Criptografía

Segundo Cuatrimestre de 2007

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Trabajo Práctico

Truco Mental

Integrante	LU	Correo electrónico
Albanesi, Matías	??/??	mac@sion.com
Carbajo, Pablo	717/04	pcarbajo@dc.uba.ar
Freijo, Diego	4/05	giga.freijo@gmail.com
Venturini, Maura	-	venturinimaura@gmail.com

Abstracto

En el presente trabajo se diseño e implementó un protocolo para jugar al truco mediante el cual se asegura el cumplimiento de las reglas de juego.

Palabras Clave

Encriptación, algoritmos de clave pública/privada y simétricos, RSA, AES, Mental Póker, Mental Truco.

Índice

1. Introducción

La motivación del trabajo surge de la necesidad que imponen ciertos juegos de cartas de poder repartir los naipes entre distintos jugadores en forma azarosa (justa), y que garantice de alguna manera que ninguno de los jugadores haga trampa en lo que al reparto y juego de las cartas se refiere. Lograr esto en una implementación por software de juegos de este tipo requiere obligatoriamente de técnicas criptográficas, ya sea de firma y/o encriptación de mensajes. Dentro de estos juegos, el Truco tiene la particularidad de que puede ser necesario que un jugador muestre ninguna, alguna, o todas las cartas que recibió.

El objetivo del trabajo es diseñar e implementar un protocolo para el reparto de cartas y juego de Truco Mental entre dos jugadores. El protocolo está diseñado para garantizar una justa repartición de cartas y que cada parte juege sólo cartas que le fueron repartidas. Además, el protocolo permite que un jugador muestre sus cartas selectivamente, y que verifique que las cartas pertenecen a un mazo inalterado.

El lenguaje elegido es Python. La implementación realizada permite que dos jugadores juegen una mano a través de una conexión por red. Al ejecutar el programa, éste pregunta si debe ser ejecutado en modo cliente o modo servidor. Si se ejecutaran varias instancias del servidor en la misma computadora, se podría dar un servicio de truco a varios jugadores simultánea e independientemente.

2. El juego del truco

2.1. Reglas de juego

Si bien reglas del juegos varían en distintos países, en

`http://usuarios.arnet.com.ar/leo890/truco.htm`

se puede encontrar una explicación de las reglas del juego tal cual se juega en Argentina. A lo largo del trabajo usaremos el término submano para referirnos a lo que el citado documento se refiere como proceso de bajar cartas. De ésta manera cada mano se puede dividir en 3 submanos, denominadas primera, segunda y tercera. Nótese que una mano puede finalizar antes de ser jugadas las 3 submanos, e incluso una submano puede quedar inconclusa si la mano termina antes que la submano.

2.2. Lógica de juego

2.2.1. Manejo de las Cartas

Valores de las cartas:

```
0   01E
1   01B
2   07E
3   07O
4   03O,03C,03B,03E
5   02O,02C,02B,02E
6   01O,01C
7   12O,12C,12B,12E
8   11O,11C,11B,11E
9   10O,10c,10B,10E
10  07B,07C
11  06O,06C,06B,06E
12  05O,05C,05B,05E
13  04O,04C,04B,04E
```

Se define un orden parcial entre las cartas, que indica el valor relativo entre ellas. Esto nos va a servir para después comparar, en base a las cartas en la mesa, quién "mató", y a quién le corresponde jugar.

Para ver quién gana la mano, buscamos las dos cartas que están sobre la mesa y vemos cuál tiene el nivel más alto, esa es la que gana la mano. En caso de estar en niveles iguales hay parda y le toca jugar al jugador que es mano.

2.2.2. Manejo de Cantos

Envido

- Se puede cantar Envido hasta antes de jugar la primer mano.
- Se puede seguir contestando hasta que se diga “Quiero”; acá se procede a ver qué cartas son del mismo palo y se suman los valores (en caso de tener flor se suman los dos más altos), o “No Quiero”; no cuento nada y sigue el juego.
- Si se cantó “Truco” no se puede cantar “Envido”.
- Si ya se dijo “Quiero” o “No Quiero”, no se puede seguir cantando.

Truco

- Se puede cantar en cualquier mano e inclusive antes de jugar la primera carta.
- El ganador de 2 de 3 manos es el que gana la mano.
- Una vez que los 2 jugaron las 3 cartas no se puede cantar “Truco”.

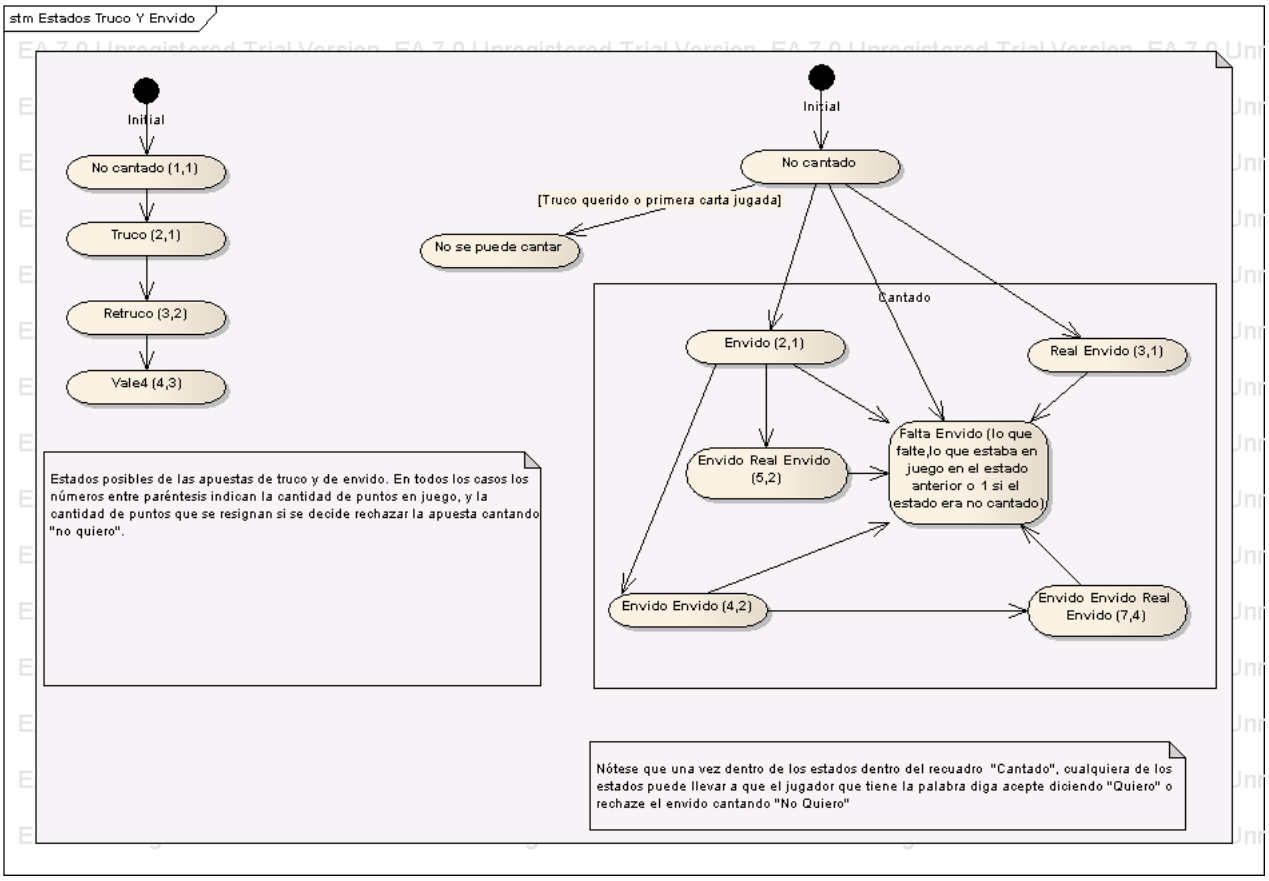


Figura 1: Estados Truco y Envido

- Los cantos deben manejarse como interrupciones. Un jugador puede cantar “Truco” habiendo jugado su carta o no. No es asi el caso del “Envido”; aca hay que controlar que el jugador tenga el token (le toque jugar) y no haya tirado su carta.

