Estructuras Algebraicas
Tarea optativa

Profesor: Cristóbal Rivas
Ayudantes: Benjamín Martinez, Javier Pavez

Lunes 3 de Octubre 2022

En clases se mencionó el protocolo Diffie-Hellman, por lo que consideramos oportuno dejarles una tarea optativa (cuyo puntaje se sumará al próximo control) para que jueguen un poco con el concepto.
Siendo que el alfabeto que usamos contiene 27 letras (contando la ñ), y 27 no es primo, agregaremos un par de símbolos para que sean 29. Es decir, asignaremos $\mathrm{A} = 00, \mathrm{B} = 01, \ldots, \mathrm{Z} = 26, ? = 27, ! = 28$. Es necesario empezar con 0 para evitar ambigüedades como confundir 0101 con 11. A modo de ejemplo, con esta asignación vemos que el mensaje HOLA!COMOESTAS? se codifica a 07/15/11/00/28/02/15/12/15/04/19/20/00/19/27.
Ahora pensemos el caso de que queramos enviar este mensaje encriptado a alguien. Según el protocolo Diffie-Hellman esta persona tiene que tener una llave publica, dado que estamos en un escenario imaginario podemos elegir esta llave publica. Como ya decidimos $p = 29$, bastará decidir el generador y la llave privada de nuestro estimado incógnito. Utilizaremos $g = 8$ (en su tiempo libre puede verificar que es generador de $(\mathbb{Z}/29\mathbb{Z})^*$) y $A = 8^{10} = (8^2)^5 \equiv 6^5 = (6^2)^2 6 = (36)^2 6 \equiv 7^2 6 = 49 \cdot 6 \equiv 20 \cdot 6 = 120 \equiv 4 \pmod{29}$, es decir, la llave publica de nuestro interlocutor será 4, su llave privada es 10 y su directorio publico es (29,8,4). Nosotros utilizaremos la llave privada 2, dándonos la llave publica $B = 8^2 = 8^2 \equiv 6 \pmod{29}$ y así, nuestro directorio publico será (29,8,6). Utilizaremos la encriptación de ElGamal, es decir, tomaremos la llave publica de nuestro amigo anónimo y la elevaremos a nuestra llave privada, dándonos $s = 4^2 \equiv 16 \pmod{29}$ es decir, nuestro secreto compartido es 16. Este es compartido pues nuestro estimado anónimo puede tomar nuestra llave publica y elevarla a su llave privada, esto funciona pues estamos usando el mismo generador, o dicho de una manera mas matemática, porque $s = (g^a)^b = g^{ab} = (g^b)^a$. Ahora multiplicamos a cada dupla de dígitos de nuestro mensaje por s para encriptarlo, dándonos la cadena 25/08/02/00/13/03/08/18/08/06/14/01/00/14/26, la cual se decodifica a YICANDIRIGÑBAÑZ, y enviamos este amistoso saludo a nuestro interlocutor anónimo (también podríamos enviar la cadena de números encriptada, pero eso seria aburrido). Para desencriptar esto, nuestro indeterminado amistoso deberá calcular s, y luego calcular s^{-1}, para esto existen varios métodos, uno muy sencillo es el algoritmo de Eucides simplificado combinado con la identidad de Meziriac, dando $s^{-1} = 20$, y multiplicar esto a cada dupla de digitos de la cadena encriptada y de esta manera recibiendo nuestro saludo.

Ahora que tenemos un directorio publico nos han empezado a llegar mensajes, desencriptelos. Recuerde que nuestro directorio publico es (29,8,6) y nuestra llave privada es 2.

1. Diego (29,8,27): OAIOABPPRIZAVÑCIDWICZWC **(0.2 puntos)**
2. Remy (29,8,19): ZEALFQIUXWO **(0.2 puntos)**
3. Rick (29,8,13): VJGJZ!MVVA!RGJTMLLH **(0.4 puntos)**
4. Gyro (29,8,14): DLUUASBKKAH **(0.2 puntos)**

Ya que ahora tenemos más practica encriptando, ¿por que no intenta enviarme (por **(0.5 puntos)**) un mensaje encriptado al directorio publico (29,8,27)? Este debe ser un mensaje legible y coherente, de al menos seis caracteres y el proceso de encriptación debe estar explicado con el mismo nivel de detalle que el texto al principio de este documento