UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE COMPUTACION
SEGUNDO CUATRIMESTRE - MMVII

Criptografía

Trabajo Práctico: Truco Mental

Diseñar e implementar un protocolo para el reparto de cartas y juego de *Truco Mental* entre dos jugadores.

El reparto debe ser tal, que todas las manos sean igualmente probables y que cada jugador conozca sus cartas sin que el contrario las pueda deducir. Al final del juego, ambos jugadores tienen que poder verificar que las cartas jugadas son las que fueron efectivamente repartidas (si es necesario).

El juego se desarrolla entre dos jugadores, *Mano* o *Cliente* y *Pie* o *Servidor*. El Pie puede recibir invitaciones de juego de varios clientes simultáneos, y tiene que ser capaz de servir a cada uno, sin necesidad de sincronismo alguno (con cada uno utiliza un juego de cartas diferente).

El mazo se compone de 40 cartas, cuyas descripciones deberán leerse de un archivo de configuración común a ambos (no es necesario intercambiar este archivo al principio del protocolo). Por otra parte, se supone que las declaraciones de *envido* o *truco*, la bajada de cartas sobre la mesa y el registro de puntuación corren por un canal alternativo que también hay que implementar.

La implementación se puede hacer en *C*/*C*++ o *Python* y en *C*/*C*++ se puede utilizar cualquier librería de números grandes.

Se deberá entregar: el diseño del protocolo, implementación, con programas fuente (requerido) y ejecutables (si los hubiera), manuales de usuario, explicación de decisiones de diseño e implementación, conclusiones y bibliografía.

Se hará especial hincapié en la calidad de la documentación, la estructura del código fuente y la facilidad de lectura de ambos.

Fuente:

1. Adi Shamir, Ronald L. Rivest, Leonard M. Adleman. Mental Poker. David A. Klarner Ed. The Mathematical Gardner, Prindle, Weber and Smith, Boston, Massachusetts, 1981.