Peer-to-peer карточные игры

Студент: Геллер М.А.
Руководитель: Давыдова М.С.

Sunday 15th January, 2017

JetBrains

ПРЕДПОЛОЖЕНИЯ

Цель - исследование возможности создания криптографически защищенных систем для карточных настольных игр

Общие положения протоколов:

- Громкое общение
- Игры должны завершаться
- Нарушения правил должно выявляться

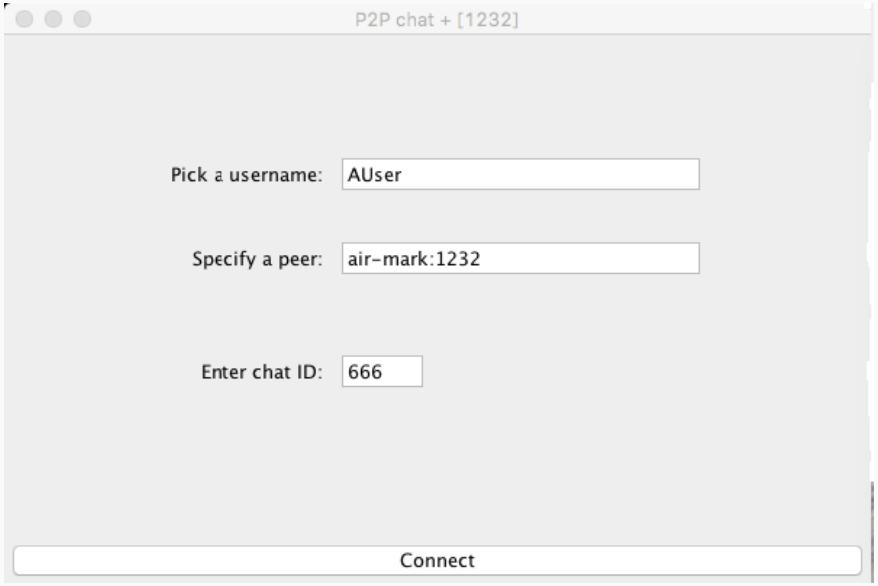
Не учитываемые уязвимости:

- Обмен данными по стороннему каналу
- Атаки порядка 2^{60} и выше
- MiM атаки во время установления соединения

P2P ЧАТ

Система P2P чатов позволяет:

- Обмениваться сообщениями
- Начинать игры
- Отображать логи



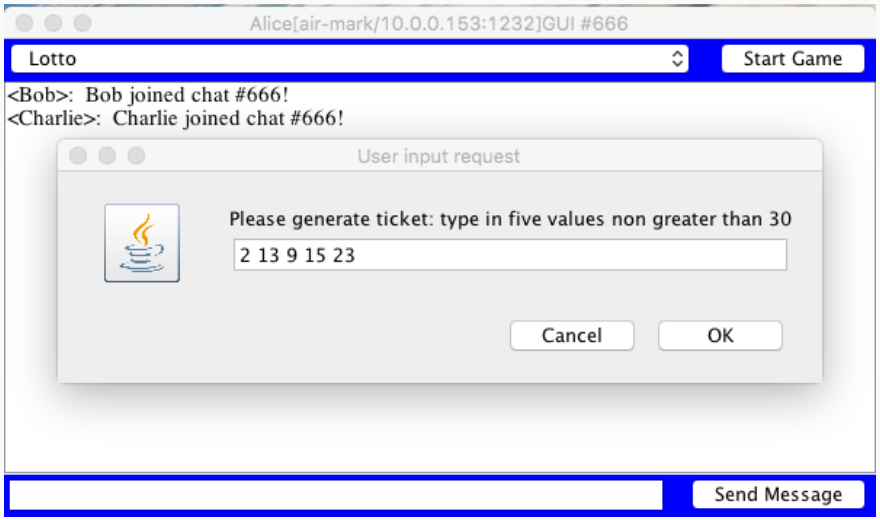
Использованные технологии:

