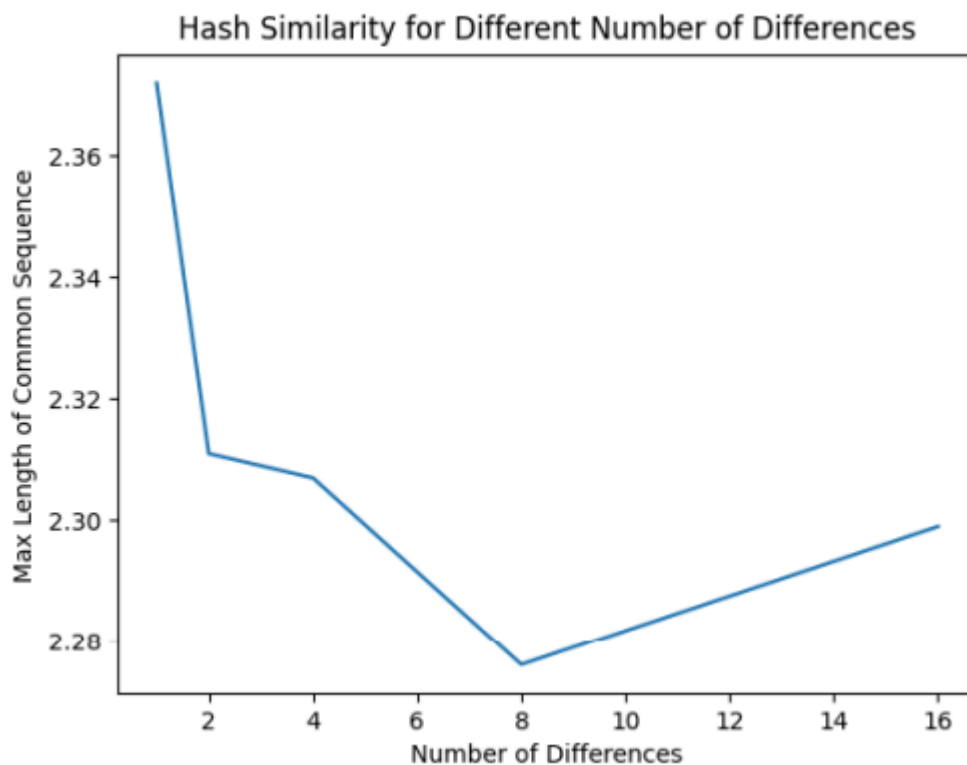
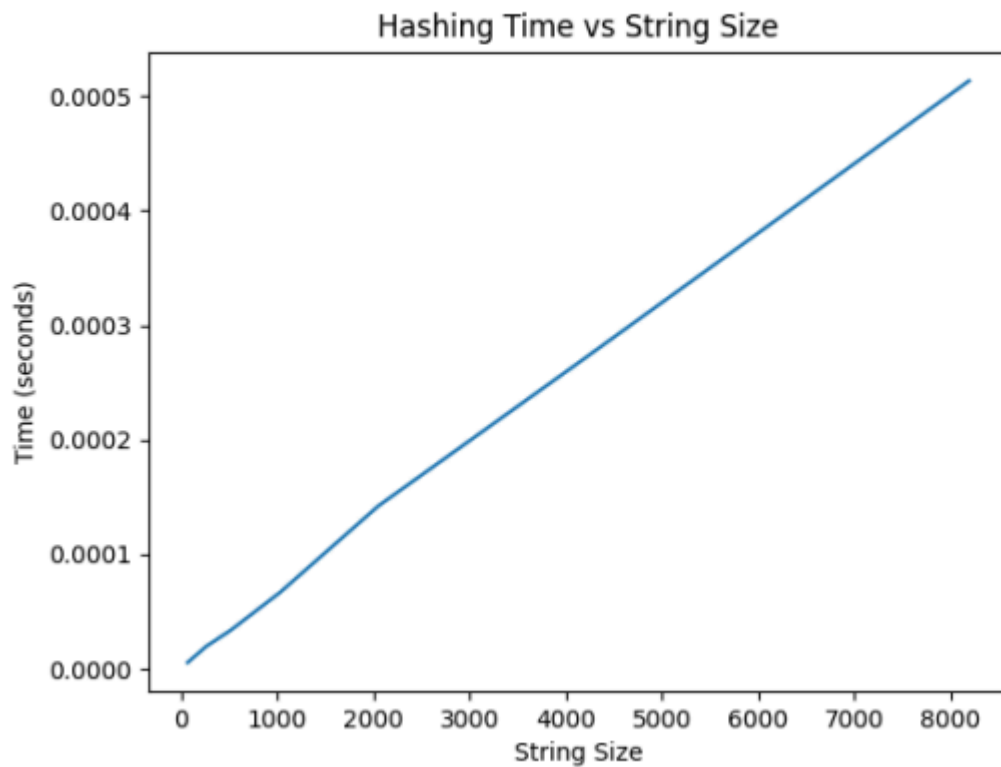


```
1 Test 1 Results:
2 Differences: 1, Avg max common length: 2.319
3 Differences: 2, Avg max common length: 2.271
4 Differences: 4, Avg max common length: 2.265
5 Differences: 8, Avg max common length: 2.305
6 Differences: 16, Avg max common length: 2.32
7
8 Test 2 Results:
9 N = 100, Collisions: 0
10 N = 1000, Collisions: 0
11 N = 10000, Collisions: 0
12 N = 100000, Collisions: 0
13 N = 1000000, Collisions: 115
14
15 Test 3 Results:
16 Size: 64, Average time (microseconds): 17.235
17 Size: 128, Average time (microseconds): 20.829
18 Size: 256, Average time (microseconds): 22.785
19 Size: 512, Average time (microseconds): 30.872
20 Size: 1024, Average time (microseconds): 53.625
21 Size: 2048, Average time (microseconds): 96.936
22 Size: 4096, Average time (microseconds): 171.657
23 Size: 8192, Average time (microseconds): 329.459
24 Ctrl+I to chat, Ctrl+K to generate
```





Заключение. Алгоритм SHA-1 обеспечивает быстрое хеширование ($O(N)$), но уязвим к коллизиям, что делает его небезопасным для криптографии. • Достоинства: Простая реализация, высокая скорость, подходит для контрольных сумм. • Недостатки: Устаревший, незащищён от атак на коллизии (атака SHAttered, может выдать одинаковый хеш для двух разных сообщений).