Offending other players

- acting against the 'spirit' of the game
    - problematic: is camping in a first-person shooter cheating or just a good tactic?
    - some rules are 'gentlemen's agreements'
- examples
    - killing and stealing from inexperiened and ill-equipped players
    - gangs and ghettoization of the game world
    - blocking exits, interfering fights, verbal abuse

Upholding justice

- players handle the policing themselves
    - theory: players take the law into their own hands (e.g., militia)
    - reality: gangs shall inherit the game world
- systems records misconducts and brands offenders as criminals
    - theory: bounties and penalties prevent crimes
    - reality: throw-away avatars commit the crimes
- players decide whether they can offend/be offended
    - theory: players know what kind of game world they want
    - reality: how to offend you? let me count the ways…

Counter-measures

- methods to prevent cheaters from tampering the network traffic
- MD5 algorithm
    - guarantee the integrity of the data
- lockstep protocol (and its variants)
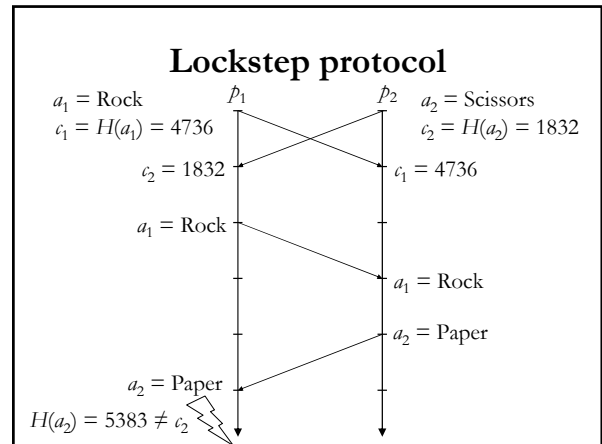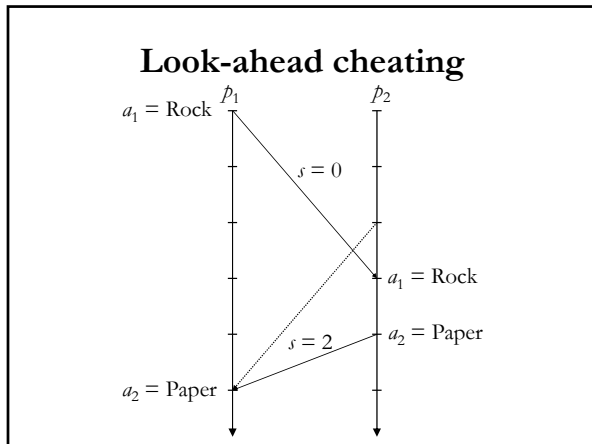   - prevent look-ahead cheating

MD5 algorithm

- message digest = a constant length 'fingerprint' of the message
- no one should be able to produce
    - two messages having the same message digest
    - the original message from a given message digest
- R. L. Rivest: MD5 algorithm
    - produces a 128-bit message digest from an arbitrary length message

Lockstep protocol

- players announce time-stamped actions
- look-ahead cheating: delay action annoucement to see what the other players are doing
- lockstep protocol
    1. announce a commitment to an action
    2. when everybody has announced their commitments, announce the action, which can be checked against the commitment

Commitment

- requirements
    - action cannot be inferred from the commitment
    - easy to compare whether an action corresponds to a commitment
- formed with a one-way function
- commitment = *hash*(action)

Look-ahead cheating

p_1 p_2

$a_1 = $ Rock

$s = 0$

$a_1 = $ Rock

$a_2 = $ Paper

$s = 2$

$a_2 = $ Paper

Lockstep protocol

$a_1 = $ Rock p_1 p_2 $a_2 = $ Scissors
$c_1 = H(a_1) = 4736$ $c_2 = H(a_2) = 1832$

$c_2 = 1832$ $c_1 = 4736$

$a_1 = $ Rock

$a_1 = $ Rock

$a_2 = $ Paper

$a_2 = $ Paper

$H(a_2) = 5383 \neq c_2$

Loosening the synchronization 1(2)

- the slowest player dictates the speed
  - short turns
  - time limits for the announcements
- asynchronous lockstep protocol
  - sphere of influence: synchronization is needed only when the players can affect each other in the next turn(s)
  - otherwise, the players can proceed asynchronously

Loosening the synchronization 2(2)

- pipelined lockstep protocol
  - player can send several commitments which are pipelined
  - drawback: look-ahead cheating if a player announces action earlier than required
- adaptive pipeline protocol
  - measure the actual latencies between the players
  - grow or shrink the pipeline size accordingly

Recapitulation

- goals
  - protect the sensitive information
  - provide a fair playing field
  - uphold justice inside the game world

- cheats
  - tampering network traffic
  - illicit information
  - exploiting design defects
  - collusion
  - offending other players
- counter-measures
  - MD5 algorithm
  - lockstep protocol