CSE 406

Computer Security Sessional

Ataf Fazledin Ahamed
1705066
May 28, 2022

Task 1 - AES Encryption Implementation

	Time (seconds)		
Input Size (char)	**Key Expansion**	**Encryption**	**Decryption**
20	0.00036	0.4937	0.4573
40	0.00056	0.6080	0.7131
80	0.00346	0.9448	1.1510
160	0.00059	1.9120	2.3305

Task 2 - RSA Encryption Implementation

	Time (seconds) [input length = 80]		
size (k)	**Key Generation**	**Encryption**	**Decryption**
16	0.0019	0.00045	0.00049
32	0.0027	0.00029	0.00084
64	0.0024	0.00031	0.00227
128	0.01768	0.000311	0.00415

Task 4 - Heuristic Application

RSA

1. In RSA algorithm, during the key generation- prime numbers are generated starting from the possible max value. Having larger value of both **p** and **q** ensures better strength for the algorithm. Since factorizing **n** becomes harder.

2. While generating the public-private key pair, public keys that are **Fermat's Prime** (expressible as 2^n + 1) ensures better strength for the algorithm.