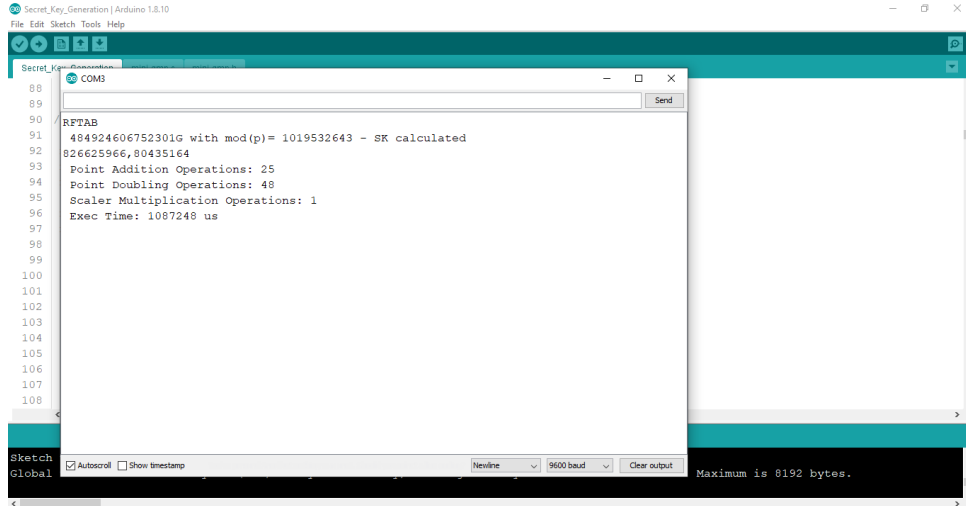


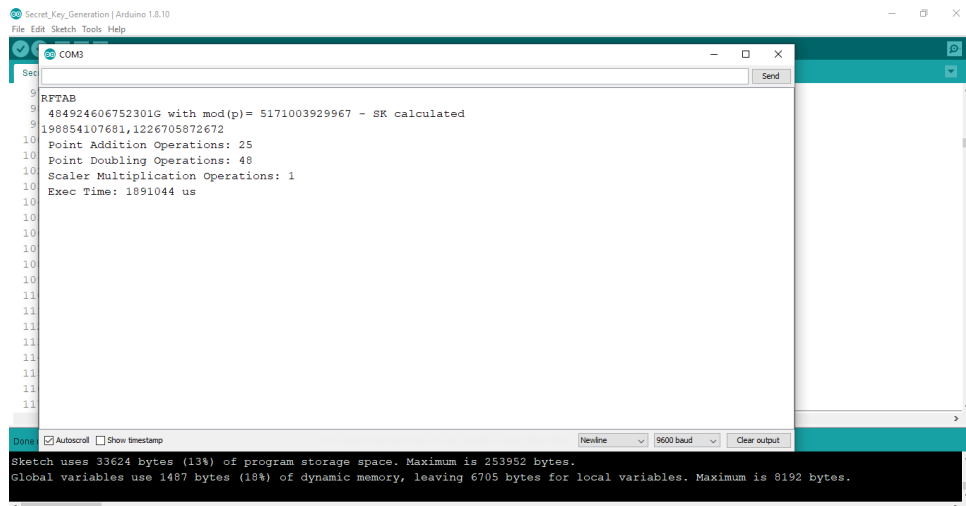
Appendix A

Cryptographic Performance States in the Presented End-To-End Encryption



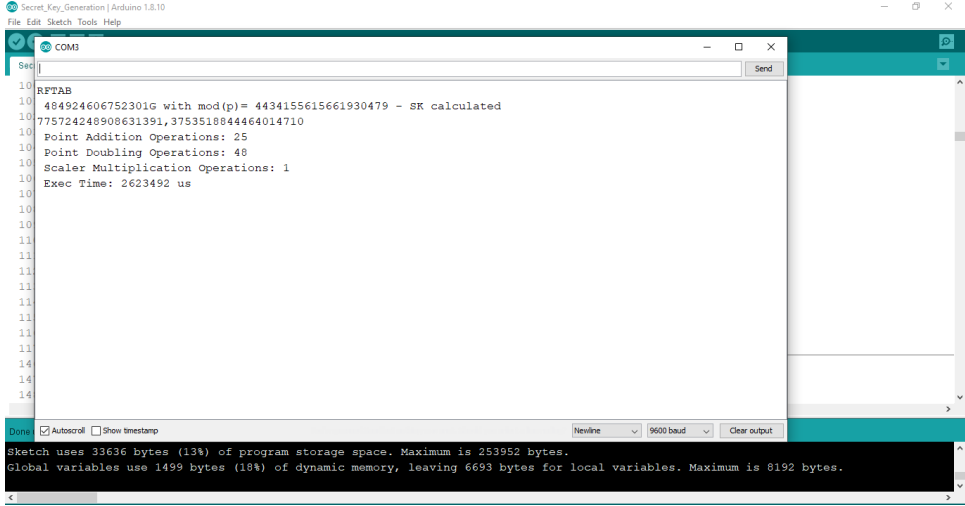
```
88
89
90
91 RFTAB
92 484924606752301G with mod(p)= 1019532643 - SK calculated
93 826625966,80435164
94 Point Addition Operations: 25
95 Point Doubling Operations: 48
96 Scaler Multiplication Operations: 1
97 Exec Time: 1087248 us
98
99
100
101
102
103
104
105
106
107
108
```

