Project (1/3)

Alice and Bob are subcontractors (security auditors) of the same company that claims it has given them different code-segments to audit. They each have received 5 segments of code (each of them is a file of*~500MB).* They want to see if they have received the same segment. But … they do not trust each-other to show their segments!

Your goal is to implement a protocol which will allow them to check the above without any of the parties revealing to the other party the contents of any of its files.

- You may assume that Alice and Bob might only launch passive attacks—i.e., will follow whatever protocol they are given but might locally try to extract information from their view.
  - Note that the parties may not follow instructions of the type: "don't look at the received message" or "erase the received message".
- The adversary will try to attack the communication between Alice and Bob.
- Alice and Bob do not initially share a key.
- You can use off-the-shelf cryptographic libraries but you need to reference the source.
- You can use c++, java, python, or rust in your implementation.
  - We will ask you to commit to your language within 2 weeks from start.

Project (2/3)

- You may form teams of up to 3 students. You may give your team a name.
- Each team will have two roles: blue (develop a solution to the problem) and red endorse or attack the solution of a dedicated blue team.
    - We will announce the red-blue combinations once codes have been submitted. (Each red team will be assigned two blue teams)
- Deliverables:
    - code + spec
    - security analysis
    - **You should specify your security goals and show that they are achieved!**
    - attack or endorsement
    - **You may attack the theory (insufficient goals incorrect argument) or implementation!**
    - in-class presentation: short description + demo + attack (if applicable)
- Indicative Points (if points are >10 then 10; if points are < 0 then 0):
    - +6: on-time submission (no late submissions will be accepted) + presentation.
    - +2: for being endorsed by at least one corresponding red team (or instructors).
    - +2: attack each of your blue teams. (in total +4 possible points)
    - +2: if you endorse or attack both your blue teams and you are not contradicted (instructors might attack too so blindly endorsing is not optimal …)
    - -3: for false endorsement or attack
    - -6 for not endorsing or attacking each of your blue teams. (in total a possible -12)

Project (3/3)

- Deadlines (all deadlines are 11:59pm of the day; no late submissions, endorsements, or attacks are allowed):
  - Code and spec final commit: Wednesday, Nov 29, 2023
  - Attack/endorsement & Presentations: Sunday, December 3, 2023
  - Presentation: In-class: Tuesday December 5 (in class), 2023