International Institute of Information Technology, Hyderabad.
Principles of Information Security

Evaluation V

April 26, 2020

Due: **May 3, 2020**.

Instructions : Each evaluation sheet consists of three categories of questions, namely: [**P**] stands for *programming* assignment, [**Q**] stands for *question* with written solution to be submitted and [**R**] stands for *research* problem. You need to submit the source-code for [**P**] along with a screen-recorded video that demonstrates its execution and for [**Q**] you may submit a pdf-file solution, all by the due-date. The research problems are *optional*, and anyone who solves any *one* of the [**R**] problems among *all* evaluation sheets will directly be awarded an **A** grade.

[**Q**] Recall that in Evaluation II, k blocks of data/information is encoded into n blocks such that if any e of the n blocks are corrupted, it is still possible to retrieve the original k blocks of information. Show how to use this to build a robust (torrent like) routing scheme where the sender and the receiver have n different connections/routes and the task is to send k blocks of data successfully even if up to any e of the n connections are corrupt. Further, using a public-key cryptosystem, say El Gamal, design a Robust Oblivious Transfer protocol between a client A (who has the index i) and server B (who has the array) such that A and B are part of a large network and reliably communicate via the above robust (torrent) routing mechanism (you may have to design four different protocols in the four cases outlined below). What do you think would be the maximum tolerable e when (a) the public-keys of A and B are known to all, (b) public-key of A is known to B, but B's public-key is not known to A, (c) public-key of B is known to A, but A's public-key is not known to B and (d) neither party knows the public-key of the other party.

[**P**] Implement (in any popular programming language of your choice) your newly designed Robust Oblivious Transfer protocol between A and B (assuming all public-keys are known to all parties).

ALL THE BEST

[**R**] Given a digraph G (a directed network, that nodes A and B are part) of which up to any e nodes may be corrupted by an adversary, what is a necessary and sufficient condition on G such that Oblivious Transfer between A and B is possible, given the condition that initially, no node knows the public-key of any of the other nodes.