(a) - S_k generation at $\text{mod}(1019532643)$



```
9
9 RFTAB
9 484924606752301G with mod(p)= 5171003929967 - SK calculated
9 198854107681,1226705872672
10 Point Addition Operations: 25
10 Point Doubling Operations: 48
10 Scaler Multiplication Operations: 1
10 Exec Time: 1891044 us
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
10
```

(b) - S_k generation at $\text{mod}(5171003929967)$

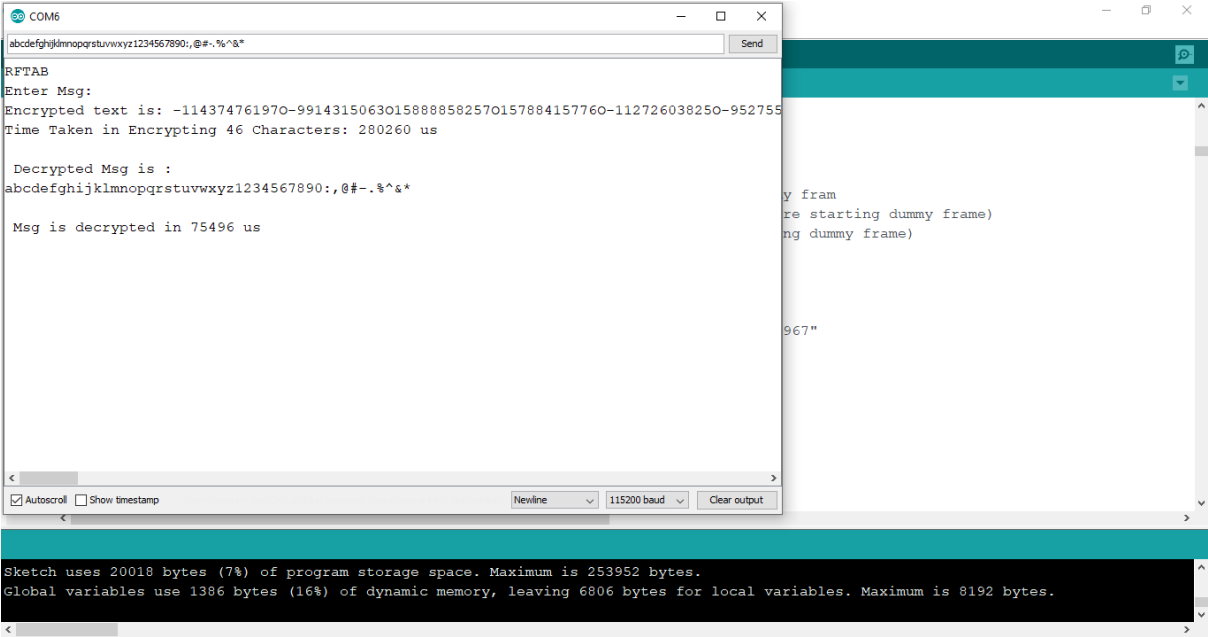


(c) - S_k generation at mod(4434155615661930479)

