Criptografía: Aspectos Teóricos y Prácticos — Práctico 3

1. La clave pública RSA de Beto tiene módulo $N = 12191$ y exponente $e = 37$. Alicia le envía a Beto el texto cifrado $c = 587$. Factorizando N, ayudar a Eva a desencriptar el mensaje de Alicia.

2. Alicia utiliza el criptosistema RSA con módulo $N = 1889570071$. Le pide a Beto que encripte su mensaje dos veces, utilizando los exponentes $e_1 = 1021763679$ y $e_2 = 519424709$. Eva intercepta los mensajes cifrados $c_1 = 1244183534$ y $c_2 = 732959706$. Asumiendo que Eva conoce el módulo N y los exponentes e_1, e_2, ayudar a Eva a recuperar el mensaje de Beto (sin factorizar N).

3. Alicia utiliza el criptosistema RSA con módulo $N = 62615533$ y exponente $e = 3$. Eva consultó a un oráculo, que le dijo que el exponente de desencriptado es $d = 41743689$. Ayudar a Eva a factorizar N.

4. Formular un ataque de tipo *hombre-en-el-medio* para el criptosistema RSA, similar al ataque de tipo *hombre-en-el-medio* para el intercambio de claves Diffie-Helman visto en la clase práctica.

5. Implementar en `SAGE` el test de Miller-Rabin. Para cada uno de los siguientes n, demostrar que n es compuesto exhibiendo un testigo de Miller-Rabin, o concluir que n es probablemente primo exhibiendo 10 números que *no* sean testigos de Miller-Rabin para n.

   a) $n = 294409$.

   b) $n = 118901509$.

   c) $n = 118901521$.

   d) $n = 118901527$.

6. Sean $0 < c_1 < c_2$ números reales. Dado un número natural N, definimos

   $$P_{c_1,c_2}(N) = \text{Probabilidad de que un número natural } n \in [c_1 N, c_2 N] \text{ sea primo.}$$

   De manera análoga a como se vio en la clase práctica, hallar una función $f(N)$ (simple) tal que

   $$\lim_{N\to\infty} \frac{P_{c_1,c_2}(N)}{f(N)} = 1.$$

7. Implementar en `SAGE` el método $p-1$ de Pollard, y utilizarlo para factorizar los siguientes enteros.

   a) $n = 1739$.

   b) $n = 220459$.

   c) $n = 48356747$.