Information Assurance and Security (IT352) 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 ($Y^2 = XV^c$), Private Key 's' and Public Key 'V'. Similarly store the appropriate values into an appropriate output-file. Program should consider only the run-time inputs. Program should be terminated by displaying an error message onto the terminal when a given input is invalid.

Sample Text Case

- Round-1: P=467, Q=479, Random Number 'r'=1111, Private Key 's'=111, Challenge 'c'= 1.
- Round-2: P=929, Q =937, Random Number 'r' = 760, Private Key 's' = 200 Challenge 'c'= 1.
- Round-3: P=727, Q=733, Random Number 'r =540, Private Key 's' =1000, Challenge 'c'= 0.

Submit program file, all screenshots and all output files (output.txt) to the Email ID which will be circulated with the text case file before the deadline.

Email subject should be IAS(IT352)-Lab-Program-4-Related-Files

File name of the program	:	RegisterNo_IT352_P4
		(P4 indicates Lab Program Number-4)
File name of the screenshot	:	RegisterNo_IT352_P4_S1-Clientside
		RegisterNo_IT352_P4_S1-Serverside

(S1 indicates screenshot for the first test case, similarly, for other test cases S2, S3, S4, S5)

File name of the Output File	:	RegisterNo_IT352_P4_Output_TC1-Clientside.txt
		RegisterNo_IT352_P4_Output_TC1-Serverside.txt

(TC1 indicates output for the first test case, similarly, for other test cases TC2, TC3, TC4, TC55)

Date of Laboratory	:	7th February 2020, Friday
Deadline of Submission	:	7th February 2020, Friday (on or before 6:00PM)

Note:

- Clarify the doubt(s) (if any) on or before 6th February 2020 (Thursday).
- No/Zero marks for incomplete submission/late submission/absent for the Lab/incomplete program.