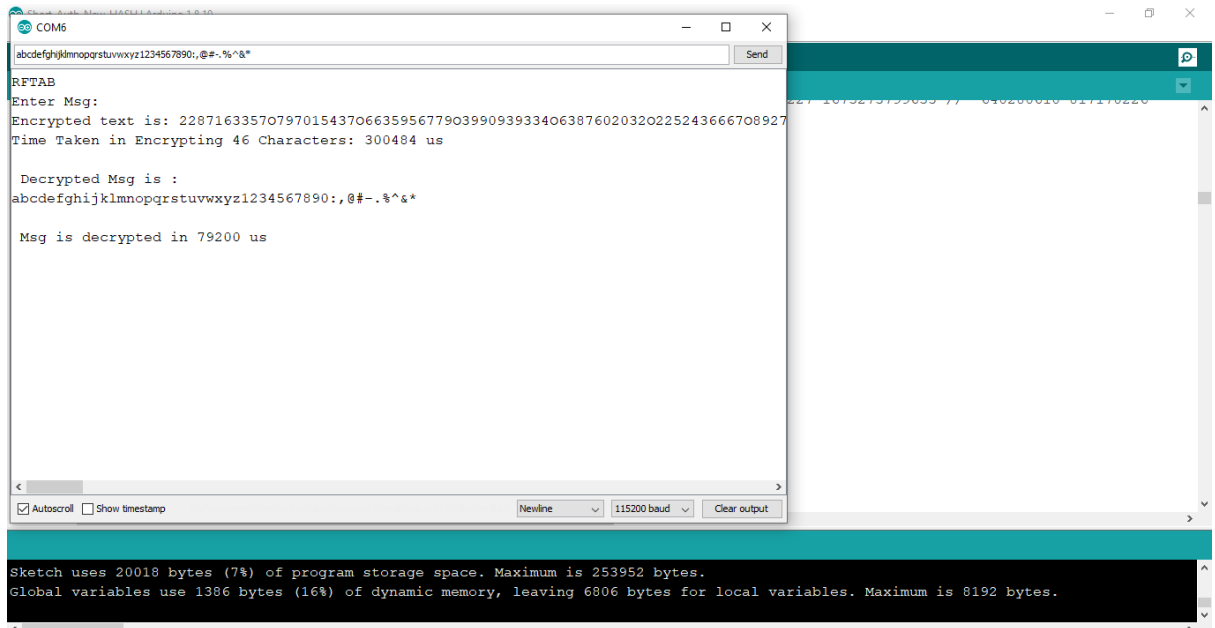
Figure 7.1 : S_k generation during experiments (a), (b) and (c)

Figure 7.1 shows experiments of different mod(p) value used to calculate the secret keys which will further be used to encrypt the current session. These secret keys will be renewed after successful mutual authentication for single session.

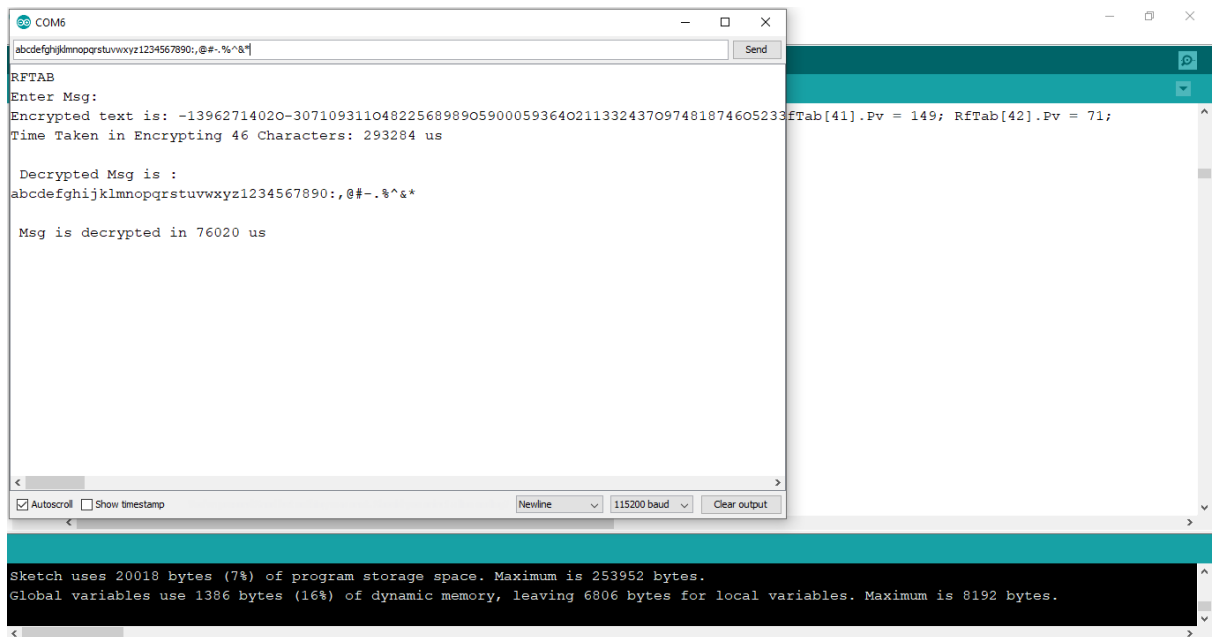
Avalanche Effect Calculation Of 46 ASCII Characters in The Presented Scheme



(a)- Avalanche effect for 32-bit S_k value for mod(1019532643)



(b) - Avalanche effect for 43-bit S_k value for mod(5171003929967)



(c) - Avalanche effect for 62-bit S_k value for mod(4434155615661930479)

Figure 7.2 : Avalanche effect in the presented end-to-end encryption (a),(b) and (c)

Figure 7.2 shows avalanche effect (time taken for encryption and decryption) of 46 ASCII characters in different mod(p) values. These secret keys will be renewed after successful mutual authentication for single session.