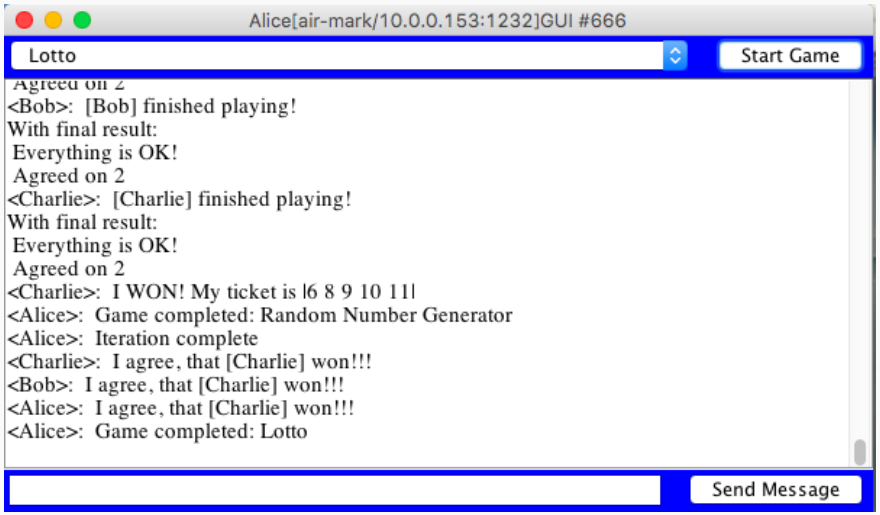
- Netty
- Google protobuf
- Swing

ЛОТТО

Простые правила:

- **«Билеты»** — уникальные наборы
  из пяти чисел от 1 до 30
- Генерация общих случайных чисел
- Определение победителя





Технологии - те же

protobuf Protocol Buffers

Netty

Java Swing

ПРЕФЕРАНС

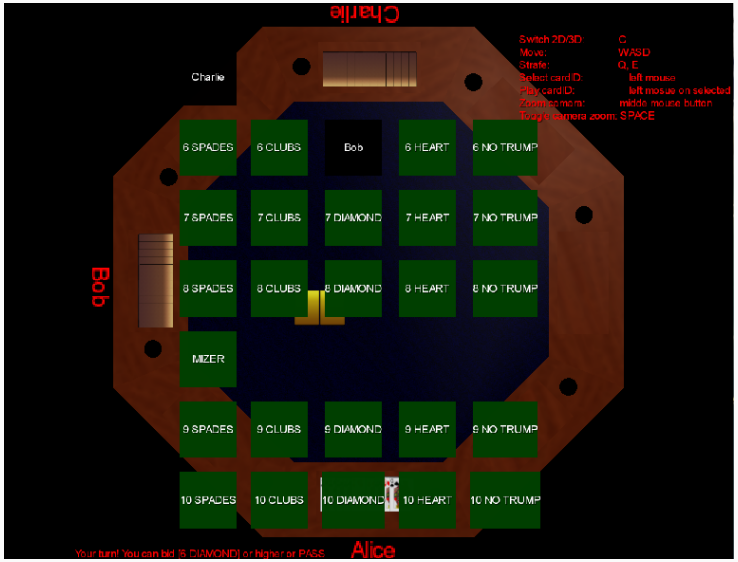
Получили

- Преферанс на трех игроков
- 2D/3D графический интерфейс

Сложные правила!

Использованные технологии:

- Libgdx
- Bouncycastle

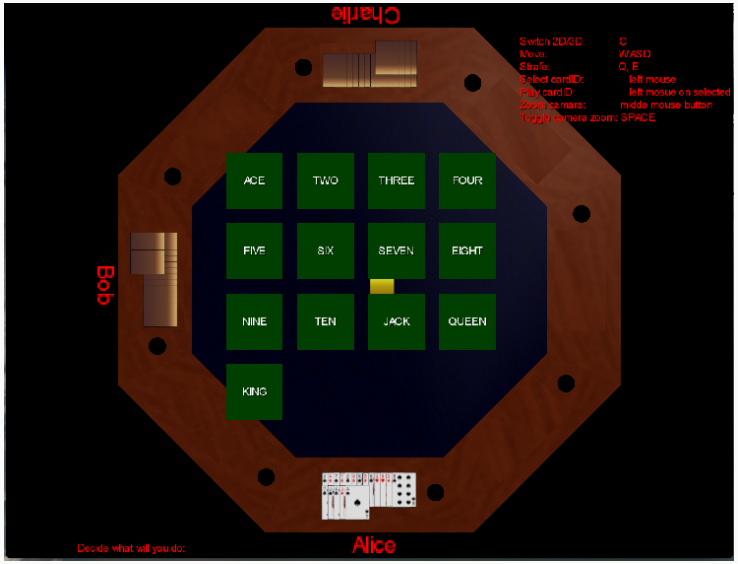


ВЕРЮ НЕ ВЕРЮ

Простые правила!

Новые задачи:

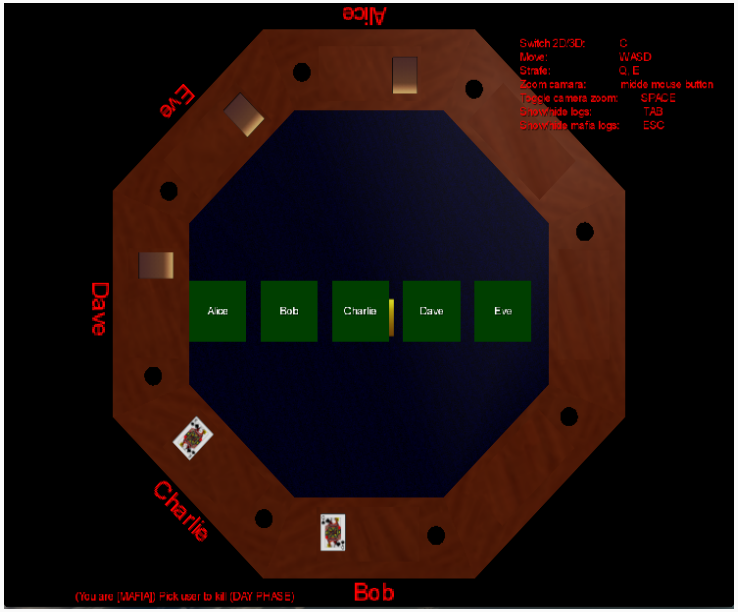
- Передача данных НЕ ВСЕМ игрокам
- Устойчивость к коалициям

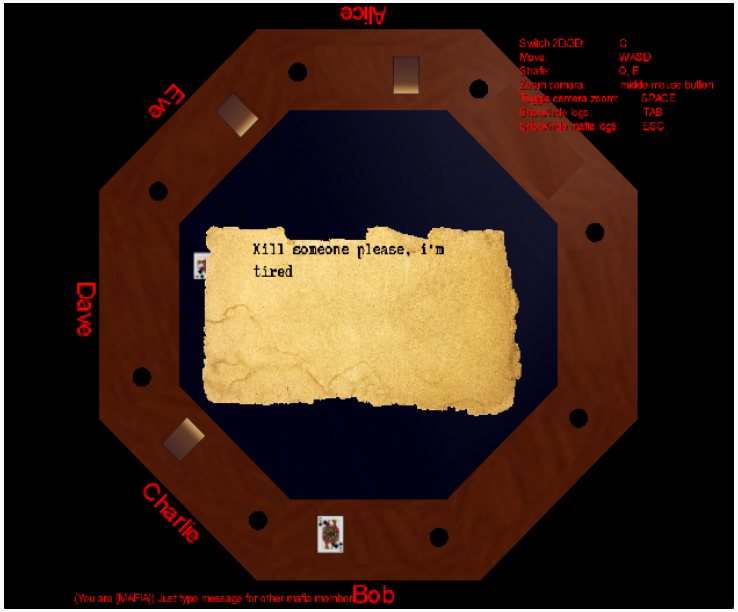


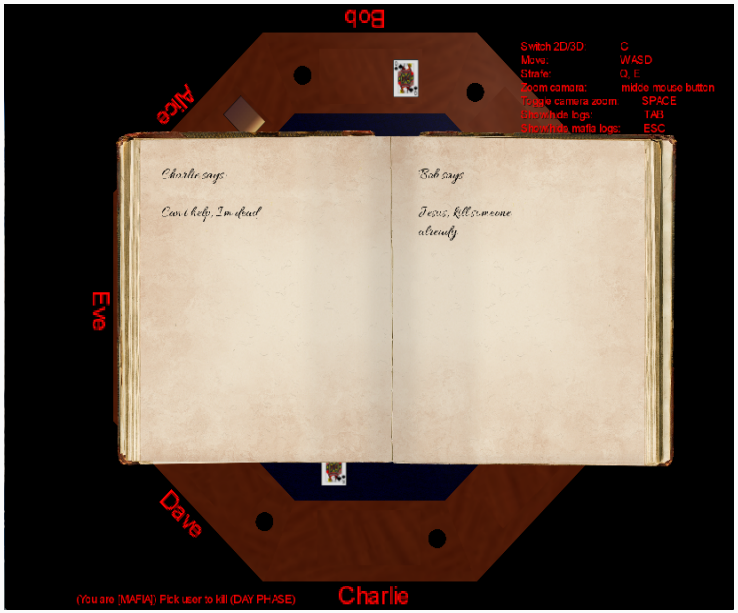
Технологии - те же:

