

TEXT 1

It is homogeneous text consisting of letter "v" repeated 1500 times.

TEXT 2

Medium diversified text consisting of the phrase "Once You Question Your Own Belief, It's Over

" Repeated 400 times

TEXT 3

Highly diversified text:

But even if I told you why, I doubt very strongly that the knowledge would change anything at all but let's just say that I take the time to explain it to you. What do you think would happen then? My goal is to fulfill the dream even Jiraya sensei was unable to achieve that is to create peace and bring about justice. Oh I see that is noble of you that would be justice. However what about my family? My friends, my village they suffered the same fate as this village at the hands of you hidden leaf ninja. How's it fair to let only you people preach about peace and justice once the land of fire and the hidden leaf had grown too big to protect the national interests. They forced feudal clans to wage war against each other and profited from it otherwise the people of the villages would've starved as it happened our little nation and its villages became the battlefield where the great nations waged through war each time they did our nation was ravaged and laid to waste after many such battles the great nations stabilized but our smaller nation suffered and barely recovered. You and I are both seeking the very same thing we both want to achieve the peace that jiraya sensei envisioned, you and I are the same, we're both motivated by our desire for peace and justice. The justice that I have delivered against the leaf village is no different from what you are trying to do to me. Everyone feels the same pain in losing something dear, you and I both have experience that same pain. You strive for your justice and I strive for mine we're both just ordinary men who have been driven to seek vengeance in the name of justice and if comes call vengeance justice such justice will only breed further vengeance and trigger a vicious cycle of hatred, right now we live in such a cycle. I know the past and can foretell our future it is the same as our history so we believe that Human beings simply cannot understand each other and they never will that the shinobi world is ruled by hatred and hatred alone. So naruto how would u confront this hatred in order to create peace? I want to know what your answer.....

TASK 1.2

Available Asymmetric Key Pairs

The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

Last name	First name	Key type	Key identifier	Created	Internal ID no.
Lab4	Key1	RSA-512		03.11.2023 19:11:42	1699035102
Lab4	Key2	RSA-1024		03.11.2023 19:12:52	1699035172
Lab4	Key3	RSA-2048		03.11.2023 19:13:12	1699035192
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 11:51:34	1152179494

Listed key types:

☒ RSA keys
☐ DSA keys
☐ EC keys

Show public parameters...

Show certificate

Delete...

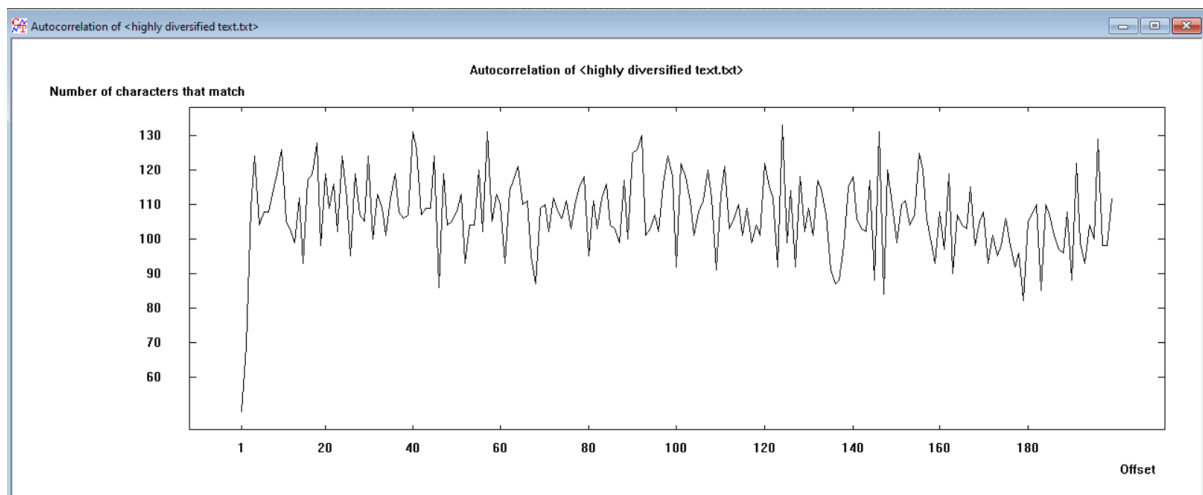
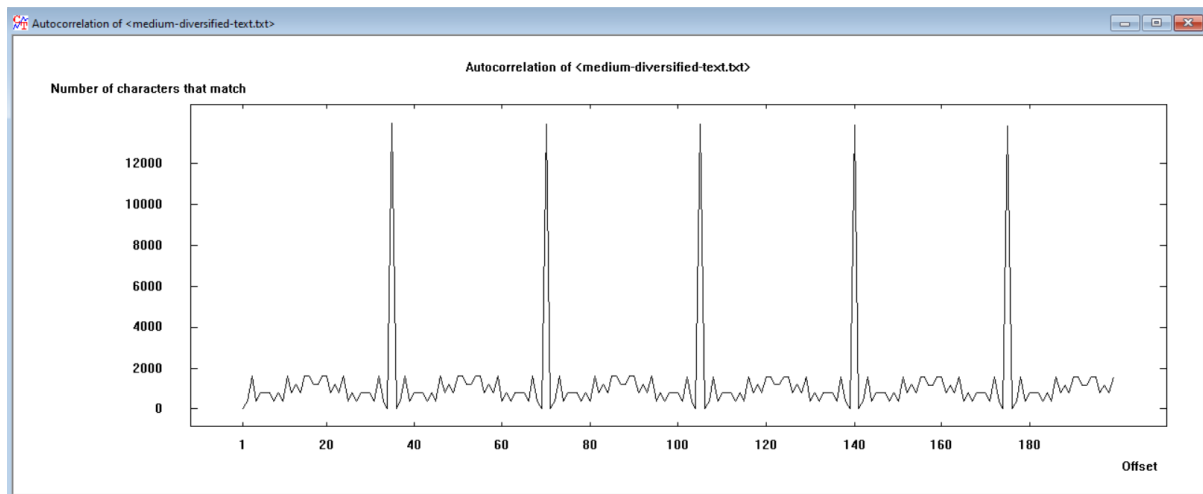
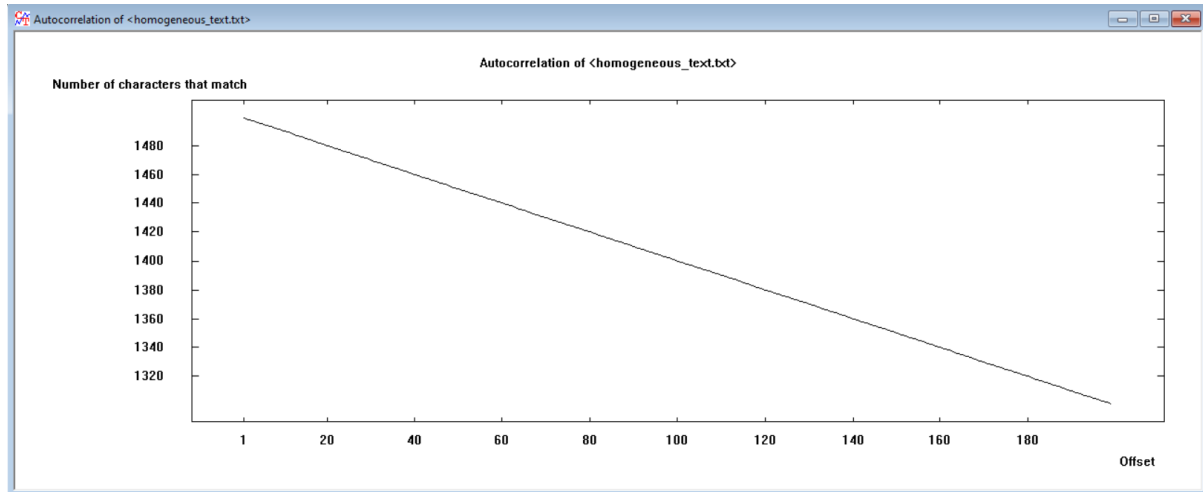
Show all parameters...

