Criptografía
SERIE-1 de TEMA 5: CRIPTOGRAFÍA ASIMÉTRICA
MC María Jaquelina López Barrientos

1.- ¿En qué basan su efectividad los algoritmos asimétricos? (explique)

2.- ¿Cuál se considera la principal característica de los algoritmos asimétricos?

3.- Los logaritmos discretos son esenciales en la criptografía asimétrica y ésta basa su robustez en el problema que representa el logaritmo discreto. Explique.

4.- El uso de números primos es importante en la criptografía asimétrica y para ello es conveniente que pasen pruebas de primalidad. ¿A qué se refieren estas pruebas y porqué se considera un reto el realizarlas?

5.- En 1976 Diffie y Hellman publican el artículo "Nuevas direcciones en Criptografía" y el algoritmo que lleva sus apellidos. ¿qué proponen a través de dicho artículo y qué problema resuelven con su algoritmo?.

6.- En qué basa su seguridad el algoritmo Diffie-Hellman.

7.- Usted y yo acordaremos una clave privada mediante el algoritmo Diffie-Hellman; para ello los parámetros a utilizar son: $\alpha = 7$ y $G = \mathbb{Z}^*_{487}$, yo ya elegí mi número secreto "a" hago los cálculos necesarios y le envío a usted el número 159, ahora elija usted su número secreto "b" el cual deberá estar en el rango $900 < b < 1000$ y obtenga nuestra clave privada.

8.- Mediante el algoritmo Diffie-Hellman obtenga la clave privada que compartirán las entidades A y B si los parámetros a utilizar son: $\alpha = 11$ y $G = \mathbb{Z}^*_{859}$, y los números secretos que eligieron son: a =571 y b = 367.

9.- El algoritmo Diffie-Hellman puede sucumbir ante el ataque conocido como "man in the middle" explique a qué se refiere este tipo de ataque y desarrolle un ejemplo considerando : $\alpha = 5$ y $G = \mathbb{Z}^*_{967}$.

10.- La tarea por parejas solicitada en clase.