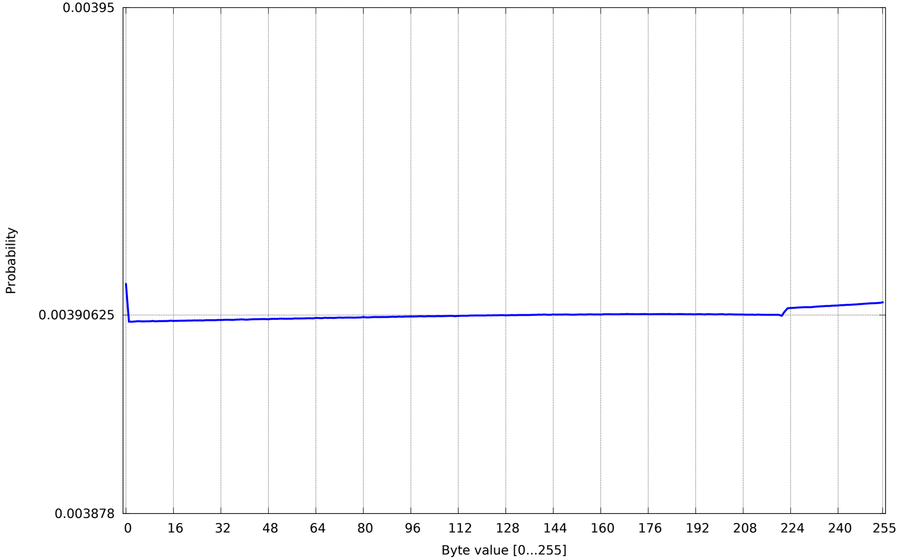
Keystream distribution at position 220



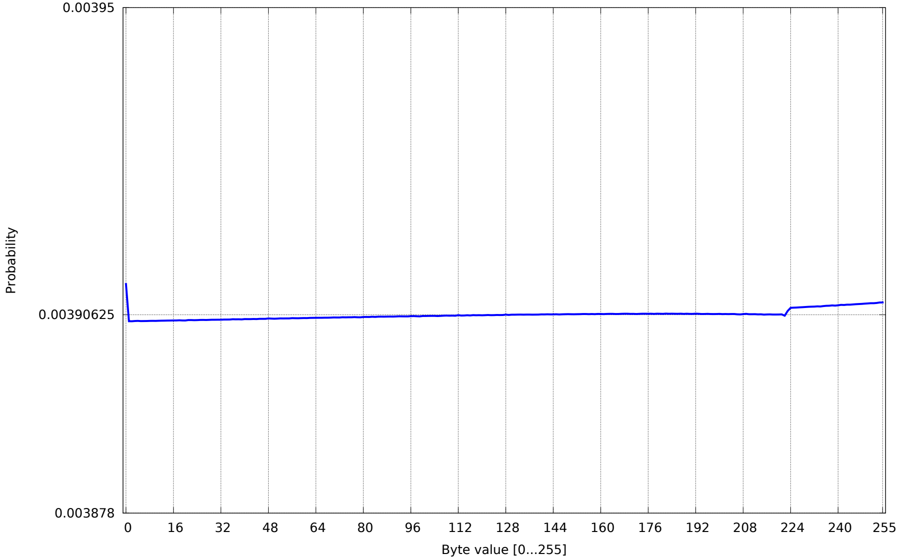
Keystream distribution at position 221



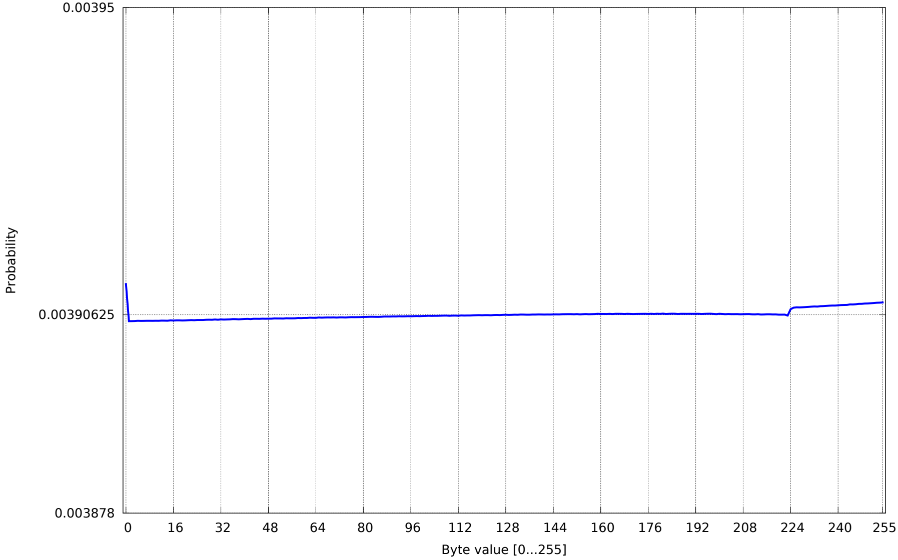
Keystream distribution at position 222



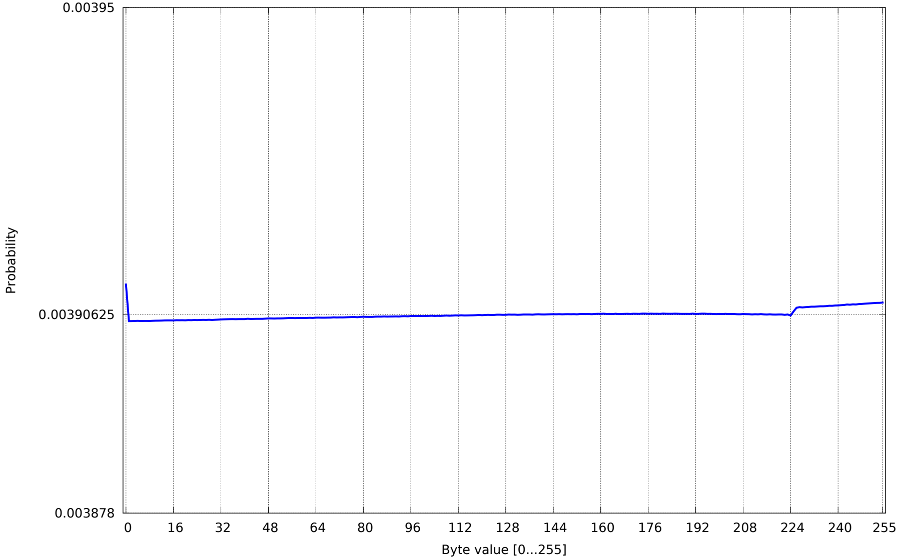
Keystream distribution at position 223



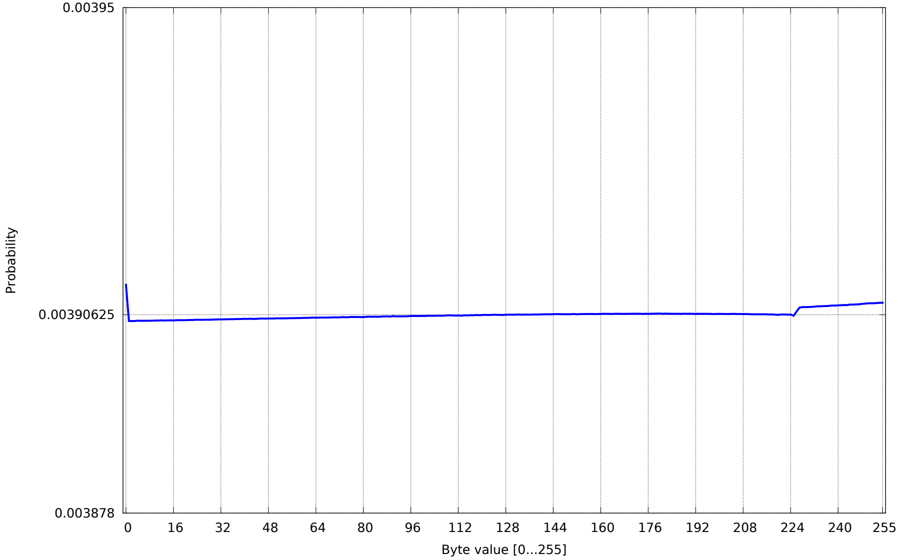