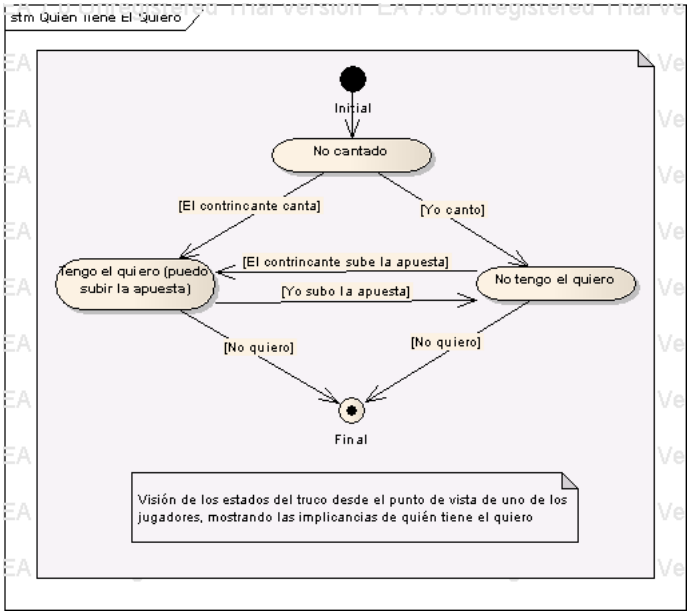


Figura 2: Quien tiene el quiero

2.2.3. Registros a Tener en Cuenta

- Cantidad de Manos Ganadas
- Si se cantó "Envido"
- Si se cantó "Truco"
- Al finalizar la mano:
  - Si se cantó "Envido" me fijo si en las cartas sobre la mesa están los puntos del "Envido". Si no, muestro las que faltan aunque se haya ido al mazo.
  - Si se fue al mazo (o se canta "Truco" y no se quiere), entonces no se deben mostrar las cartas que no se hayan jugado a menos que ocurra el caso anterior.

2.2.4. Decisiones de Implementación

Se van a necesitar las siguientes variables para saber en que estado estamos dentro de Envido durante la partida:

Envido

Una variable EstadoEnvido que va a asumir los valores:

```
0, si no se canto nada
1, si se canto Envido
2, si se canto Envido Envido
3, si se canto Real Envido
4, si se canto Falta Envido
5, si ya no se puede seguir cantando (si el jugador respondio
```

```
  ''Quiero'' o '' No Quiero'')
```

Una variable que almacene la cantidad de puntos en juego si se dice Quiero (PtosQuieroEnv)

Una variable que almacene la cantidad de puntos en juego si se dice No Quiero (PtosNQuieroEnv)

Una variable que me indique si puedo redoblar la apuesta del Envido (Es decir, si tengo el Quiero, PuedoCantarEnv)

Nota: La cantidad de Puntos en juego si se dice "No Quiero" es la cantidad de cantos que se hayan efectuado y la cantidad de puntos en juego si se dice "Quiero" es sumar 2 si se canta Envido, 3 si se canta Real Envido. Se tomo esta decision ya quela cantidad de puntos en juego si se canta Envido, Envido, Real Envido no es la misma que si se canta Envido, Real Envido.

