Criptografía: Aspectos Teóricos y Prácticos — Práctico 2

1. Sea p un primo, y sea $g \in \mathbb{F}_p^*$ una raíz primitiva.

   a) Sean $x, y \in \mathbb{Z}$, y sea $a \in \mathbb{F}_p^*$. Probar que si $x \equiv y \mod p-1$, entonces $a^x \equiv a^y \mod p$.

   b) I. Sea $x \in \mathbb{Z}$. Probar que $g^x \equiv 1 \mod p$ si y solo si $p-1 \mid x$.

   II. Probar que si la base es g, vale la recíproca a *a*). Es decir, probar que si $x, y \in \mathbb{Z}$ son tales que $g^x \equiv g^y \mod p$, entonces $x \equiv y \mod p-1$.

   En adelante supondremos que p es impar.

   c) Probar que $g^{\frac{p-1}{2}} \equiv -1 \mod p$.

   d) I. Probar que $a = g^x$ es un cuadrado en $\mathbb{F}_p^*$ si y solo si x es par. En tal caso, ¿quiénes son las raíces cuadradas de a?.

   II. Deducir que la mitad de los elementos de $\mathbb{F}_p^*$ son cuadrados, y la otra mitad no lo son.

   III. Deducir que -1 es un cuadrado en $\mathbb{F}_p^*$ si y solo si $p \equiv 1 \mod 4$.

   El ítem anterior nos da un método para calcular raíces cuadradas en $\mathbb{F}_p^*$, pero requiere previamente calcular $\log_g(a)$. Buscamos un método que no involucre el cálculo de logaritmos

   e) Sea $a \in \mathbb{F}_p^*$.

   I. Probar que a es un cuadrado si y solo si $a^{\frac{p-1}{2}} \equiv 1 \mod p$. Más aún, probar que $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$, donde $\left(\frac{*}{p}\right)$ es el símbolo de Legendre visto en la clase práctica.

   II. Supongamos que $p \equiv 3 \mod 4$. Probar que si a es un cuadrado, entonces $a^{\frac{p+1}{4}}$ es una raíz cuadrada de a.

   En particular, las raíces cuadradas se calculan elevando a potencias enteras (!)

2. Supongamos que Eva tiene acceso a un oráculo que sabe resolver el problema de Diffie-Hellman. Explicar cómo puede usar el oráculo para desencriptar mensajes que fueron encriptados usando el criptosistema de clave pública ElGamal.

3. Alicia y Beto fijan el primo $p = 32611$, el cual es conocido públicamente. Alicia quiere enviarle a Beto el mensaje $m = 11111$. Para esto, elige un exponente secreto aleatorio $a = 3589$, y le envía a Beto el mensaje $u = m^a \equiv 15950 \mod p$. Beto elige un exponente secreto aleatorio $b = 4037$, y le devuelve a Alicia el mensaje $v = u^b \equiv 15422 \mod p$. Alicia calcula $w = v^{15619} \equiv 27257 \mod p$, y finalmente Beto calcula $w^{31883} \mod p$ obteniendo así m, el mensaje de Alicia.

   a) Explicar por qué este este algoritmo funciona (es decir, por qué Beto finalmente obtiene m). ¿Cómo están relacionados los exponentes 3589 y 15619 que usó Alicia y los exponentes 4037 y 31883 que usó Beto?

   b) Formular una versión general de este criptosistema.

   c) ¿Qué desventaja tiene este criptosistema con respecto a ElGamal?

4. Implementar en `SAGE` el algoritmo *babystep-giantstep* de Shanks para resolver las siguientes instancias del problema del logaritmo discreto.

   a) $11^x \equiv 21 \mod 71$.

   b) $650^x \equiv 2213 \mod 3571$.