HIT — Cryptography — Homework 6

September 19, 2014

Problem 1. We have almost finished the course. Let's put things together to design a secure communication system for a multi-player on-line game platform, such as the DOTA or the SanGuoSha. Communications are among players with or without a centric server. In your report, please describe the threats your system may face, the cryptographic requirements and the corresponding constructions to satisfy the requirements. The description of threat may look like this:

- In on-line gaming, one player may eavesdrop the messages between another player and the centric server, which can happen when two players are within the same LAN. Then the eavesdropping player may learn something which should be confidential, such as the current position of the other on the map in the DOTA, or cards in the other's hand in the SanGuoSha.

Please present at least two other threats besides the above example. If the threat you proposed is novel and different with others, and you give a reasonable design to avoid or detect the threat, you will be awarded 5 extra points.

Now let's make on-line gaming fair-play!