Supongamos que la variable PtosQuieroEnv no existe y que manejamos el Envido con las otras dos variables. En el primer caso, la variable PtosNQuieroEnv tendria un valor 3 y en el segundo caso 2. La variable EstadoEnvido en el primer caso, pasaria del estado 0 al 1, luego al 2 y finalmente el 3; y en el segundo, pasaria del estado 0 al 1 y finalmente al 3. Ahora, cuando computemos los puntos en juego, suponiendo que se dijo "Quiero" a partir de EstadoEnv, en los dos casos terminaria con el mismo valor!, lo cual es incorrecto. Es por esto que se opto por tener un registro de las estapas del Envido en la que se encuentra (EstadoEnv), la cantidad de puntos en juego si se sice "Quiero" (esto soluciona el problema antes mencionado), y la cantidad de puntos en juego si se dice "No Quiero" que sirve para contar la cantidad de cantos que se efectuaron.

Truco

Una variable EstadoTruco que va a asumir los siguientes valores:

```
0, si no se canto nada
1, si se canto Truco
2, si se canto Re Truco
3, si se canto Vale Cuatro
4, si ya no se puede seguir cantando (si el jugador respondio
  ''Quiero'' o ''No Quiero'')
```

Una variable que cuente los puntos del truco en caso que la respuesta sea "Quiero" (PtosQuieroTru)

Una variable que cuente los puntos del truco en caso que la respuesta sea "No Quiero" (PtosNQuieroTru)

Una variable que me indique si puedo redoblar la apuesta del Truco (Es decir, si tengo el Quiero, PuedoCantarTru)

Nota: Tanto los puntos del truco querido como los del no querido se van incrementando de a uno. La diferencia esta en que PtosQuieroTru de 0 pasa al valor 2; en cambio, PtosNQuieroTru pasa de 0 a 1.

3. El protocolo

Se define un procotolo que permite el reparto de cartas previo a una mano de truco y la posterior utilización de las mismas durante la mano. El diseño del protocolo se hizo con los objetivos de garantizar la transparencia del juego, tanto en el reparto de las cartas como durante el desarrollo del juego.

El protocolo brinda cierta seguridad de que las cartas han sido repartidas azarosamente, y permite verificar que cada jugador haya recibido las cartas que decide jugar.

Durante la especificaión del protocolo, se usará A para referirse al servidor, y B para referirse al cliente.

3.1. El reparto

3.1.1. Protocolo de reparto de cartas

El siguiente es el protocolo que da como resultado tres cartas para cada jugador elegidas de forma azaroza.

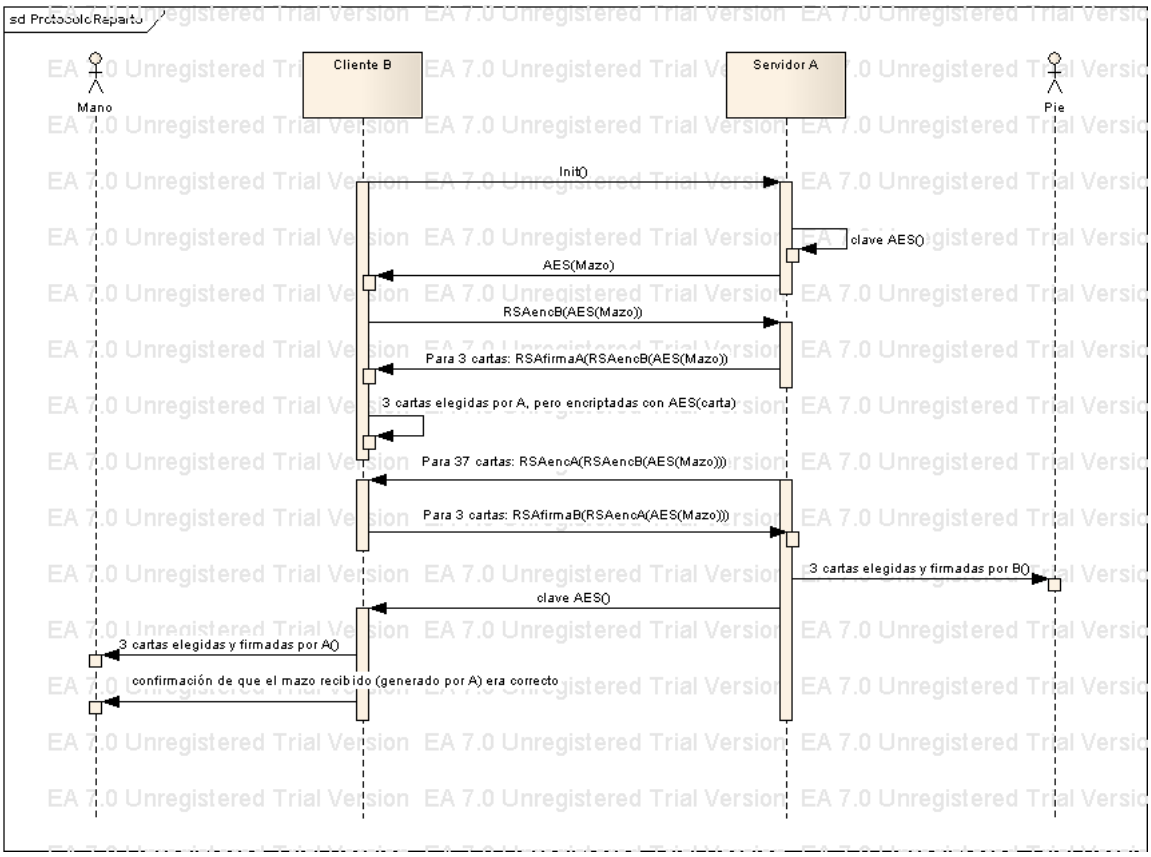
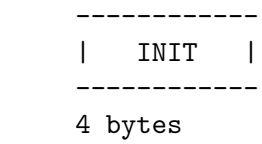


Figura 3: Protocolo de reparto

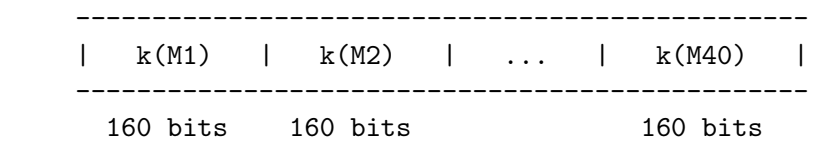
Notar que cuando se hace referencia a RSA no es estrictamente al algoritmo RSA, sino a la variante que utiliza un módulo primo descripta en Mental Poker, y que en ningún momento hay intercambio de claves de algoritmos asimétricos. La

única clave transmitida es la utilizada por AES. En este caso "firmar" equivale a encriptar y enviar a la otra parte tanto el plaintext como el encriptado. En este esquema, el firmate es el único que puede validar su firma, pero esto es suficiente si lo que se desea es validar que la carta jugada por el oponente sea una de las que uno mismo le repartió.

1. B le pide conexión a A



2. A genera una clave simétrica k (por ejemplo, con AES), encripta las 40 cartas $M_1...M_40$ con k y las envía a B (k sirve para asegurar que el mazo enviado por A en este paso es válido).

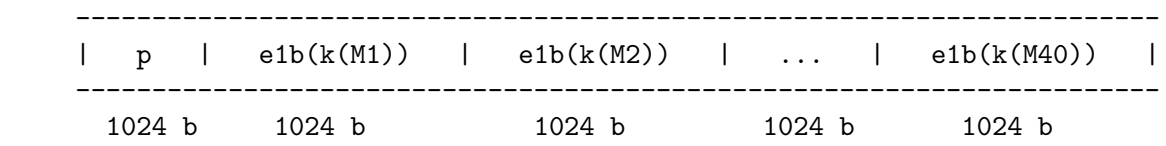


3. B genera un p primo grande y genera e_b^1, d_b^1 (utilizadas para asegurar un reparto justo) y e_b^2, d_b^2 (utilizadas para asegurar que se jueguen las cartas repartidas) tal que

$$e_b^1 * d_b^1 = 1[mod\ p-1] = e_b^2 * d_b^2$$

Envía a A el p y las cartas ya encriptadas con k encriptadas a su vez con e_b^1 (usando RSA)

$$e_b^1(k(M_i)) = k(M_i)^{e_b^1}$$



4. A usa p para generarse sus propias claves

$$e_a^1 * d_a^1 = 1[mod\ p-1] = e_a^2 * d_a^2$$

Elige al azar 3 cartas de las enviadas por B (B_1, B_2, B_3) y las firma con e_a^2. Envía cada carta como una tupla

$$< e_b^1(k(Bi)), e_a^2(e_b^1(k(Bi))) >=< k(Bi)^{e_b^1}[mod\ p], k(Bi)^(e_b^1 * e_a^2)[mod\ p] >$$

A su vez, repite el paso anterior realizado por B enviándole a este el resto de las cartas (Ri) encriptadas con su clave:

$$e_a^1(e_b^1(k(Ri))) = k(Ri)^(e_b^1 * e_a^1)[mod\ p]$$

```
-------------------------------------------------------------------------
|   e1b(k(B1))   |   e1b(k(B2))   |   e1b(k(B3))   |   e2a(e1b(k(B1)))   |
-------------------------------------------------------------------------
     1024 b           1024 b           1024 b              1024 b

-----------------------------------------
   e2a(e1b(k(B2)))   |   e2a(e1b(k(B3)))   |
-----------------------------------------
       1024 b                1024 b

-------------------------------------------------------------------------------
|    e1a(e1b(k(R1)))   |   e1a(e1b(k(R2)))   |   ...   |   e1a(e1b(k(R37)))  |
-------------------------------------------------------------------------------
        1024 b                1024 b                          1024 b
```

5. B recibe sus cartas (las tuplas) y les aplica la desencripción de e_b^1 con d_b^1:

$$< d_b^1(k(B_i)^{e_b^1}[mod\ p]), d_b^1(k(B_i)^{e_b^1 * e_a^2}[mod\ p]) >=$$
$$< k(B_i)^{e_b^1 * d_b^1}[mod\ p], k(B_i)^{e_b^1 * e_a^2 * d_b^1}[mod\ p] >=$$
$$< k(B_i), k(B_i)^{e_a^2}[mod\ p] >$$

A su vez, elige 3 cartas al azar (A_1, A_2, A_3) del resto (las R_i) y les aplica también d_b^1:

$$d_b^1(k(A_i)^{e_b^1 * e_a^1}[mod\ p]) = k(A_i)^{e_b^1 * e_a^1 * d_b^1}[mod\ p] = k(A_i)^{e_a^1}[mod\ p]$$

Para completar la mano de A, debe completar las tuplas con su firma:

$$e_b^2(k(A_i)^{e_a^1}[mod\ p]) = k(A_i)^{e_a^1 * e_b^2}[mod\ p]$$

y se las envía a A:

$$< k(A_i)^{e_a^1}[mod\ p], k(A_i)^{e_a^1 * e_b^2}[mod\ p] >$$

```
-------------------------------------------------------------------------
|   e1a(k(A1))   |   e1a(k(A2))   |   e1a(k(A3))   |   e2b(e1a(k(A1)))   |
-------------------------------------------------------------------------
     1024 b           1024 b           1024 b              1024 b
```

```
-----------------------------------------
   e2b(e1a(k(A2)))   |   e2b(e1a(k(A3)))   |
-----------------------------------------
       1024 b                1024 b
```

6. A recibe sus cartas y les aplica la desencripción de e_a^1 con d_a^1:

$$< d_a^1(k(A_i)^{e_a^1}[mod\ p]), d_a^1(k(A_i)^{e_a^1 * e_b^2}[mod\ p]) >=$$
$$< k(A_i)^{e_a^1 * d_a^1}[mod\ p], k(A_i)^{e_a^1 * e_b^2 * d_a^1}[mod\ p] >=$$
$$< k(A_i), k(A_i)^{e_b^2}[mod\ p] >$$