Keystream distribution at position 224



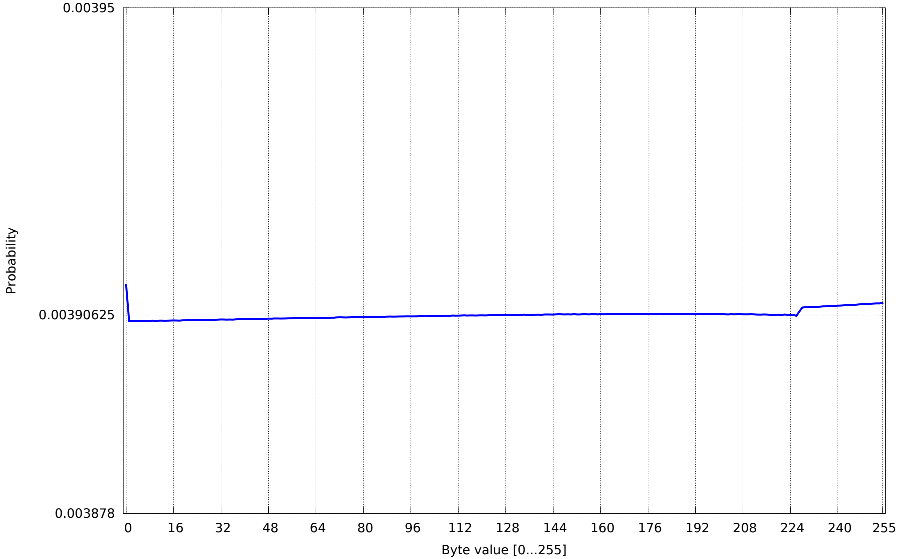
Keystream distribution at position 225



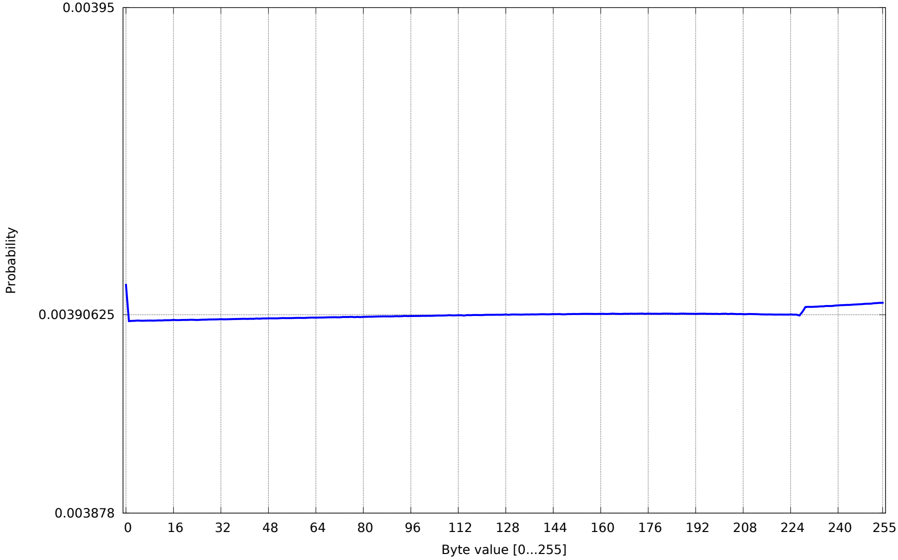
Keystream distribution at position 226



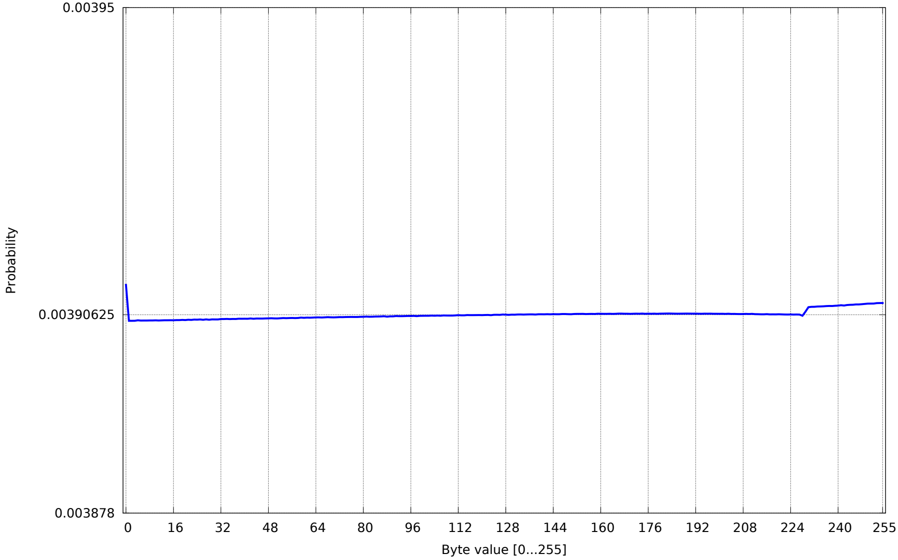
Keystream distribution at position 227



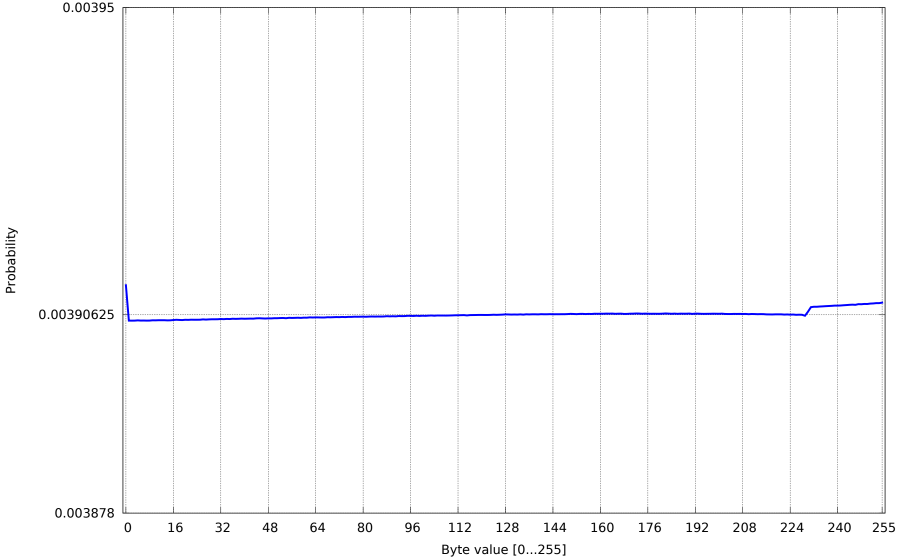
Keystream distribution at position 228



