UNIVERSIDAD DE LA LAGUNA
Departamento de Estadística,
Investigación Operativa y Computación.

Pino Caballero Gil

PRÁCTICA: ALGORITMO DE FIAT-SHAMIR

Objetivo: Implementar la demostración de conocimiento nulo de Fiat-Shamir.
Desarrollo:

Inicialización			Escoger dos números primos secretos p,q y publicar N=p*q
Identificación secreta de A			Escoger un número secreto s tal que 0<s<N, y es primo con N
Identificación pública de A			Publicar $v \equiv s^2 \pmod N$
i Iteraciones	**Compromiso** secreto de A		Escoger un número secreto x tal que 0<x<N
	Testigo: A envía a B		Enviar $a \equiv x^2 \pmod N$
	Reto: B envía a A		Enviar un bit e, elegido al azar
	Respuesta: A envía a B	Si e=0	Enviar $y \equiv x \pmod N$
		Si e=1	Enviar $y \equiv xs \pmod N$
	Verificación: B comprueba la información recibida	Si e=0	Comprobar que $y^2 \equiv a \pmod N$
		Si e=1	Comprobar que $y^2 \equiv a * v \pmod N$

Ejemplo 1:

1. Entrada:
   a. p=7, q=5
   b. s=3
   c. i=2 (número de iteraciones)
   d. 1ª iteración: x=16, e=0
   e. 2ª iteración: x=2, e=1
2. Salida:
   a. N=35
   b. v= 9
   c. 1ª iteración: a= 11, comprobar que $16^2 \equiv 11 \pmod{35}$ y dar por válida la iteración
   d. 2ª iteración: a= 4, y = 6, comprobar que $6^2 \equiv 4*9 \pmod{35}$ y dar por válida la iteración

Ejemplo 2:

1. Entrada:
   a. p = 683, q = 811
   b. s=43215
   c. i=1 (número de iteraciones)
   d. 1ª iteración: x=16785, e=1
2. Salida:
   a. N=553913
   b. v= 295502
   c. 1ª iteración: a= 348421, y = 291658, comprobar que $291658^2 \equiv 348421*295502 \pmod{553913}$ y dar por válida la iteración