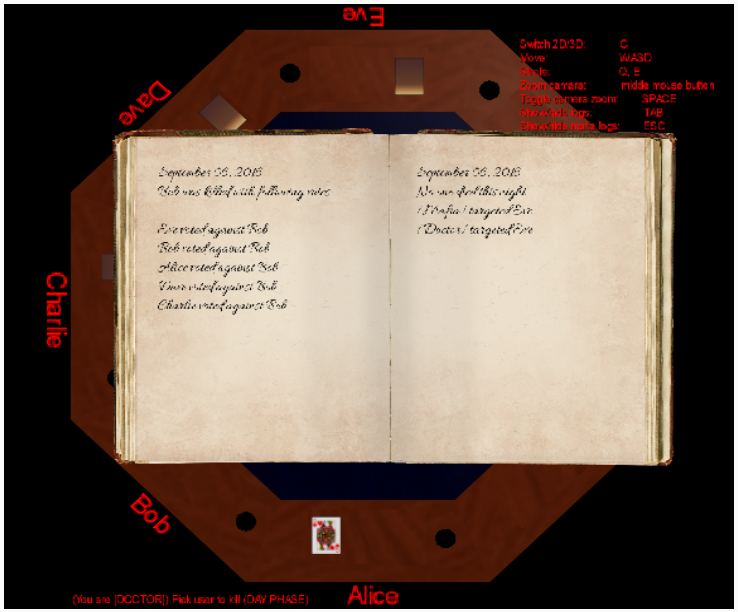
libGDX

МАФИЯ (БЕЗ ВЕДУЩЕГО)









THE END.

https://github.com/JetBrains/p2p-games

ПРЕФЕРАНС

«Преферанс» - популярная в России карточная игра

Идеологическая сложность - Создание общей колоды

Решение:

Imre Bárány — Mental poker with three or more players, 1983

Choongmin Lee — Simple TTP-free Mental Poker protocol, 2014

ПРЕФЕРАНС

«Преферанс» - популярная в россии карточная игра

Идеологическая сложность - Создание общей колоды

Решение:

Imre Bárány — Mental poker with three or more players, 1983

Choongmin Lee — Simple TTP-free Mental Poker protocol, 2014

А еще у преферанса длинные, запутанные правила

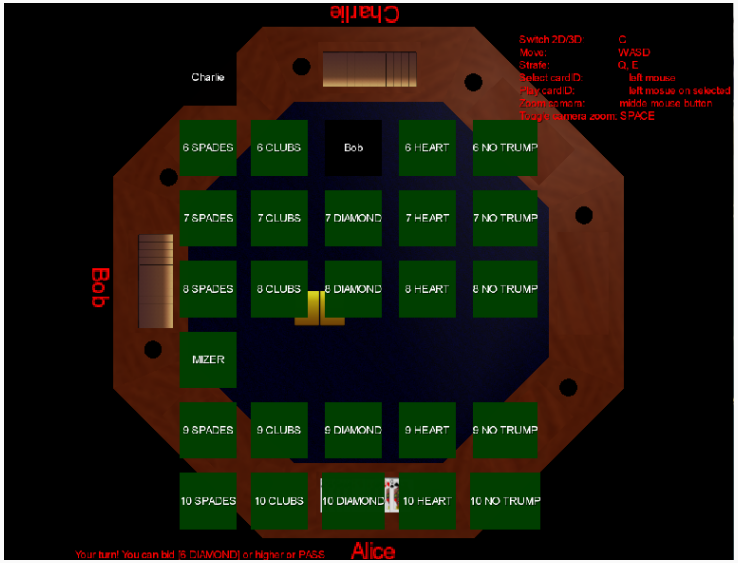
ПРЕФЕРАНС

В результате имеем:

- Преферанс на трех игроков
- 2D/3D графический интерфейс

Использованные технологии:

- Libgdx
- Bouncycastle



ВЕРЮ НЕ ВЕРЮ

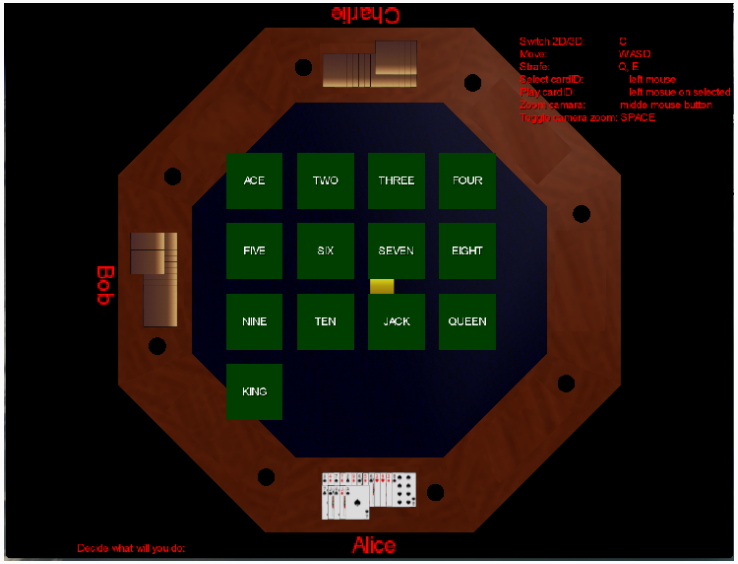
Простые правила!

Новые задачи:

Передача данных НЕ ВСЕМ игрокам

Решение: Ассиметричное шифрование

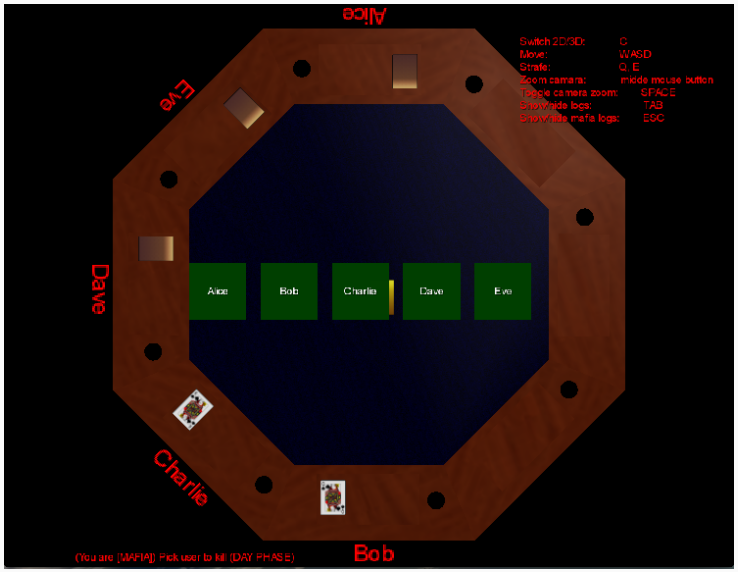
Устойчивость к коалициям

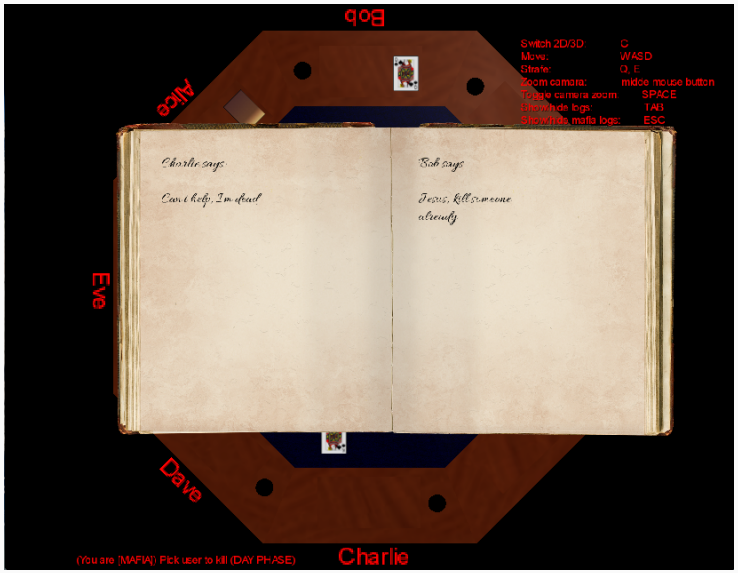


МАФИЯ (БЕЗ ВЕДУЩЕГО)

Интересные задачи:

- **Распределение ролей** — основано на mental poker
- **Создание распределенного секрета** — основано на mental poker
- **Создание общего секретного ключа** — основано на mental poker
- **Общее голосование(День)** — commitment scheme





МАФИЯ (БЕЗ ВЕДУЩЕГО)

Интересные задачи:

- **Мафия, общение** — commitment scheme, общий секретный ключ
- **Комиссар: выбор цели** — EC Secure Multiparty Sum, распределенный секрет
- **Мафия, Доктор: выбор цели** — EC Secure Multiparty Sum