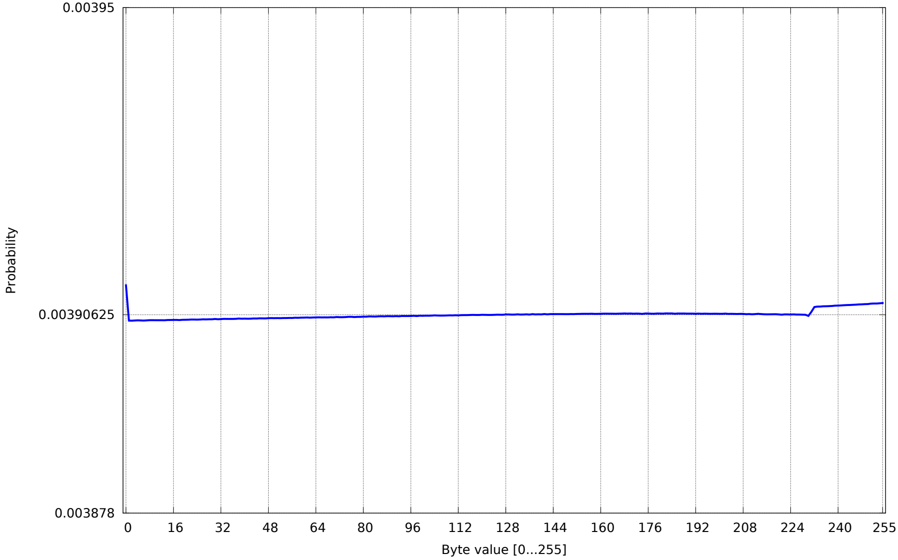
Keystream distribution at position 229



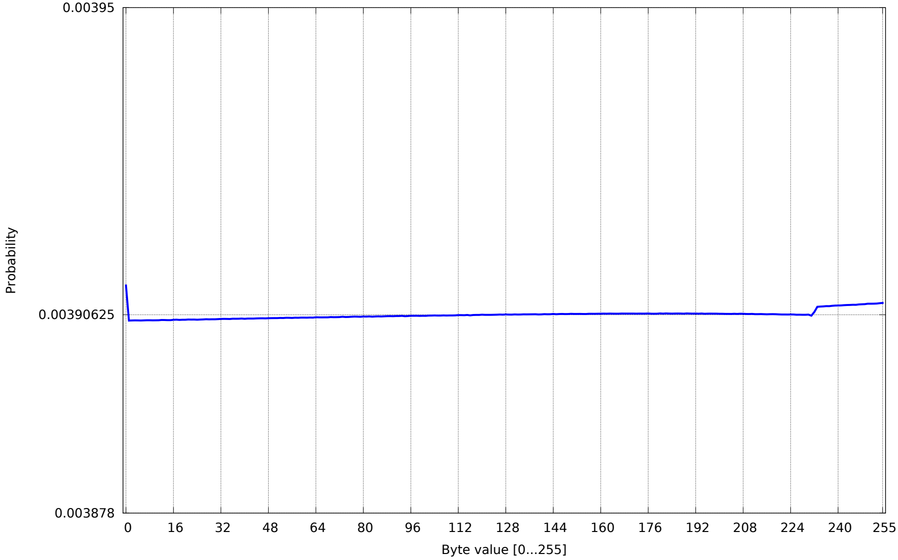
Keystream distribution at position 230



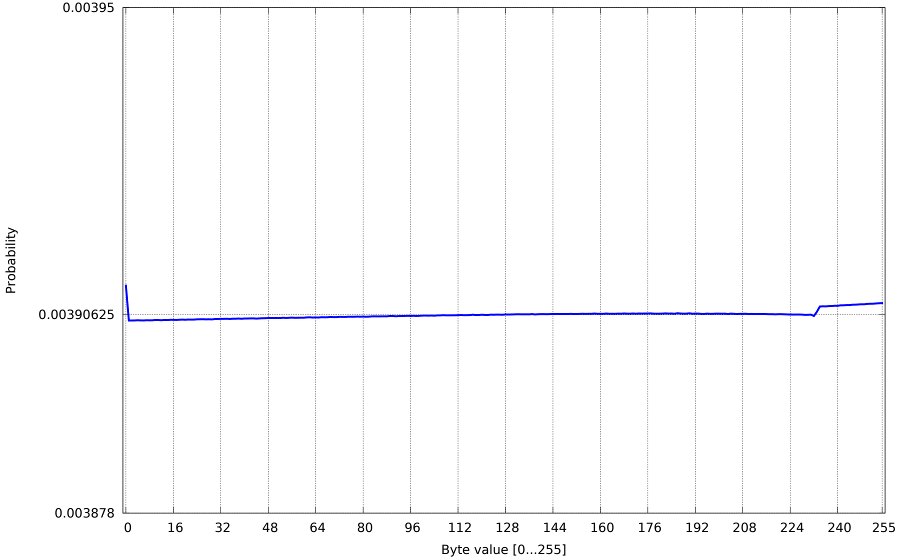
Keystream distribution at position 231



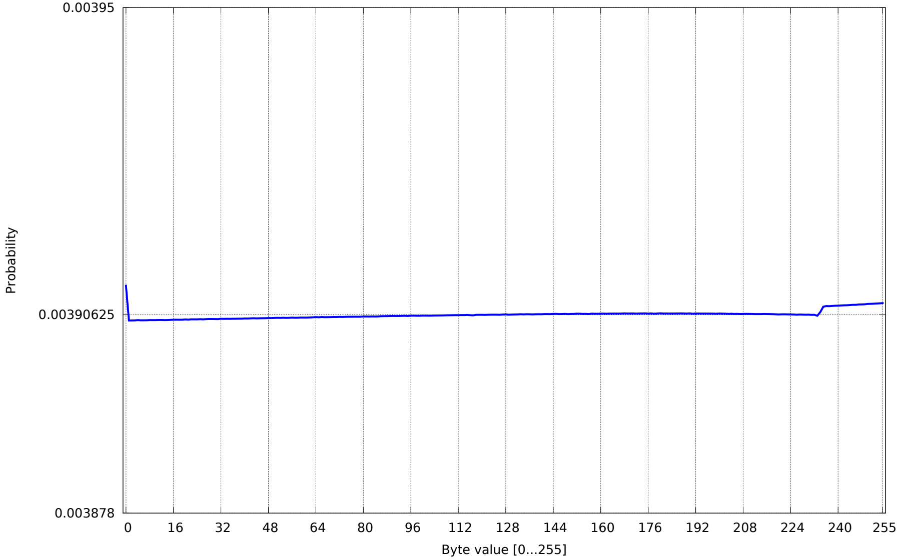
Keystream distribution at position 232



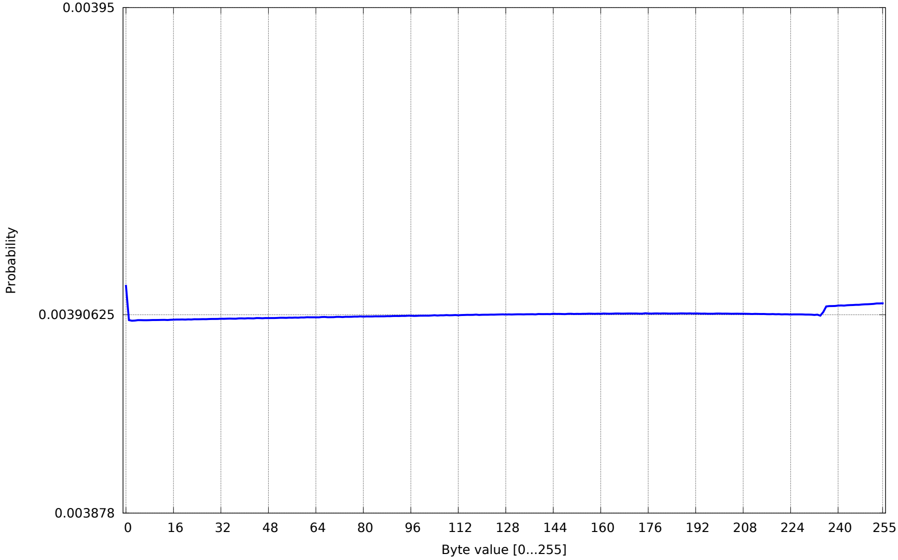