Export PSE (PKCS#12)

Close

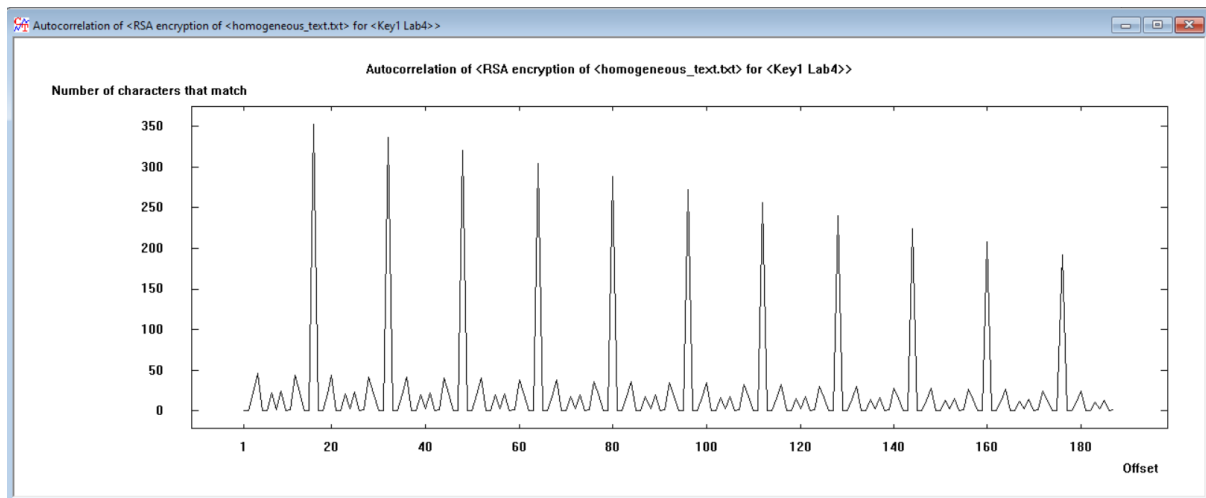
Entropy of plaintext and ciphertext depending on key length				
	Plaintext	Ciphertext		
Key length(bits)	-	512	1024	2048
homogeneous	0	5.98/8	6.78/8	7.41/8
middle-diversified	3.71/4.7	7.93/8	7.96/8	7.98/8
highly diversified	4.17/4.7	7.92/8	7.9/8	7.9/8

Autocorrelation of plaintext:

