**IAS Lab Program-4**

Use any one of the programming language C/python/java/C++ to demonstrate Fait-Shamir Authentication scheme using Client-Server model. Use only three rounds to demonstrate the authenticity. Client system can be your host system and Server system can be a virtual machine running on your host system. Show all steps of Fait-Shamir authentication scheme by displaying their values onto the terminal such as witness ‘X’, commitment/Random Number ‘r’, Challenge ‘c’ and response ‘Y’, verification step (Y2 = XVc ), Private Key ‘s’ and Public Key ‘V’. Program should be terminated by displaying an error message when a given input is invalid.

**Test Case 1**

• Round-1: P=467, Q=479, Random Number ‘r’=11, Private Key ‘s’=223694, Challenge ‘c’=0.

• Round-2: P=467, Q =479, Random Number ‘r’ = 60, Private Key ‘s’ = 223694 Challenge ‘c’= 0.

**Test Case 2**

• Round-1: P=929, Q =937, Random Number ‘r’=15, Private Key ‘s’=22, Challenge ‘c’= 0.

• Round-2: P=929, Q =937, Random Number ‘r =41, Private Key ‘s’ =22, Challenge ‘c’= 1

**Test Case 3**

• Round-1: P=727, Q=733, Random Number ‘r’=101, Private Key ‘s’=36, Challenge ‘c’= 1.

• Round-2: P=727, Q=733, Random Number ‘r’ = 60, Private Key ‘s’ = 36 Challenge ‘c’= 1.

**Test Case 4**

• Round-1: P=727, Q=733, Random Number ‘r’=532893, Private Key ‘s’=6, Challenge ‘c’=1.

• Round-2: P=727, Q=733, Random Number ‘r =532897, Private Key ‘s’ =6, Challenge ‘c’=1.

**Test Case 5**

• Round-1: P=89, Q=97, Random Number ‘r’=53, Private Key ‘s’=8635, Challenge ‘c’= 1.

• Round-2: P=89, Q=97, Random Number ‘r’ = 52, Private Key ‘s’ = 8635 Challenge ‘c’= 0.

**Submit the Program file and screenshots to the assigned evaluator on or before 03-03-2021 @ 1:00PM**