Keystream distribution at position 233



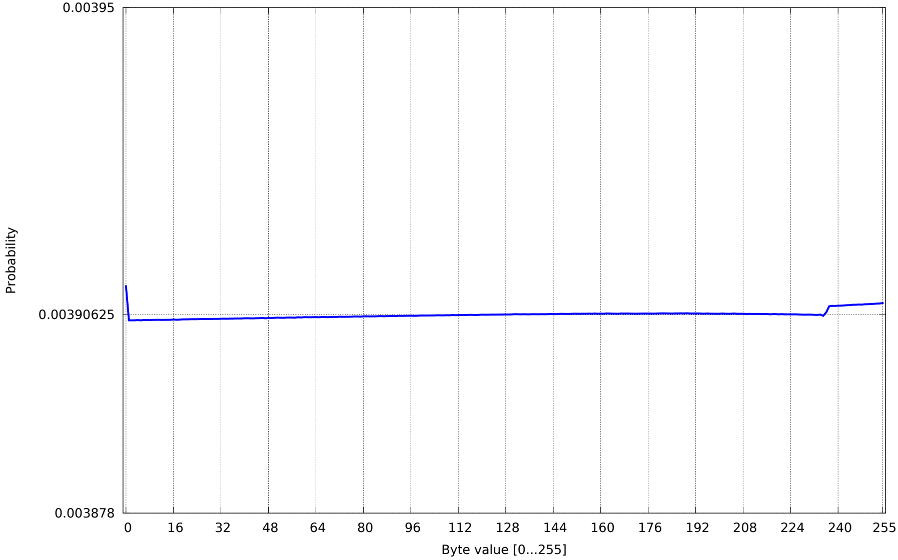
Keystream distribution at position 234



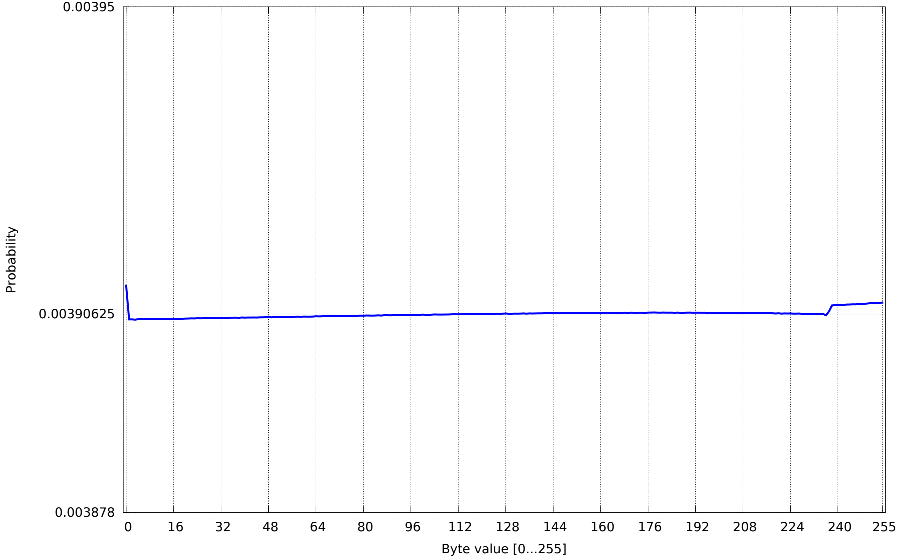
Keystream distribution at position 235



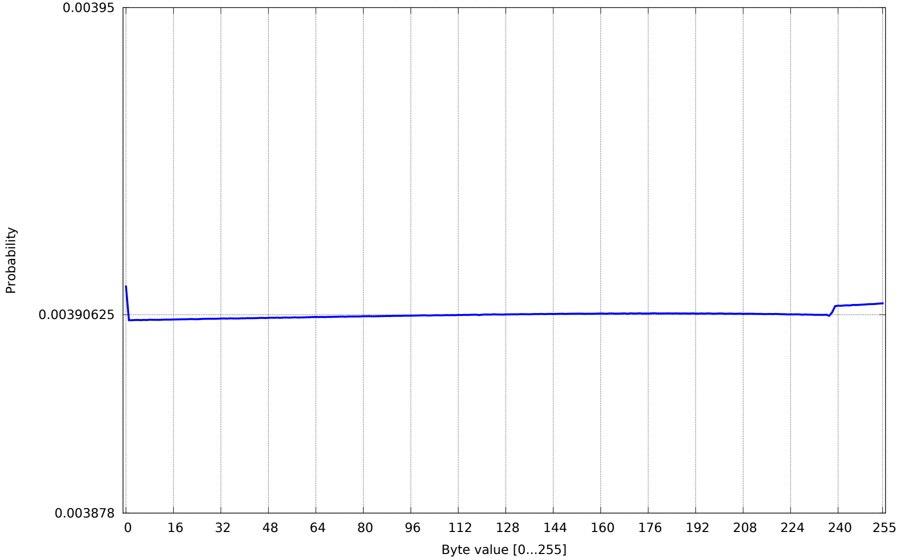
Keystream distribution at position 236



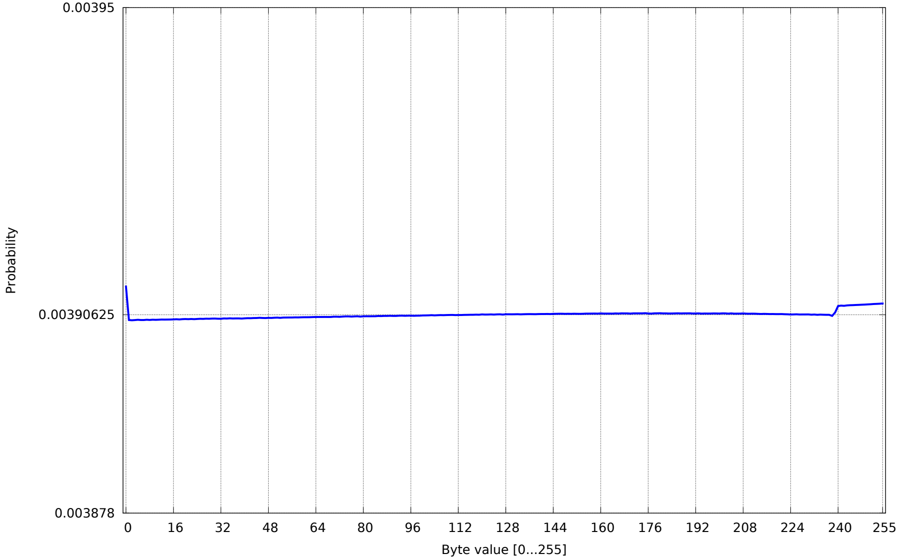
Keystream distribution at position 237



