Indian Institute of Information Technology (IIIT) Chittoor, Sricity
Questionnaire for BTP-Progress Evaluation
Wednesdays, 3:30 – 5pm
Spring 2016

1. Describe what you have done in the last 3 weeks.

First part of our BTP I.e Authentication is done. We evaluated the performance of 2 cryptography algorithms (RSA and ECC). We are writing a paper on our work and are planning to submit the paper to mobihoc conference. We also tried to establish connection between two machines (assuming them as vehicles at rest). These two machines were able to chat/communicate with each other. We also tried implementing another assymetric key cryptographic algorithm (El Gamal)

2. How many times did you meet / talk with your faculty / guide?

Almost 3-4 times a week.

3. How many papers / articles / technical materials have you read in the last 3 weeks?

Since we were writing paper, we went through 10-12 papers not completely but to an extent that we needed

4. Provide a brief summary of your learning?

The performance of ECC algorithm is very good and is apt for real-time usage compared to that of RSA algorithm. We have tabulated the results of the time taken by each algorithm for key-generation, encryption and decryption.

5. What development / programming / practical activity did you do in the last 3 weeks.

We established a TCP connection (network coding) between two machines and successfully sent message between the two machines.

6. How close/far are you from the milestone set by your Guide?

Our faculty asked us to write a paper on our work and we reached the milestone set.

7. What specific challenges are you facing/you faced in the last 3 weeks?

El Gamal algorithm coding is taking time. We are trying to understand how this algorithm actually works. Then we started implementing it. We are struck with the key generation part. We are clear how to encrypt and decrypt the data once the public and the private keys are generated.

8. Propose your plan for the next 3 weeks; as agreed with your supervisor. It would be verified in the next round Q1.

Performance evaluation of RSA, ECC algorithms with the El Gamal algorithm.