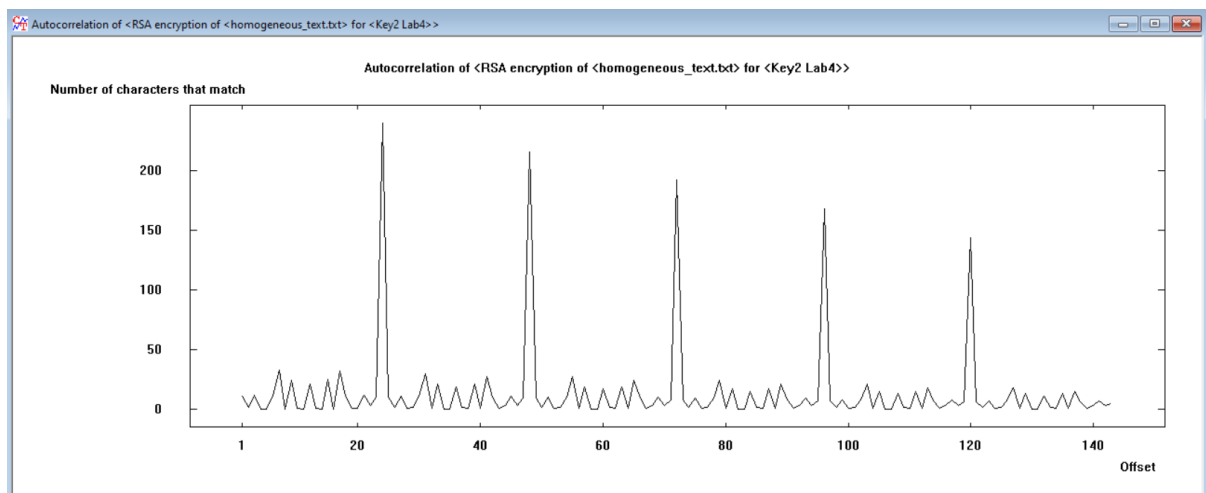


Ciphertext(homogeneous text) autocorrelation

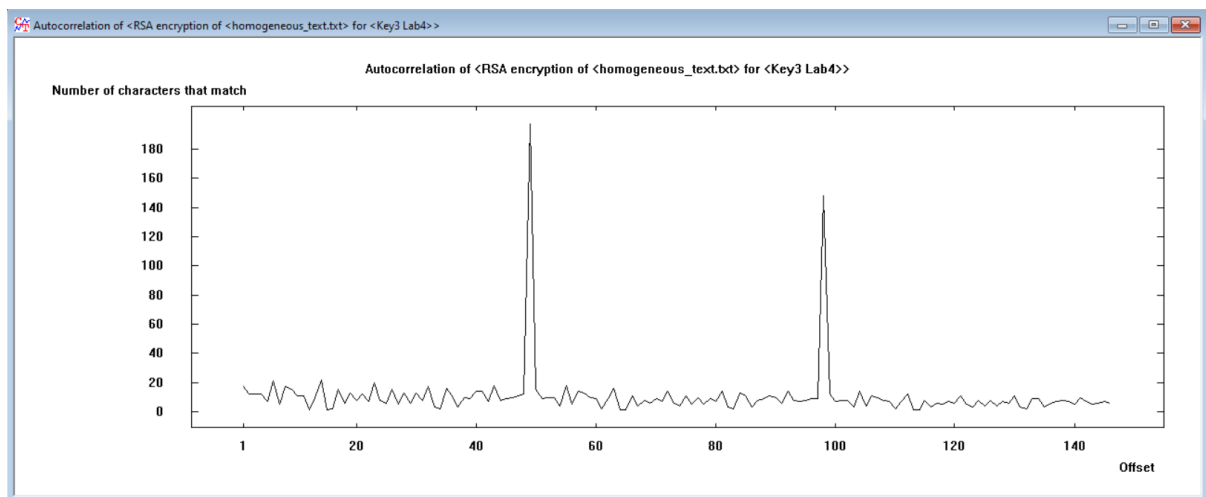
512:



1024:

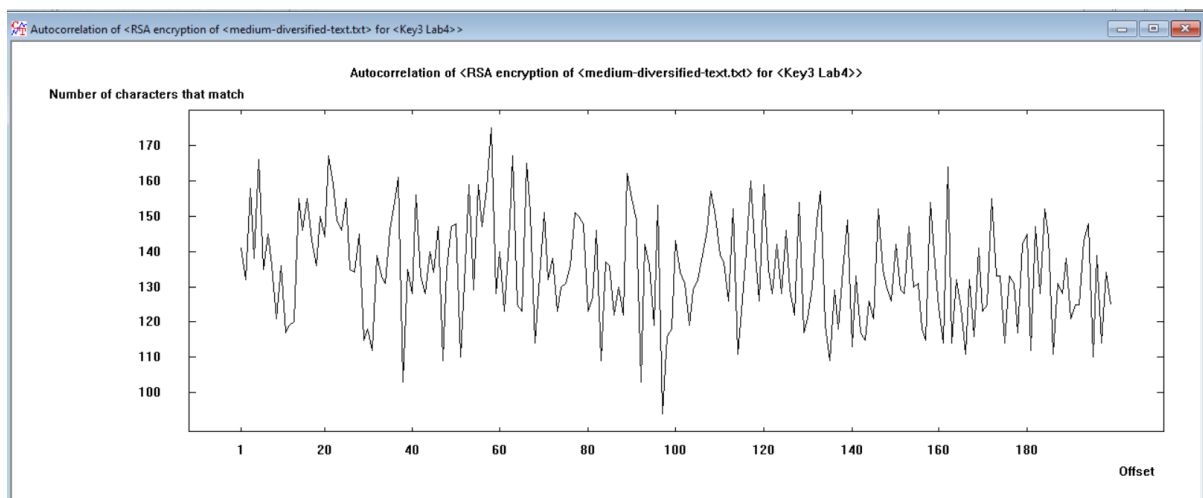
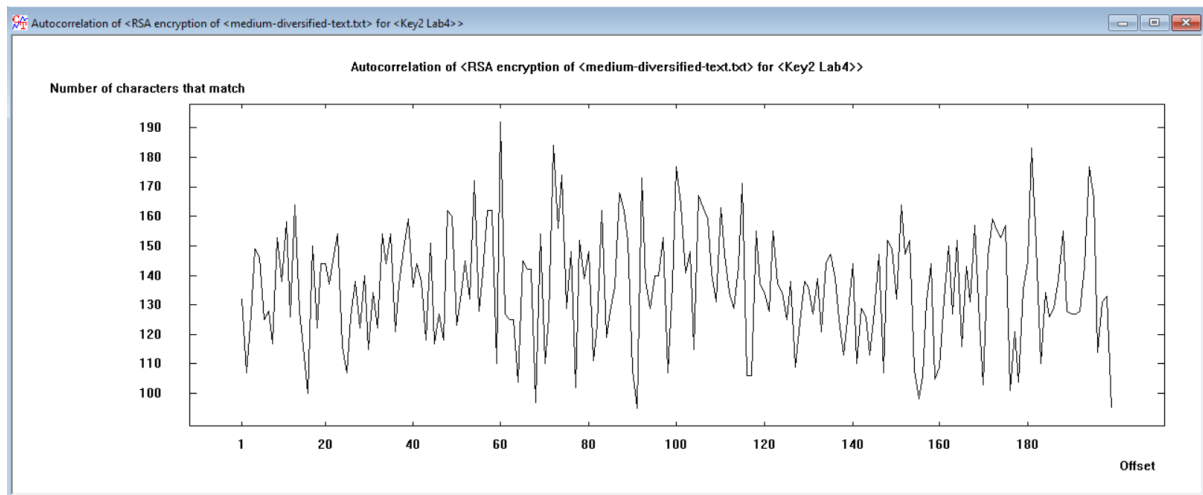
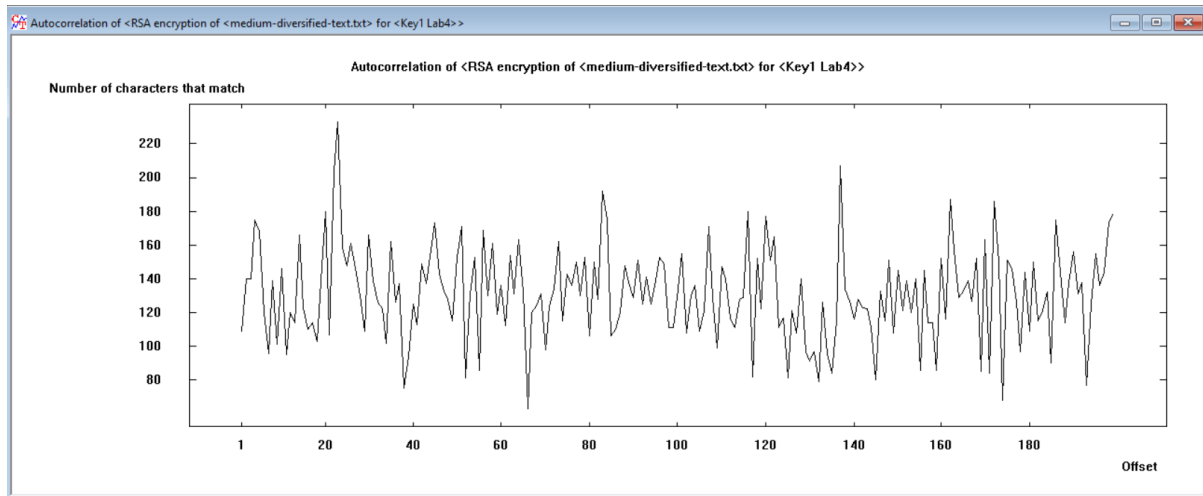


2048:



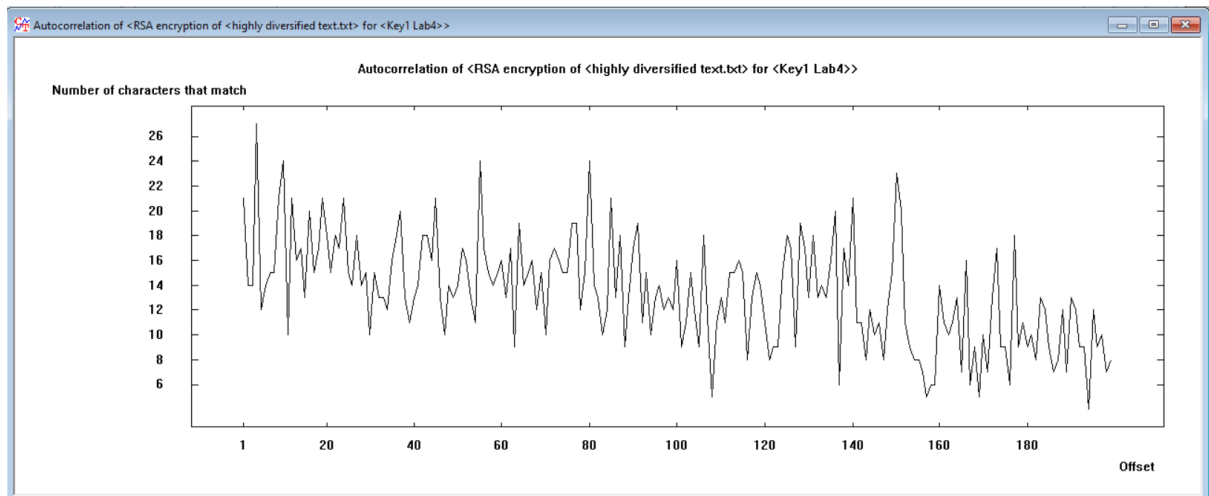
Ciphertext(middle diversified text) autocorrelation:

512:

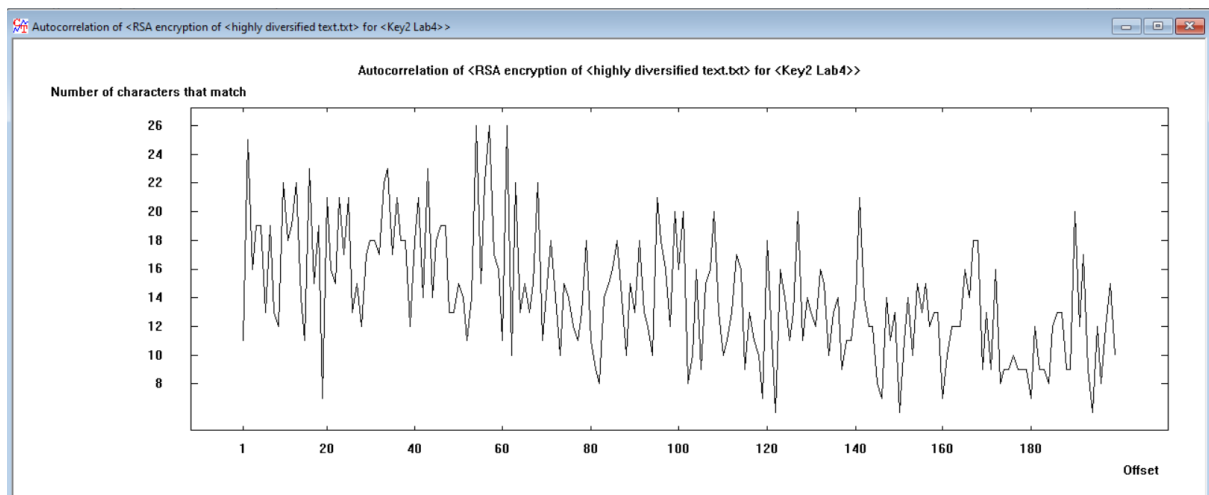


Ciphertext(highly diversified text) autocorrelation:

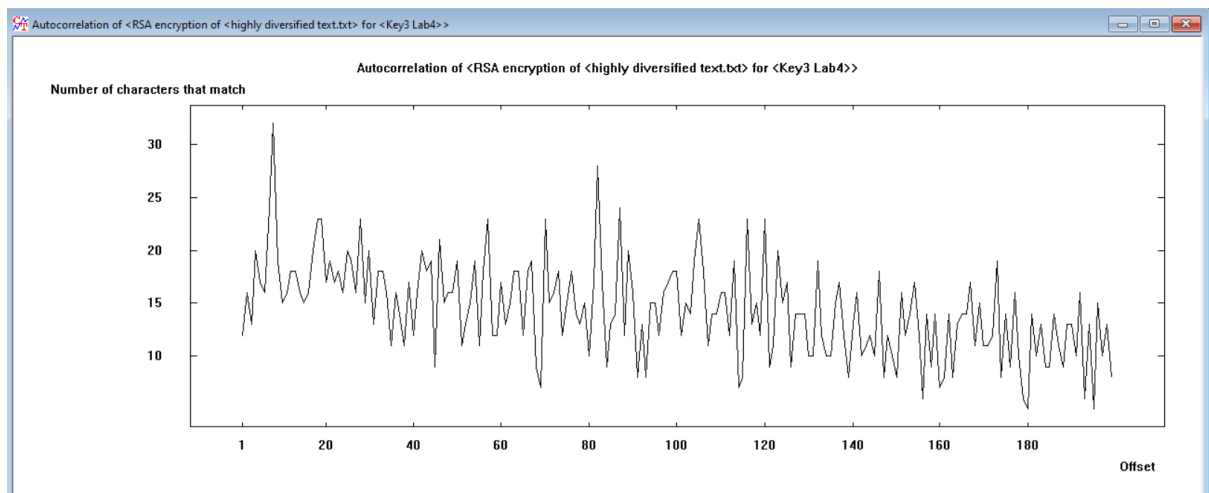
512:



1024:



2048:



Time of encryption and decryption for different files						
	Encryption			Decryption		
key length	512	1024	2048	512	1024	2048
1 mb file	0.28	0.424	0.794	3.726	9.673	33.183
2mb file	0.549	0.872	1.572	7.388	19.343	66.066
5mb file	1.381	2.13	3.922	18.515	48.273	165.567

Time of encryption and decryption using AES for different files						
	Encryption			Decryption		
key length	128	192	256	128	192	256
1 mb file	<0.3	<0.3	<0.3	<0.3	<0.3	<0.3
2mb file	<0.5	<0.5	<0.5	<0.5	<0.6	<0.7
5mb file	<0.6	<0.6	<0.6	<0.6	<0.7	<1

RSA 512:

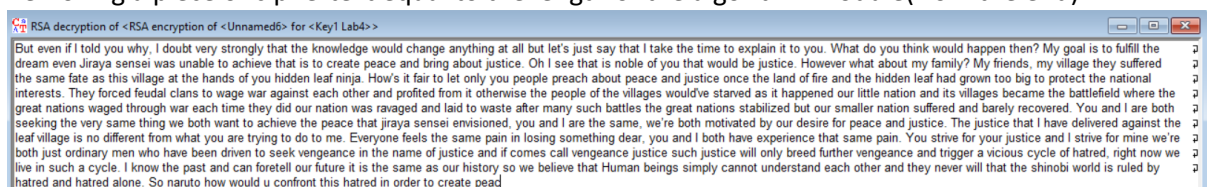
Change the value of one byte(last byte):

```
00000000 42 75 74 20 65 76 65 6E 20 69 66 20 49 20 74 6F 6C 64 20 79 6F 75 20 77 68 79 2C 20 49 20 64 6F 75 62 74 20 76 65 72 79 20 73 74 72
00000002 6F 6E 67 6C 79 20 74 68 61 74 20 74 68 65 20 6B 6E 6F 77 6C 65 64 67 65 20 77 6F 75 6C 64 20 63 68 61 6E 67 65 20 61 6E 79 74 68 69
00000008 6E 67 20 61 74 20 61 6C 6C 6C 62 65 74 20 6C 65 74 27 73 20 6A 75 74 20 73 61 79 20 74 68 61 74 20 49 20 74 61 6B 65 20 74 68 65
00000004 20 74 69 6D 65 20 74 6F 20 65 70 70 6C 61 69 6E 20 69 74 20 74 6F 20 79 6F 75 2E 20 67 68 61 74 20 64 6F 20 79 6F 75 20 74 68 69 6E
00000000 68 20 77 6F 75 6C 64 20 68 61 70 70 65 6E 20 74 68 65 6E 3F 20 40 7D 20 67 6F 61 6C 20 69 73 20 74 6F 20 66 75 6C 66 69 6C 6C 20 74
0000000C 68 65 20 64 72 65 61 6D 20 65 76 65 6E 20 4A 69 72 61 79 61 73 73 65 6E 73 65 69 20 77 61 73 20 75 6E 61 62 6C 65 20 74 6F 20 61 63
00000108 68 69 65 76 65 20 74 68 61 74 20 69 73 20 74 6F 20 63 72 65 61 74 65 20 70 65 61 63 65 20 61 6E 64 20 62 72 69 6E 67 20 61 62 6F 75
00000134 74 20 6A 75 73 74 69 63 65 2E 20 4F 68 20 49 20 73 65 65 20 74 68 61 74 20 69 73 20 6E 6F 62 6C 65 20 6F 66 20 79 6F 75 20 74 68 61
00000160 74 20 77 6F 75 6C 64 20 62 65 20 6A 75 73 74 69 63 65 2E 20 48 6F 77 65 76 65 72 20 77 68 61 74 20 61 62 6F 75 74 20 6D 79 20 66 61
0000018C 6D 69 6C 79 3F 20 4D 79 20 66 72 69 65 6E 64 73 2C 20 6D 79 20 76 69 6C 6C 61 67 65 20 74 68 65 79 20 73 75 66 66 65 72 65 64 20 74
000001B8 68 65 20 73 61 6D 65 20 66 61 74 65 20 61 73 20 74 68 69 73 20 76 69 6C 6C 61 67 65 20 61 74 20 74 68 65 20 68 61 6E 64 73 20 6F 66
000001E4 20 79 6F 75 20 68 69 64 64 65 6E 20 6C 65 61 66 20 6E 69 6E 6A 61 2E 20 48 6F 77 73 20 69 74 20 66 61 69 72 20 74 6F 20 6C 65 74
00000210 20 6F 6E 6C 79 20 79 6F 75 20 70 65 6F 70 6C 65 20 72 65 61 63 68 20 61 62 6F 74 20 70 65 61 63 65 20 61 6E 64 20 6A 75 73 74
0000023C 69 63 65 20 6F 68 63 65 20 74 68 65 20 6C 61 6E 64 20 6F 66 20 66 69 72 65 20 61 6E 64 20 74 68 65 20 68 69 64 64 65 6E 20 6C 65 61
00000268 66 20 68 61 64 20 67 72 6F 77 6E 20 74 6F 6F 20 62 69 67 20 74 6F 20 70 72 6F 74 65 63 74 20 74 68 65 20 6E 61 74 69 6F 6E 61 6C 20
00000294 69 6E 74 65 72 65 73 74 73 2E 20 54 68 65 79 20 66 6F 72 63 65 64 20 66 65 75 64 61 6C 20 63 6C 61 6E 73 20 74 6F 20 77 61 67 65 20
00000320 77 61 72 20 61 67 61 69 6E 73 74 20 65 61 63 68 20 6F 74 68 65 72 20 61 6E 64 20 70 72 6F 66 69 74 65 64 20 66 72 6F 6D 20 69 74 20
0000032C 6F 74 68 65 72 77 69 73 65 20 74 68 65 20 70 65 6F 70 6C 65 20 6E 66 20 74 68 65 20 76 69 6C 6C 61 67 65 73 20 77 6F 75 6C 64 27 76
00000318 65 20 73 74 61 72 76 65 64 20 61 73 20 69 74 20 68 61 70 70 65 6E 65 64 20 76 75 72 20 6C 69 74 74 6C 65 20 6E 61 74 69 6F 6E 20 61
00000344 6E 64 20 69 74 73 20 76 69 6C 6C 61 67 65 73 20 62 65 63 61 6D 65 20 74 68 65 20 62 61 74 74 6C 65 66 69 65 6C 64 20 77 68 65 72 65
00000370 20 74 68 65 20 67 72 65 61 74 20 6E 61 74 69 6F 6E 73 20 77 61 67 65 64 20 74 68 72 6F 75 67 68 20 77 61 72 20 65 61 63 68 20 74 69
0000039C 6D 65 20 74 68 65 79 20 64 69 64 20 6F 75 72 20 6E 61 74 69 6F 6E 20 77 61 73 20 72 61 76 61 67 65 64 20 61 6E 64 20 6C 61 69 64 20
000003C8 74 6F 20 77 61 73 74 65 20 61 66 74 65 72 20 6D 61 6E 79 20 73 75 63 68 20 62 61 74 74 6C 65 73 20 74 68 65 20 67 72 65 61 74 20 6E
000003F4 61 74 69 6F 6E 73 20 74 61 62 69 6C 69 74 65 64 20 62 75 74 20 6F 75 72 20 73 6D 61 6C 6C 65 72 20 6E 61 74 69 6F 6E 20 73 75 65
00000420 66 65 72 65 64 20 61 6E 64 20 62 61 72 65 6C 79 20 72 65 63 6F 76 65 72 65 64 2E 20 59 6F 75 20 61 6E 64 20 49 20 61 72 65 20 62 6F
0000044C 74 68 20 73 65 65 68 69 6E 67 20 74 68 65 20 76 65 72 79 20 73 61 6D 65 20 74 68 69 6E 67 20 77 65 20 62 6F 74 68 20 77 61 6E 74 20
00000478 74 6F 20 61 63 68 69 65 76 65 61 74 68 65 20 70 65 61 63 65 20 74 68 61 74 20 6A 69 72 61 69 73 73 65 6E 73 65 69 20 65 6E 76 69
000004A4 73 69 6F 6E 65 64 2C 20 79 6F 75 20 61 6E 64 20 49 20 61 72 65 20 74 68 65 20 70 61 6D 65 2C 20 77 65 92 72 65 20 62 6F 74 68 20 6D
000004D0 6F 74 69 76 61 74 65 64 20 62 79 20 6F 75 72 20 64 65 73 69 72 65 20 68 6F 72 20 70 65 61 63 65 20 61 6E 64 20 6A 75 73 74 69 63 65
000004FC 2E 20 54 68 65 20 6A 75 73 74 69 63 65 20 74 68 61 74 20 49 20 68 61 76 65 20 64 65 6C 69 76 65 72 65 64 20 61 67 61 69 6E 73 74 20
00000528 74 68 65 20 6C 65 61 66 20 76 69 6C 6C 61 67 65 20 69 73 20 6E 6F 20 64 69 66 66 65 72 65 6E 74 20 66 72 6F 6D 20 77 68 61 74 20 79
00000554 6F 75 20 61 72 65 20 74 74 6F 20 64 6F 20 74 6F 20 6D 65 2E 20 45 76 65 72 6F 6F 6E 65 20 66 65 6C 73 20 74 68
00000580 6E 65 20 73 61 6D 65 20 70 61 69 6E 20 69 6E 20 6C 6F 73 69 6E 67 20 73 6F 6E 67 20 73 6F 6E 67 20 64 65 61 72 2C 20 79 6F 75 20 61 6E
000005AC 64 20 49 20 62 6F 74 68 20 68 61 76 65 20 65 70 70 65 72 69 65 6E 63 65 20 74 68 61 74 20 73 61 6D 65 20 70 61 69 6E 2E 20 59 6F 75
000005D8 20 73 74 72 69 76 65 20 66 6F 72 20 79 6F 75 75 73 74 69 63 65 20 61 6E 64 20 49 20 73 74 72 69 69 76 65 20 66 6F 72 20 6D 69
00000604 6E 65 20 77 65 92 72 65 20 62 6F 74 68 20 6A 75 73 74 20 6F 72 64 69 6E 61 72 79 20 6D 65 6E 20 77 68 6F 20 68 61 76 65 20 62 65 65
00000630 6E 20 64 72 69 76 65 6E 20 74 6F 20 73 65 65 68 20 76 65 6E 67 65 61 6E 63 65 20 69 6E 20 74 68 65 20 6E 61 6D 65 20 6F 66 20 6A 75
0000065C 73 74 69 63 65 20 61 6E 64 20 69 66 20 63 6F 6D 65 73 20 63 61 6C 6C 20 76 65 6E 67 65 61 6E 63 65 20 6A 75 73 74 69 63 65 20 73 75
00000688 63 68 20 6A 75 73 74 69 63 65 20 77 69 6C 6C 20 6F 6E 6C 69 70 62 72 65 65 64 20 66 75 72 74 68 65 72 20 76 65 6E 67 65 61 6E 63 65
000006B4 20 61 6E 64 20 74 72 69 67 67 65 72 20 61 20 76 69 63 69 6F 75 73 20 63 79 63 6C 65 20 6F 6E 20 68 61 74 72 65 64 2C 20 72 69 67 68
000006E0 74 20 6E 6F 77 20 77 65 20 6C 69 76 65 20 69 6E 20 73 75 63 68 20 61 20 63 79 63 6C 65 2E 20 49 20 68 6E 6F 77 20 74 68 65 20 70 61
0000070C 73 74 20 61 6E 64 20 63 61 6E 20 66 6F 72 65 74 65 6C 6C 20 6F 75 72 20 66 75 74 75 72 65 20 69 74 20 69 73 20 74 68 65 20 73 61 6D
00000738 65 20 61 73 20 76 75 72 20 68 69 73 74 6F 72 79 20 73 6F 20 77 65 20 62 65 6C 69 6F 66 20 74 68 61 74 20 48 75 6D 61 6E 20 62 65
00000764 69 6E 67 73 20 73 69 6D 70 6C 79 20 63 61 6E 6E 6F 74 20 75 6E 64 65 72 73 74 61 6E 64 20 65 61 63 68 20 6F 74 68 65 72 20 61 6E 64
00000790 20 74 68 65 79 20 6E 65 76 65 72 20 77 69 6C 6C 20 74 68 61 74 20 74 65 64 20 68 61 74 72 65 64 20 61 6C 6F 6E 65 2E 20 53 6F 20 6E 61 72 75 74 6F 20 68
000007BC 75 6C 65 64 20 62 79 20 68 61 74 72 65 64 20 61 6E 64 20 68 61 74 72 65 64 20 61 6C 6F 6E 65 2E 20 53 6F 20 6E 61 72 75 74 6F 20 68
000007E8 6F 77 20 77 6F 75 6C 64 20 75 20 63 6F 6E 66 72 6F 6E 74 20 74 68 69 73 20 68 61 74 72 65 64 20 69 6E 20 6F 72 64 65 72 20 74 6F 20
00000814 63 72 65 61 74 65 20 70 65 61 63 00 4E AA 2E A8 6C DD BB 4E 55 E1 FA 9E 68 32 27 6C 65 4F 6D E4 8F BF 80 6F 53 EE 63 D1 3C DD 2A D4
00000840 0A 9C 55 1D 83 78 2F D0 94 E7 29 75 7A 0B A3 50 BE 4A BB A4 87 F8 F7 2B 3B 41 25 4D 7F 16
```