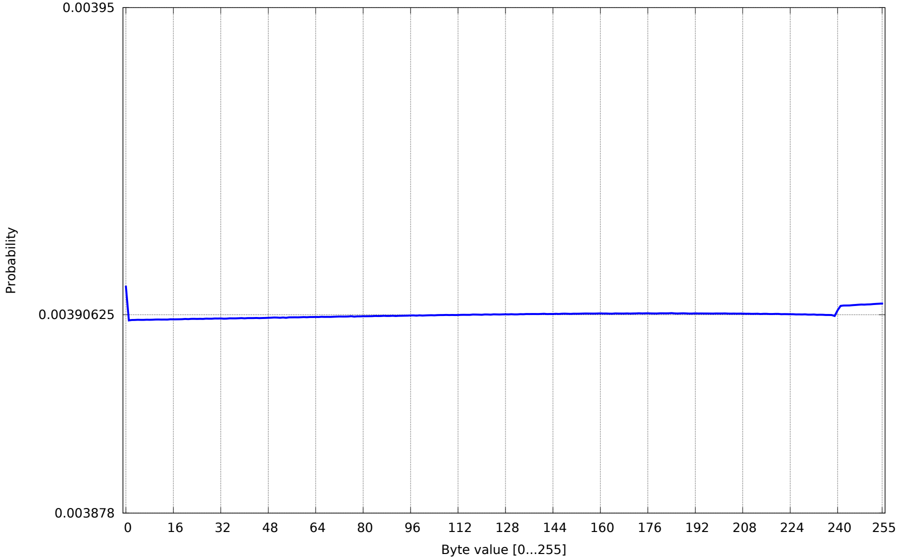
Keystream distribution at position 238



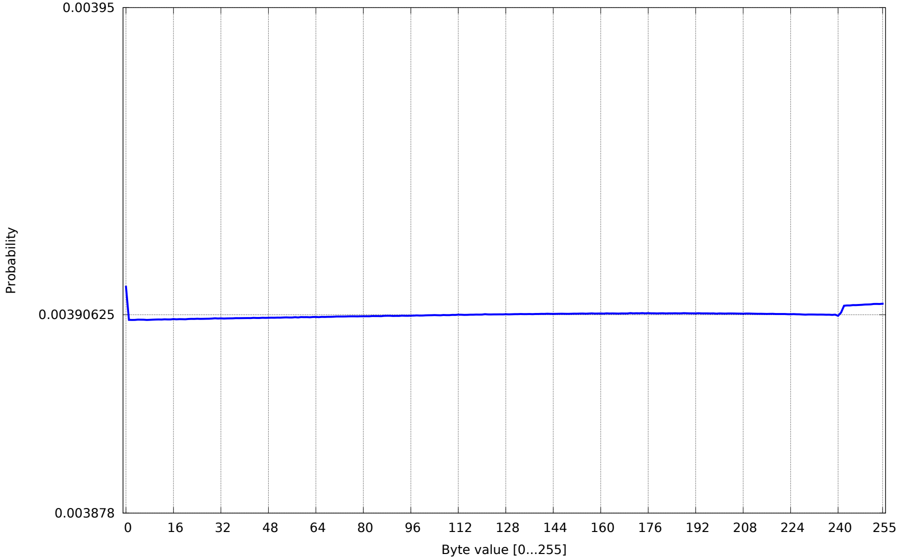
Keystream distribution at position 239



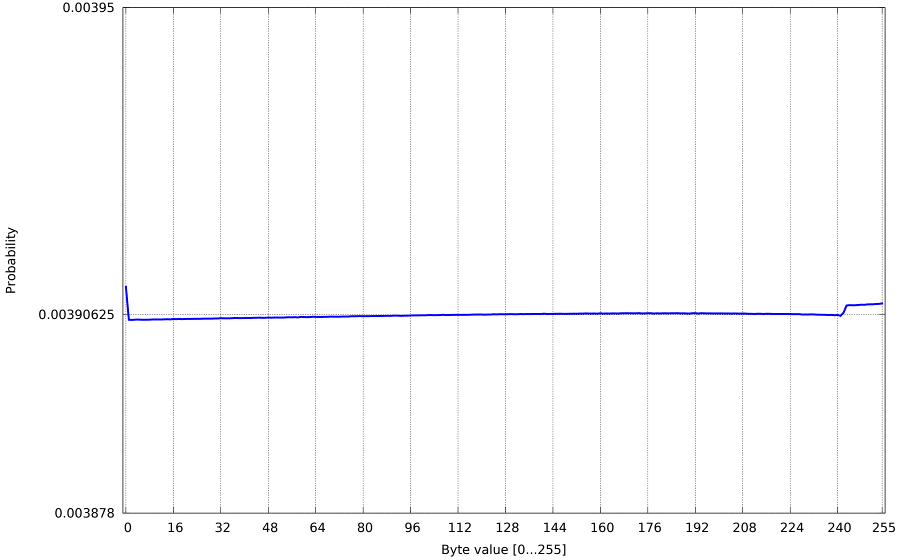
Keystream distribution at position 240



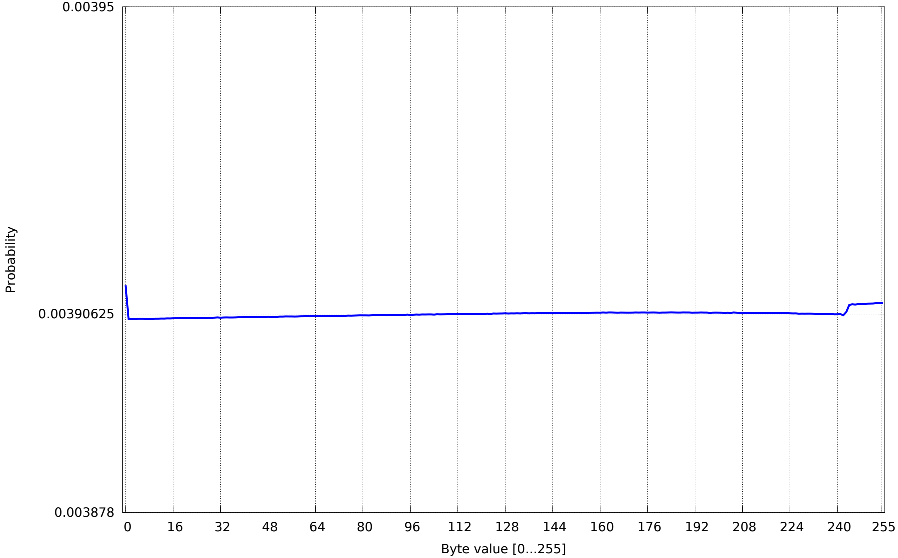
Keystream distribution at position 241



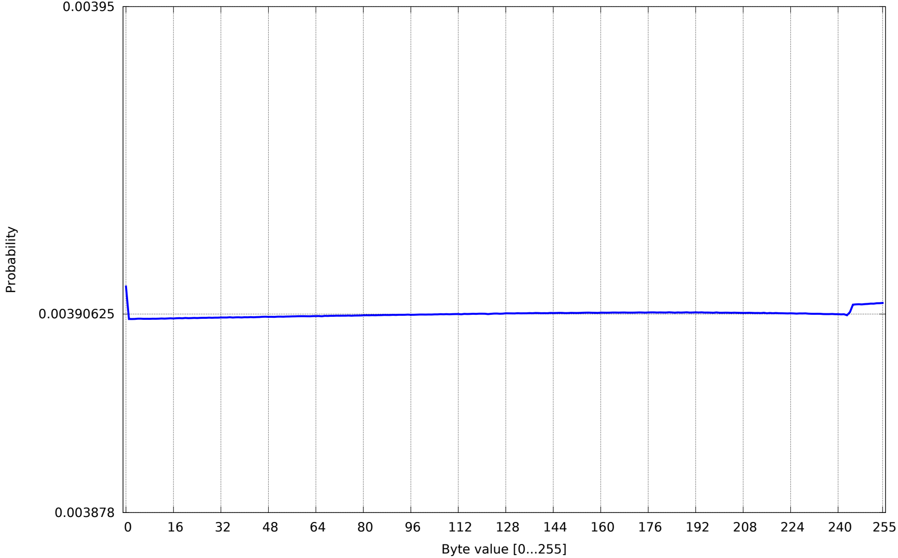