   A utiliza k para ver las cartas que le tocaron, su mano queda

$$< A_i, k(A_i)^{e_b^2}[mod\ p] >$$

   Por último, envia k a B

```
---------
|   k   |
---------
  128 b
```

7. B recibe k, con lo que la utiliza para ver los M_i que le mando A en el paso 2 (poseia $k(M_i)$) y verificar que le mandó un mazo valido. También desencripta su mano para ver las cartas que le tocaron:

$$< B_i, k(B_i)^{e_a^2}[mod\ p] >$$

3.1.2. Pre-inicio del juego

Este es final del inicio del juego. Se setean datos para ser usados durante el resto de la mano.

1. Ahora que ambos tienen sus manos, B se genera un par de claves RSA comunes y corrientes

$$(e_b^3, n_b), (d_b^3, n_b)$$

   y envía la pública (e_b^3, n_b) a A. Usará d_b^3 sólo para firmar sus acciones.

   A su vez, genera un paquete con el número de secuencia inicial.

```
-------------
|   sec_i   |
-------------
   32 b
```

2. A lee con la clave pública de B lo firmado por él y guarda el número de secuencia. Se genera también sus pares de claves RSA, y envia la clave publica a B

$$(e_a^3, n_a), (d_a^3, n_a)$$

A partir de este momento se considera finalizado todo el protocolo de inicio, por lo que B se queda a la espera de la primer jugada de A (siempre el servidor es mano).

3.2. Transcurso del juego

3.2.1. Envio y recepción

Durante el transcurso del juego se deberán cumplir las siguientes reglas:

- Es mano el que pidió conexion.
- Supongo que B quiere jugar B_2. Entonces debe enviar la firma que posee:

$$k(B_2)^{e_a^2}[mod\ p]$$

Cuando A lo recibe, le aplica su desencripción:

$$d_a^2(k(B_2)^{e_a^2}[mod\ p]) = k(B_2)^{e_a^2 * d_a^2}[mod\ p] = k(B_2)$$

Y con aplicar k, obtiene B_2.

- Cada vez que se canta o se juega una carta, se debe adjuntar un timestamp del momento del canto/juego. Luego, el paquete debe ser firmado (con d_a^3 / d_b^3 según corresponda) para evitar el repudio del emisor más adelante ("...no no, yo no te cante, entendiste mal...") y la reutilización del canto como prueba falsa más adelante ("...sí sí, vos cantaste truco; hace 5 horas, pero cantaste, mirá...").
- El que finalize el juego (el que se vaya al mazo, el que mate la última carta del contrincante, el que gane en el falta envido) debe además enviar un timestamp firmado, marcándolo como el final oficial del juego. El oponente, aunque esté caliente, debe confirmarle si la hora es válida.

3.2.2. Formato de las jugadas

Suponiendo que se envían los datos en limpio, el formato de paquete sería

sec	comando	[long] carta(opcional)	tanto(opcional)
32 b	8 b	(variable)	8 b

Número de secuencia

Número de secuenciamiento de paquetes. Quien comienza el juego setea el valor inicial. Se debe respetar la correlatividad, sino se aborta la conexión.

Comandos

- QUIERO ENVIDO
- NO QUIERO ENVIDO
- ENVIDO
- ENVIDO ENVIDO
- REAL ENVIDO
- FALTA ENVIDO
- QUIERO TRUCO
- NO QUIERO TRUCO
- TRUCO
- RETRUCO
- VALE CUATRO
- JUEGO CARTA
- CANTO TANTO
- SON BUENAS
- ME VOY AL MAZO
- GANE
- PERDI