But even if I told you why, I doubt very strongly that the knowledge would change anything at all but let's just say that I take the time to explain it to you. What do you think would happen then? My goal is to fulfill the dream even Jiraya sensei was unable to achieve that is to create peace and bring about justice. Oh I see that is noble of you that would be justice. However what about my family? My friends, my village they suffered the same fate as this village at the hands of you hidden leaf ninja. How's it fair to let only you people preach about peace and justice once the land of fire and the hidden leaf had grown too big to protect the national interests. They forced feudal clans to wage war against each other and profited from it otherwise the people of the villages would've starved as it happened our little nation and its villages became the battlefield where the great nations waged through war each time they did our nation was ravaged and laid to waste after many such battles the great nations stabilized but our smaller nation suffered and barely recovered. You and I are both seeking the very same thing we both want to achieve the peace that jiraya sensei envisioned, you and I are the same, we're both motivated by our desire for peace and justice. The justice that I have delivered against the leaf village is no different from what you are trying to do to me. Everyone feels the same pain in losing something dear, you and I both have experience that same pain. You strive for your justice and I strive for mine we're both just ordinary men who have been driven to seek vengeance in the name of justice and if comes call vengeance justice such justice will only breed further vengeance and trigger a vicious cycle of hatred, right now we live in such a cycle. I know the past and can foretell our future it is the same as our history so we believe that Hsuan beings simply cannot understand each other and they never will that the shinobi world is ruled by hatred and hatred alone. So naruto how would u confront this hatred in order to create peace? 1. WY...K? 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 82