Keystream distribution at position 242



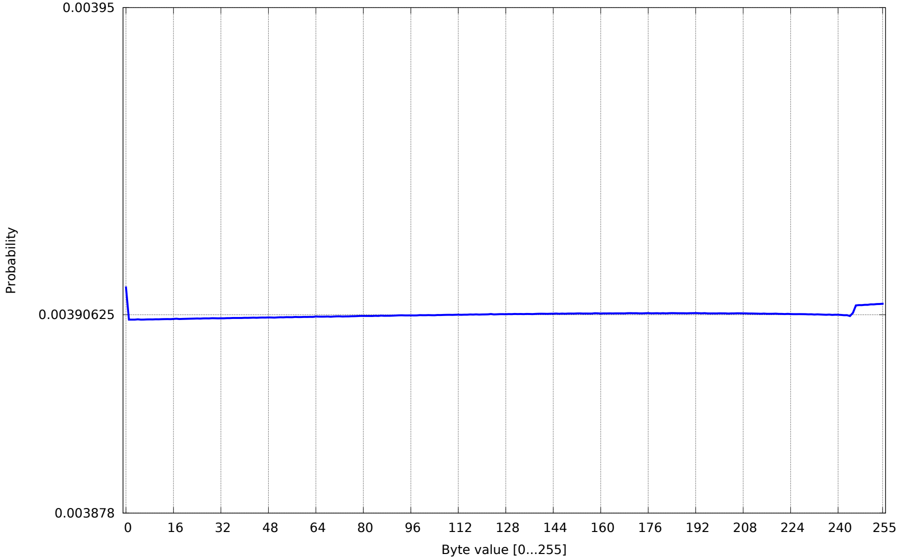
Keystream distribution at position 243



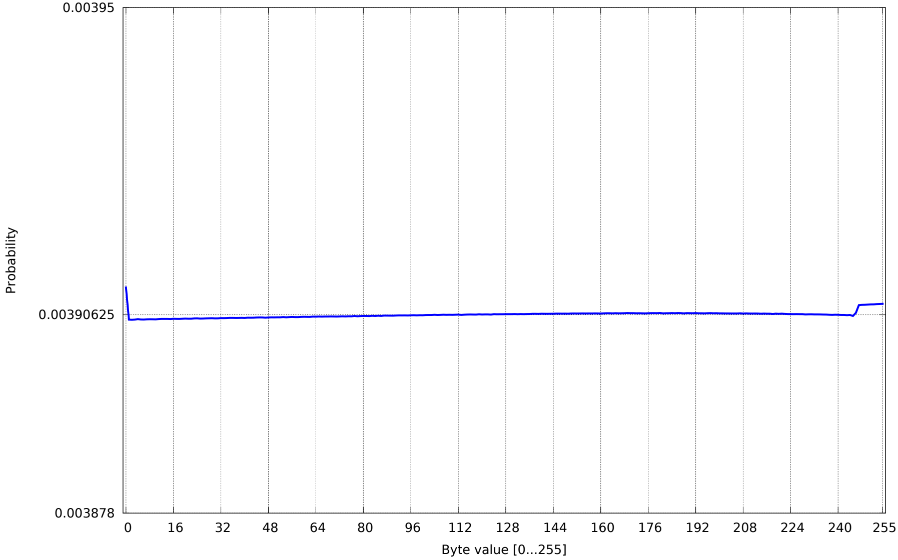
Keystream distribution at position 244



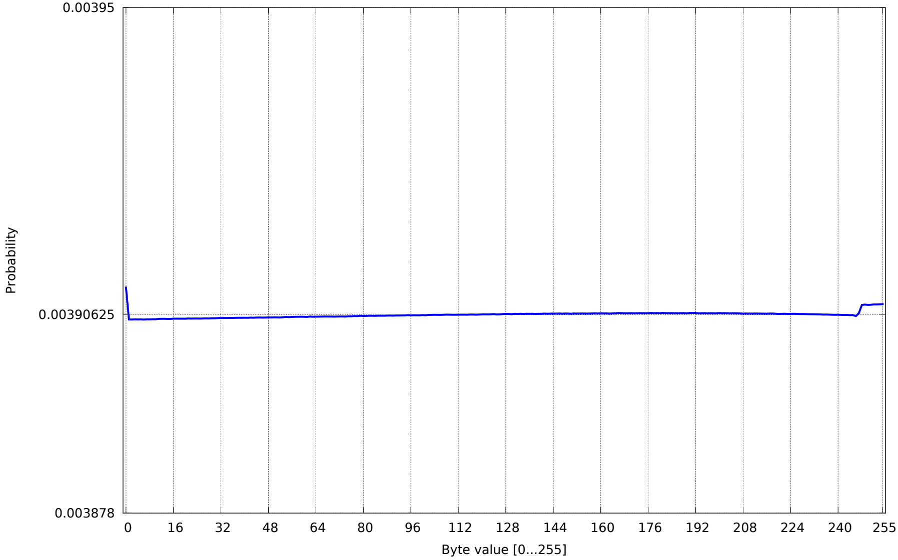
Keystream distribution at position 245



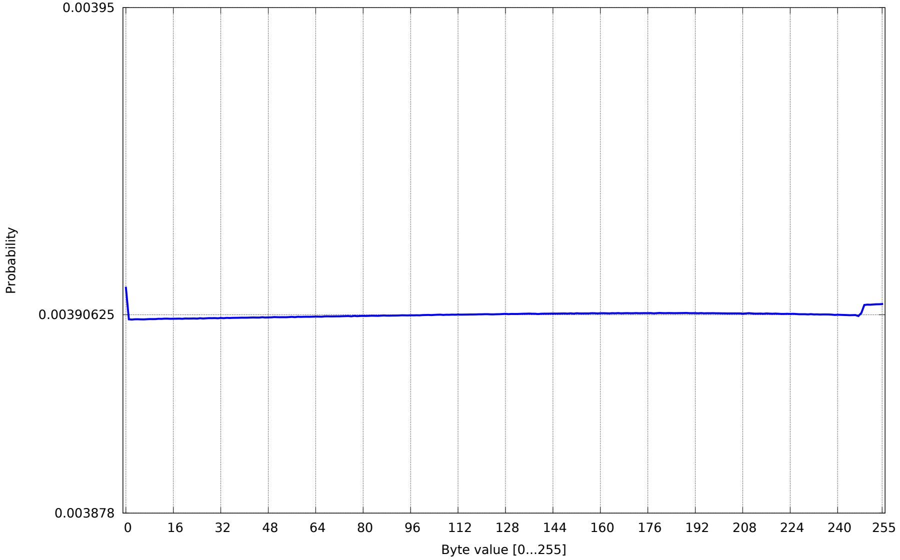
Keystream distribution at position 246



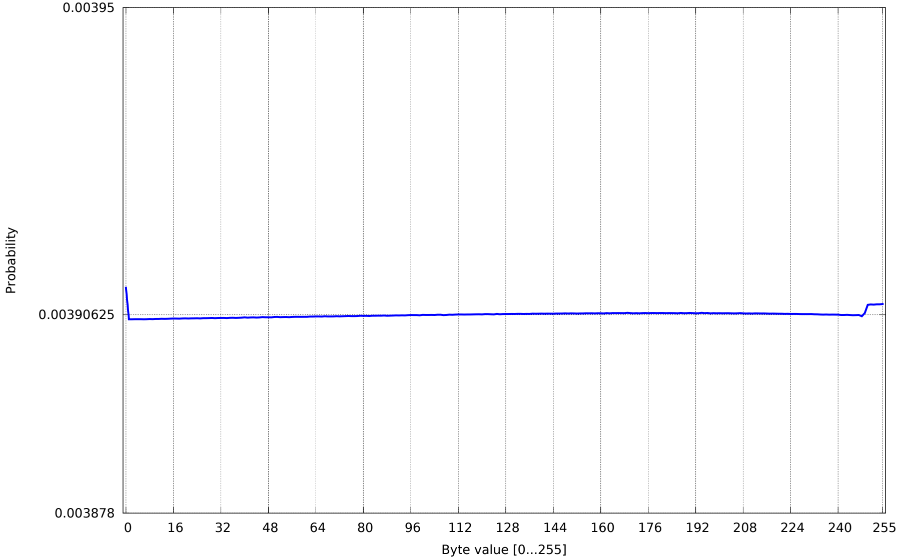
Keystream distribution at position 247



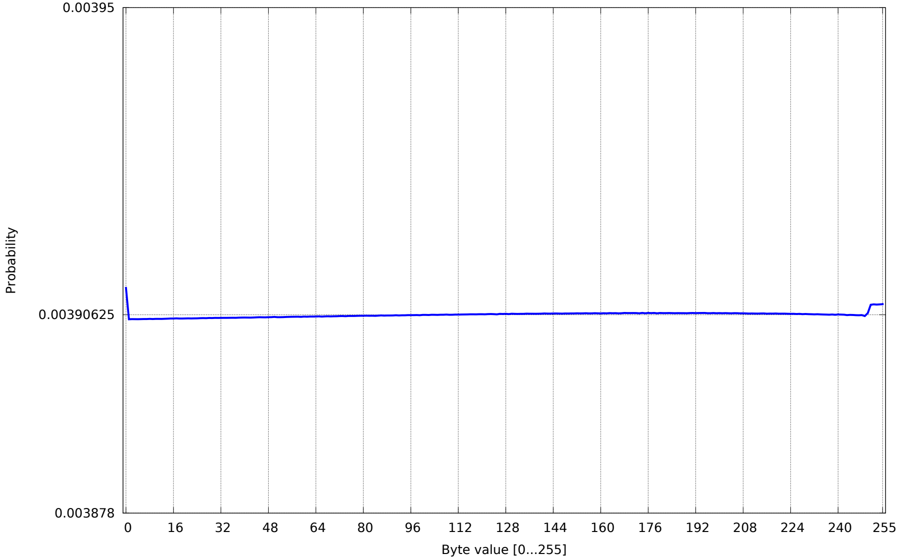
Keystream distribution at position 248



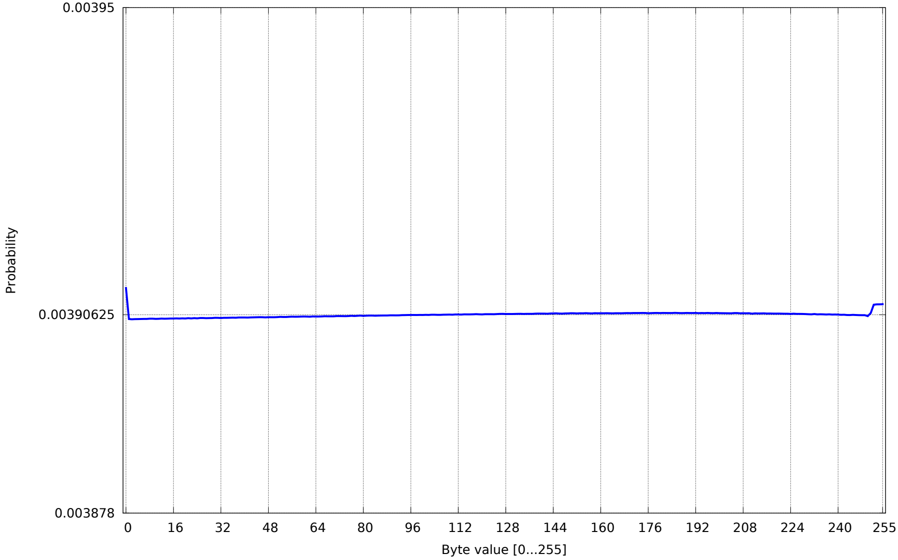
Keystream distribution at position 249



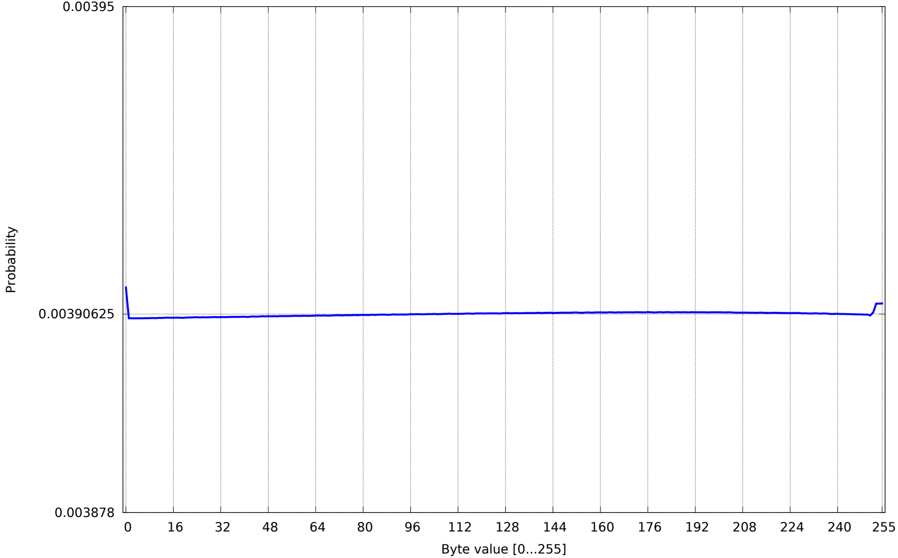
Keystream distribution at position 250



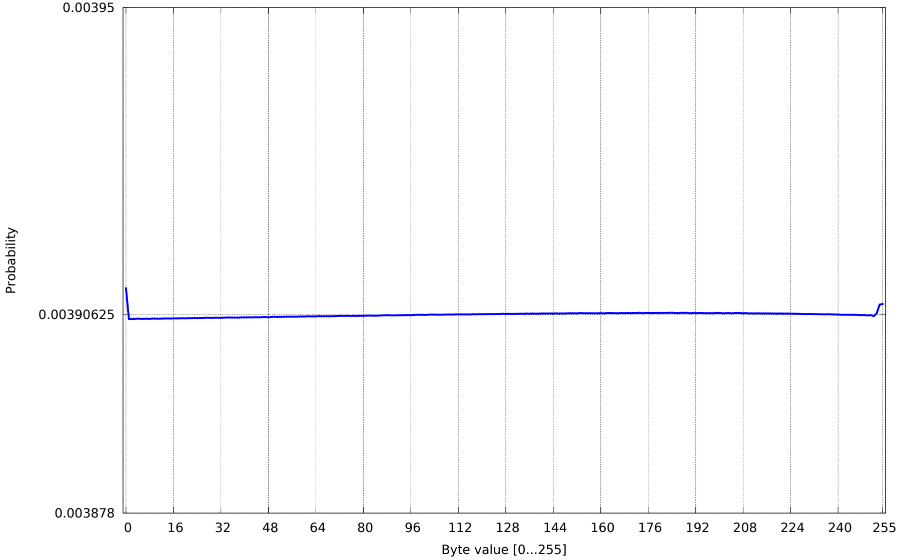
Keystream distribution at position 251



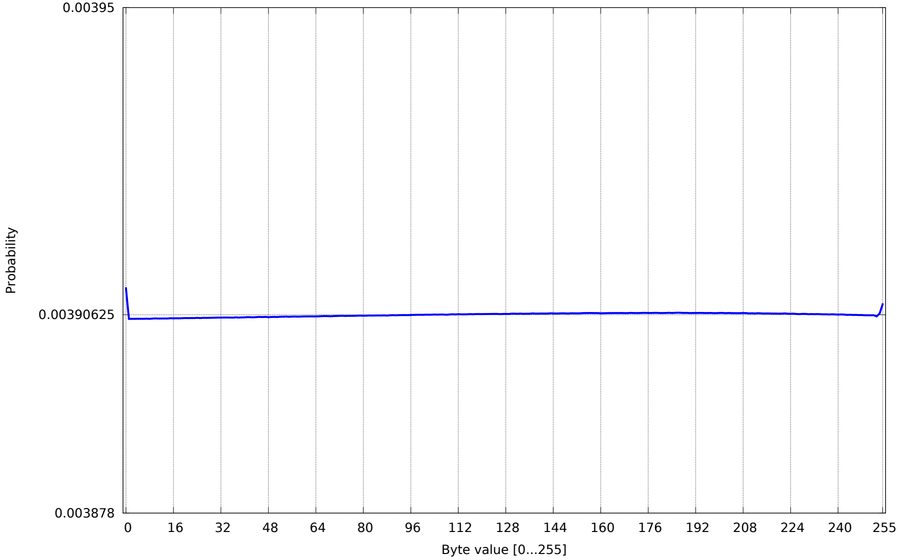
Keystream distribution at position 252



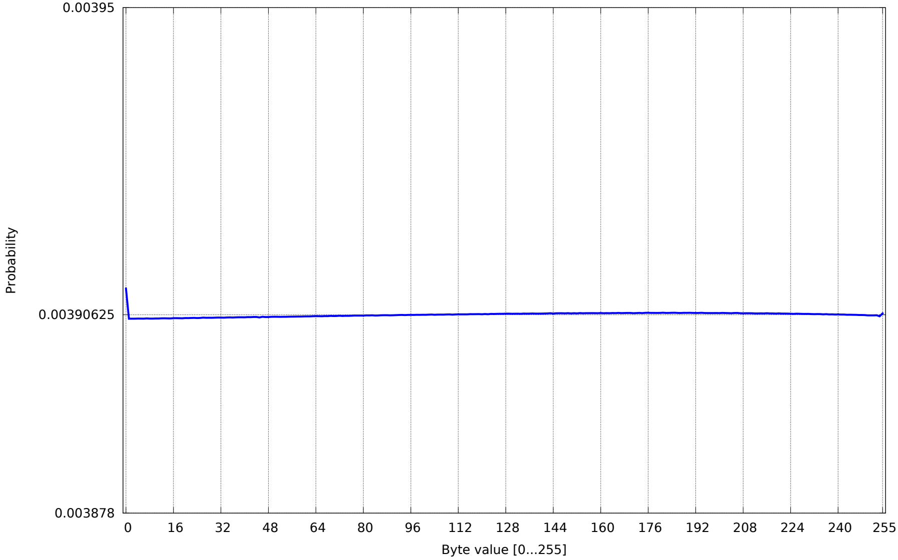
Keystream distribution at position 253



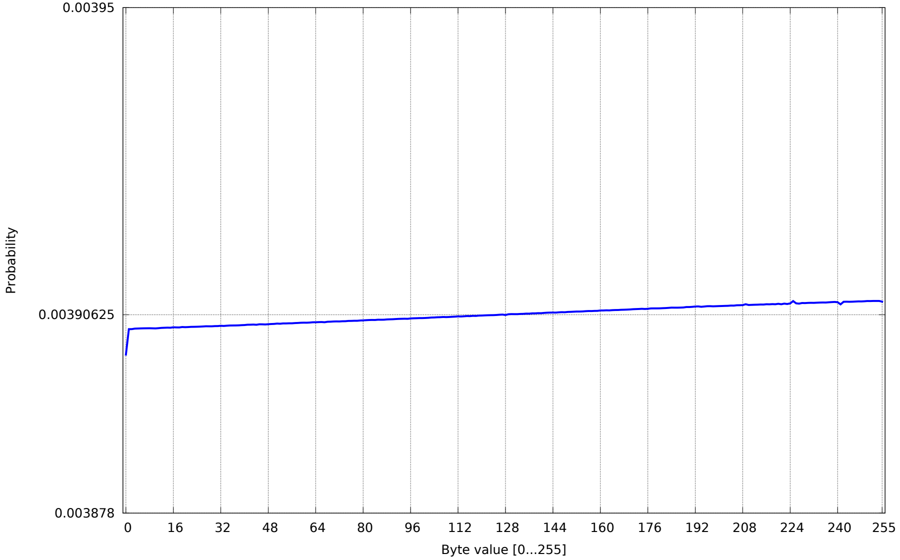
Keystream distribution at position 254



Keystream distribution at position 255



Keystream distribution at position 256


Probability
Byte value [0...255]