4. Consideraciones

Se decidió dejar los aspectos asincrónicos del juego del truco fuera del alcance del trabajo, ya que el foco está en la parte criptográfica del mismo. Por lo tanto, se implementó una simplificación del juego en la cual los turnos de juego están bien definidos, y cada jugador debe esperar su turno para poder jugar una carta o realizar algún canto. Esta simplificación no trae grandes inconvenientes a la hora de jugar, pero simplifica notablemente la implementación del juego, ya que permite prescindir del uso de threads, evitando cualquier posible condición de carrera (por ejemplo si un jugador canta "truco" pero el otro también canta "truco" antes de recibir el canto del primero). De esta manera, el jugador que debe bajar una carta es el que tiene el turno. Si en lugar de jugar una carta, decide hacer un canto, cede su turno momentáneamente y sólo hasta que el contrincante conteste el canto. Una vez realizados los intercambios de turno requeridos por el canto realizado, el turno vuelve al jugador que debía bajar una carta. En este sentido, sirvió de inspiración el popular juego Truco para DOS, de Ariel y Enrique Arbiser

`http://www-2.dc.uba.ar/charlas/lud/truco/`

que también es orientado a turnos.

Se decidió dividir el sistema en distintos módulos, cada uno con su responsabilidad bien definida. Toda la lógica necesaria para poder jugar al Truco y manejar los turnos se encuentra en el módulo ManoTruco. El módulo red se encarga de mantener una conexión TCP entre los jugadores, mientras que el módulo Lógica de red es el que implementa el protocolo diseñado, utilizando los módulos RSA y AES según corresponda, y brindando una interfaz que permita al resto del sistema enviar y recibir jugadas de cartas y cantos. El módulo main es el que implementa la interfaz con el usuario, y usando una instancia de ManoTruco y una de Logica de red se encarga coordinar y llevar adelante la mano de truco.

En el siguiente diagrama se muestran los módulos mencionados y cómo se relacionan entre sí.

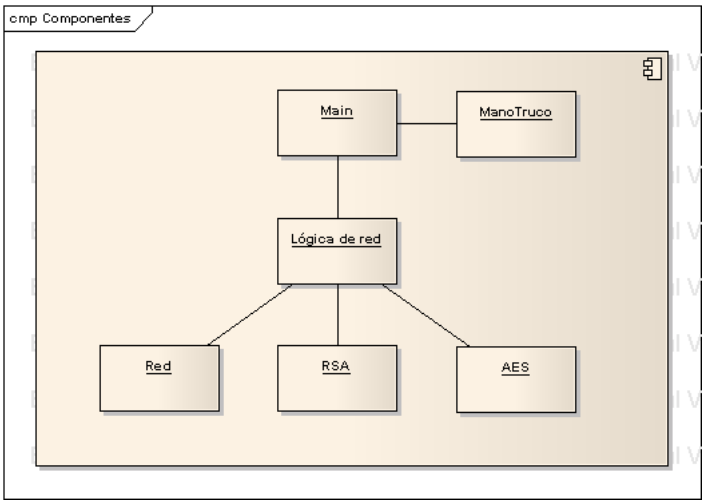


Figura 4: Componentes

Se quiso implementar la generación de primos fuertes (de la forma $2 * p + 1$, con p primo) para usar con RSA, pero para primos del tamaño que se espera usar la performance se vio afectada por un factor de aproximadamente 10, lo que teniendo en cuenta que hoy en día el uso de primos fuertes no agrega mucha más seguridad, hizo que se desistiera del uso de los mismos.

5. Manual de uso del software implementado

Al ejecutar el programa, se pide que el usuario indique si se usará el software en modo cliente o en modo servidor. Luego se debera elegir interfaz de red / direccion de red y puerto (segun el modo elegido). Y jugar!

6. Bibliografía

- Adi Shamir, Ronald L. Rivest, Leonard M. Adleman. Mental Poker. David A. Klarner Ed. The Mathematical Gardner, Prindle, Weber and Smith, Boston, Massachusetts, 1981.
- `http://usuarios.arnet.com.ar/leo890/truco.htm`
- `http://www-2.dc.uba.ar/charlas/lud/truco/`