

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	??/??	@
Carbajo, Pablo	717/04	pcarbajo@dc.uba.ar
Freijo, Diego	4/05	giga.freijo@gmail.com
Venturini, Maura	??/??	@

Abstracto

En el presente trabajo se diseñó 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 Truco

Índice

1. Logica de juego	3
2. El juego del truco	4
2.1. Reglas de juego	4
2.2. Logica de juego	4
3. El protocolo	5
3.1. El reparto	5
3.1.1. Protocolo de reparto de cartas	5
3.1.2. Pre-inicio del juego	7
3.2. Transcurso del juego	8
4. Consideraciones	9

1. Logica de juego

2. El juego del truco

2.1. Reglas de juego

2.2. Logica de juego

3. El protocolo

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 azarosa.

1. B le pide conexión a A

```

-----
|  "INIT"  |
-----
4 bytes

```

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).

```

-----
|  k(M1)  |  k(M2)  |  ...  |  k(M40)  |
-----
160 bits   160 bits               160 bits

```

3. B genera un p primo grande y genera e_b^1, d_b^1 (utilizadas para asegurar una repartición justa) y e_b^2, d_b^2 (utilizadas para asegurar que se jueguen las cartas tocadas) 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)

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

```

-----
|  p      |  e1b(k(M1))  |  e1b(k(M2))  |  ...  |  e1b(k(M40))  |
-----
1024 b    1024 b          1024 b          1024 b    1024 b

```

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

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

A su vez, repite el paso anterior realizado por B enviandole a este el resto de las cartas (R_i) 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 desecripcion de e_b^1 con d_b^1 :

$$\begin{aligned} &\langle d_b^1(k(Bi)^{e_b^1} [mod\ p]), d_b^1(k(Bi)^{e_b^1 * e_a^2} [mod\ p]) \rangle = \\ &\langle k(Bi)^{e_b^1 * d_b^1} [mod\ p], k(Bi)^{e_b^1 * e_a^2 * d_b^1} [mod\ p] \rangle = \\ &\langle k(Bi), k(Bi)^{e_a^2} [mod\ p] \rangle \end{aligned}$$

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

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

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 descriptpción de e_a^1 con d_a^1 :

$$\begin{aligned}
 &< d_a^1(k(A_i)^{e_a^1} \bmod p), d_a^1(k(A_i)^{e_a^1 * e_b^2} \bmod p) > = \\
 &< k(A_i)^{e_a^1 * d_a^1} \bmod p, k(A_i)^{e_a^1 * e_b^2 * d_a^1} \bmod p > = \\
 &< k(A_i), k(A_i)^{e_b^2} \bmod p >
 \end{aligned}$$

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

$$< A_i, k(A_i)^{e_b^2} \bmod p >$$

Por ultimo, 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 descripta su mano para ver las cartas que le tocaron:

$$< B_i, k(B_i)^{e_a^2} \bmod p >$$

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 envia la publica (e_b^3, n_b) a A. Usará d_b^3 sólo para firmar sus acciones.

A su vez, genera un paquete con el timestamp inicial decretando esta como la hora de inicio de juego. Lo envía firmado con d_b^3 .

4. Consideraciones