Removing several bytes:

Removing a piece of ciphertext equal to the length of the algorithm module(from the end):



[illegible][illegible]

goal is to fulfill the dream even Jiraya sensei was unable to
village at the hands of you hidden leaf ninja. How's it fair to let
and profited from it otherwise the people of the villages would've
battles the great nations stabilized but our smaller nation
aspire for peace and justice. The justice that I have delivered
justice and I strive for mine we're both just ordinary men who
such a cycle. I know the past and can foretell our future it is the

TASK 1.7

The key length significantly influences the entropy of encrypted text primarily when dealing with homogeneous text. It's evident that as the key length increases, the entropy of the encrypted text also rises. However, when working with highly diverse and middle-diversified text, the key length does not seem to have any noticeable effect on the post-encryption text's entropy.

TASK 1.8

When dealing with homogeneous and middle diversified text, there is a trend: longer keys lead to wider gaps between the "peaks" in the graphs. However, with highly diverse text, the key length doesn't seem to make any difference. The autocorrelation graphs look pretty much the same, without any clear recurring patterns.

TASK 1.9

In the context of the examined algorithm, the entropy of the encrypted text consistently surpasses that of the original text, without regard to the text's characteristics or the key length. When dealing with less varied texts, the encrypted text's entropy might occasionally fall slightly short of the maximum value, but for more diverse texts, it consistently approaches the maximum attainable entropy.

TASK 1.10

The time it takes for encryption goes up as the file size and key length increase. But for files up to 5MB, it never took more than 4 seconds, which was quite manageable.

Decrypting files always took a lot more time than encrypting them, especially when dealing with bigger files and longer encryption keys. With a 2048-bit key, decryption consistently took more than 30 seconds, and for a 5 MB file, it often dragged on for over 2.5 minutes.

TASK 1.11

The encryption process for symmetric algorithms typically lasted around 0.3 seconds. It can be concluded that symmetric algorithm encryption happens virtually instantly. There was no noticeable difference with larger file sizes or longer keys.

Decryption, however, required more time as file sizes and key lengths grew. For smaller files (up to 2 MB), decryption finished in less than a second, possibly even in under 0.7 seconds. Even for a 5 MB file, decryption took nearly a full second. This slight increase in time might have been affected by other concurrent system processes, but it didn't pose a significant inconvenience.

TASK 1.12

If you modify a single byte, only a segment of the text changes after decryption, with the altered byte spanning the length of the block used in the algorithm (either 512 bits or 1024 bits). The rest of the text remains unchanged.

When a single byte is removed, the text alteration starts from the block where the byte was deleted, extending to the very end of the text and encompassing the key's length. Deleting multiple bytes yields a similar outcome as removing a single byte: information is lost from the block with the first deleted byte to the end of the text, regardless of the locations of the other deleted bytes. Deleting bytes from the beginning of the text results in the complete loss of the entire content.

If you eliminate a fragment from the ciphertext that matches the block length of the algorithm, only a segment of the same length in the text is lost. The information before and after the deleted block remains intact.

TASK 1.13

Certainly, the segment to be removed must align with the algorithm block's length or multiples of it. In this case, only the portion of the text matching the length of the deleted block is affected, while the remainder of the text remains legible after decryption.

TASK 1.14

Asymmetric algorithms provide greater security compared to symmetric algorithms due to the use of different keys for encryption and decryption. In symmetric algorithms, a single key is employed for both tasks, which means that if one key is compromised, the entire message can be decrypted easily. In contrast, asymmetric algorithms use distinct keys, so knowing one key does not guarantee the ability to decrypt the message, thus enhancing security. Regarding the entropy of the plaintext and encrypted data, both types of algorithms perform similarly, exhibiting better performance with dissimilar texts as opposed to homogeneous ones, regardless of key length.

However, when it comes to the speed of encryption and decryption operations, symmetric algorithms excel. Their encryption and decryption processes are considerably faster due to shorter key lengths and less complex mathematical operations. Asymmetric algorithms, on the other hand, exhibit significantly longer decryption times, particularly for files larger than 5 MB, often surpassing 2.5 minutes. This makes them impractical for encrypting large data files. Furthermore, asymmetric algorithms are more prone to data misrepresentation or partial loss in messages, often resulting in a significant portion of the plaintext or even the entire text being lost. In contrast, symmetric algorithms, depending on the mode of operation, may only lose a very small portion of the text or even just 1 byte.

TASK 1.15

If our priority is to swiftly encrypt and decrypt large volumes of data in near real-time, symmetric algorithms are the more suitable choice, as they involve less complex mathematical operations.

Similarly, if we anticipate frequent interference in the ciphertexts, symmetric algorithms will result in a significantly smaller portion of the text being affected. On the contrary, if the data to be encrypted is relatively small, interference is minimal, and our primary concern is enhancing security rather than the speed of encryption and decryption, then asymmetric algorithms can be employed.