Tarea 2: Criptografía y Seguridad.

Fecha de entrega: lunes 29 de octubre de 2018.

1. El siguiente mensaje fue cifrado usando **RSA**.

   ```
   32020, 47286, 177452, 80202, 185908, 32020, 47286, 215221, 196322,
   17038, 176712, 0, 80202, 185908, 67201, 176712, 47286, 0,1, 28557,
      32020, 80202, 0, 47286, 28557, 32020,176712, 177452, 32020.
   ```

   Los parámetros públicos son $(N, e) = (256961, 53)$. Factoriza N utilizando el algoritmo $\rho - 1$ Pollard para encontrar un factor no trivial y así calcular $N = pq$, finalmente descifra el mensaje.

2. En este ejercicio vas usar el software de tu preferencia (se recomienda factor.exe) para atacar dos claves RSA y posteriomente encontrar la clave privada d a partir del conocimiento solamente de la clave pública n y e que se indican, factorizando ese módulo n:

   i) Ataque 1:
   $n = 29724098192314172173806795056310772584967388982187877634080 9$;
   $e = 1999$.

   ii) Ataque 2:
   $n = 643590535502220839951864707825089693683144561318250505739519366732215705459; e = 101$.

   iii) ¿De qué tamaño en bits son las claves atacadas y los valores de p y q encontrados?

   iv) ¿Cuánto tiempo has tardado en factorizar los dos módulos? Describir las características de hardware del equipo en la cual fueron ejecutados estos ataques.

   v) En cada caso, genera la clave RSA con el software de tu preferencia (se recomienda ExpoCrip) para encontrar la clave privada.

3. Aplicar el test de primalidad de Solovay-Strassen a:
   $n = 661521349351105000008725817463$ y concluir si es primo o compuesto.

4. Supongamos que $n = 4633$

   i) Para $x = 68, 69$ y 96 calcula $x^2 \ mod \ n$.

   ii) Factoriza los residuos obtenidos en el paso anterior en la base: $\{-1, 2, 3, 5\}$.

   iii) Usa las tres factorizaciones en el paso anterior para generar una congruencia de la forma $y^2 \equiv x^2 \ mod \ n$ y factoriza n.

5. Encontrar un factor no trivial de $N = 87463$ utilizando el algoritmo de la criba cuadrática.

   Hints:

- Para ver el tamaño de la base puedes usar $B = \left\lfloor \left(e^{\sqrt{ln(N)ln(ln(N))}} \right)^{\frac{\sqrt{2}}{4}} \right\rfloor$
- Para el intervalo de la criba usa $I = \left\lfloor \left(e^{\sqrt{ln(N)ln(ln(N))}} \right)^{\frac{3\sqrt{2}}{4}} \right\rfloor$, es decir $i \in [-I, I]$.

6. La persona A desea enviar el mensaje $C = (y_1, y_2) = (800, 1888)$ a la persona B. Los parámetros del sistema son $P = 3121$, $\alpha = 2$ y $\beta = 316$ resuelve el Problema del Logaritmo Discreto $log_\alpha(\beta) = x$ mediante el método de cálculo de índices y descifra el mensaje.

7. El entero $p = 458009$ es primo y $\alpha = 2$ tiene orden 57251 en $\mathbb{Z}_p^*$. Use el algoritmo Rho de Pollard para calcular el Logaritmo Discreto en $\mathbb{Z}_p^*$ de $\beta = 56851$ en base α. Tome el valor inicial $x_0 = 1$ y defina la partición $\{S_1, S_2, S_3\}$ como el ejemplo visto en clase. Encuentre el entero más pequeño i tal que $x_i = x_{2i}$ y calcule el logaritmo discreto buscado. Elija 10 iteraciones y muestre los resultados.

8. Argumentar por que la dificultad del PGLD es independiente del generador.