Projeto de Formatura – Turmas 2016

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia Elétrica – Ênfase Computação

Tema:

VSCryptoPoker: um Pôquer P2P Seguro

Introdução

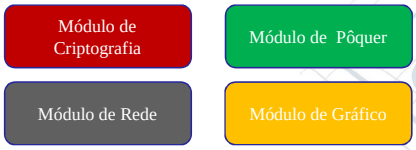
Atualmente, duas grandes tendências na área de *Software*, têm sido o desenvolvimento de sistemas mais independentes e seguros. Aliando essas tendências com o nosso interesse em criptografia e jogos, nosso projeto foi a implementação de um jogo de *Mental Poker*.

Mental Poker

Mental Poker é o termo acadêmico utilizado para um jogo de pôquer em que dois ou mais jogadores não confiáveis, podem jogar um jogo honesto. O maior problema no desenvolvimento desse tipo de jogo, é o fato que todos jogadores precisam dividir um "baralho" em comum, ou seja, um dilema pois as cartas precisam ser um conjunto de dados que todos podem ver mas não podem saber qual é a carta. Para atingir tal feito, utiliza-se criptografia, tal que todos podem tem os dados, mas até que os mesmos sejam decifrados, não dá para saber qual carta cada um representa.

Módulos

O sistema foi desenvolvido em 4 módulos: Módulo de criptografia, Módulo de pôquer, Módulo de rede e Módulo gráfico.



Módulos de criptografia

Esse módulo é o responsável por criar a chave pública e privada de cada jogador, também é responsável por encriptografar e descriptografar os dados . A criptografia usada nesse módulo é a ElGamal.

Criptografia ElGamal

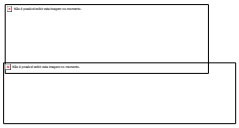
q,**p** e **g** são parâmetros aleatórios

m = conteúdo não-cifrado (valor original)

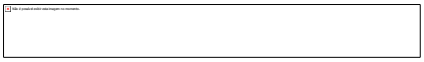
r = Chave privada (inteiro aleatório)

$\boldsymbol{u = g^r \bmod p}$ = Chave pública

Cifração (recebe **m** e retorna $\boldsymbol{c_1}$ *e* $\boldsymbol{c_2}$):



Decifração (recebe $\boldsymbol{c_1}$ *e* $\boldsymbol{c_2}$ *e retorna* $\boldsymbol{m}$) :



Módulos de pôquer

Esse módulo é o responsável por fazer a lógica do jogo de pôquer e é onde guarda-se todos os dados do jogo (cartas na mesa, cartas da mão, aposta, dinheiro) e também faz a avaliação da mão vencedora do jogo.

Módulos de rede

Esse módulo é o responsável pela comunicação. Nele, são instanciados e conectados todos os *Sockets* de cada um dos jogadores. Permitindo assim uma comunicação e transferência bilateral entre todos os jogadores, formando a nossa rede P2P.

Módulos gráfico

Esse módulo é o responsável pela *GUI(Graphic User Interface*) gerando uma interface gráfica do jogo, também é responsável por receber a interação do usuário com a tela.

Imagem retirada do jogo

Outras tentativas de criptografia, RSA

Durante o desenvolvimento do sistema, nós utilizamos inicialmente a criptografia RSA modificada para ser comutativa, por ser muito utilizada e ser fácil de implementar. Entretanto, depois de implementada, verificamos que as chaves criptográficas ficavam muito fracas, tornando-se uma brecha de segurança. Por esse motivo, resolvemos utilizar a criptografia ElGamal modificada.

Código Aberto

Todo o código do nosso projeto desenvolvido foi postado tanto na rede social Github como no site do nosso grupo na matéria PCS2502, nosso código é aberto (*Open Source*) para que qualquer um que tenha interesse no projeto possa testá-lo ou utilizá-lo para o desenvolvimento de seus próprios sistemas.

Integrantes: Arthur Kenzo Motinaga Sato
Tomas Monteiro Vitorello

Professor Orientador: Prof. Dr. Marcos Antonio Simplicio Junior
Co-orientador: