Universidad Nacional Autónoma de México

Facultad de Ciencias



Criptografía y Seguridad

# Tarea 2

*Sebastián Alamina Ramírez* - 318685496

*Carlos Alberto Desiderio Castillo* - 312183839

*Camila Alexandra Cruz Miranda* - 316084707

Trabajo presentado como parte del curso de **Criptografía y Seguridad**, impartido por el profesor **Manuel Díaz Díaz** durante el semestre 2023-1 en la Facultad de Ciencias, UNAM.

Fecha de entrega: **23:59 jueves 10 de noviembre del 2022**.

Nota: Todos los cifrados han sido codificados en unicode. En el caso de entregar código fuente deben ser con: Nombres de programadores o programador (solo nombre de personas involucradas en la programación) fecha de elaboración, comentado en cada módulo y deben expresar que son tareas.

1. Dado el siguiente número $n = 1,148,289,976,600,001$ aplique una prueba de primalidad en la cual se ocupe testigo (testigo de Fermat,testigo de Euler,testigo fuertes,...) y cite cual es.

   (a) Determina si el número $n = 1,148,289,976,600,001$ es primo con una prueba de primalidad probabilística vista en clase. Para el caso de ser primo explique como llega a tal conclusión.

   (b) En caso de ser compuesto de explícitamente la iteración y su testigo determina que es compuesto.

   Usaremos la prueba que **Miller-Rabin** para saber si $n = 1,148,289,976,600,001$ es probablemente primo o concluir con algún testigo que es compuesto.
   Tómenos primero $n-1 = 1,148,289,976,600,000$, y lo descomponemos de las forma que $n-1 = 2^s d$, con d un impar, así las potencias de los factores de $n-1$ son $\{2^6, 5^5, 13, 41, 113, 95327\}$, es decir:

$$n-1 = 1,148,289,976,600,000 = 2^6 \times 5^5 \times 13 \times 41 \times 113 \times 95327 = 2^6 \times 17942030884375$$

   Así encontramos que $r = 6$ y $d = 17942030884375$, ahora debemos ver cómo se comporta la siguiente congruencia:

$$a^{2^r d} \equiv x \bmod n \quad \text{con } r \in \{0 \leq r < 6\}$$

   Si n es primo se debe cumplir que $x = 1$, cuando $r = 0$ es decir $a^d \equiv 1 \bmod n$, o también si se da el caso $x = -1$, para alguna $r \in \{0 < r < 6\}$.
   Tomemos $a = 2$, y veamos el caso cuando $r = 0$, entonces tenemos los siguiente:

$$2^d \equiv (2^{5^5})^{13\times41\times113\times95327} \equiv 673926467533955^{13\times41\times113\times95327} \bmod n$$

   Ya que $2^{5^5} = 2^{3125} \equiv 673926467533955 \bmod 1148289976600001$, si desarrollamos más tenemos:

$$673926467533955^{13\times41\times113\times95327} = (673926467533955^{13})^{41\times113\times95327} \equiv 418721271939970^{41\times113\times95327} \bmod n$$

$$418721271939970^{41\times113\times95327} = (418721271939970^{41})^{113\times95327} \equiv 753110474208 15^{113\times95327} \bmod n$$

$$753110474208 15^{113\times95327} = (753110474208 15^{113})^{95327} \equiv 1028681460498095^{95327} \bmod n$$

$$1028681460498095^{95327} \equiv 657880504940123 \bmod n, \text{ es decir } 2^d \equiv 657880504940123 \bmod n$$

   Por lo tanto vemos que para $r = 0$, no se cumple la primera prueba, ya que $2^d \not\equiv 1 \bmod n$.
   Ahora veamos si para $r \in \{1,2,3,4,5\}$, se cumple que $a^{2^r d} \equiv -1 \bmod n$.
   Para $r = 1$, como $2^d \equiv 657880504940123 \bmod n$, entonces $2^{2^r d} = (2^d)^{2^r} \equiv 657880504940123^{2^r} \bmod n$, si sustituimos $r$, obtenemos la siguiente congruencia: $2^d)^{2^r} = (2^d)^2 \equiv 657880504940123^2 \bmod n$, por lo y tanto se tiene:

$$657880504940123^2 \equiv 1114603305721383 \bmod n$$

   Por lo tanto para $r = 1$, $(2^d)^2 = 2^{2d} \not\equiv -1 \bmod n$, tampoco pasa la prueba de primalidad.
   Con $r = 2$, de nuevo usamos lo anterior: $(2^d)^{2^2} = 2^{d2^2} \equiv 1114603305721383^2 \bmod n$, y resulta la siguiente congruencia:

$$2^{d2^2} \equiv 157814533018698 \bmod n \text{ , lo que implica que } 2^{d2^2} = 2^{d4} \not\equiv -1 \bmod n$$

   Ahora para $r = 3$, usando el mismo procedimiento $(2^d)^{4^2} = 2^{d4^2} \equiv 157814533018698^2 \bmod n$, lo que implica que:

$$2^{d4^2} \equiv 1082247192662216 \bmod n \text{ , lo que implica que } 2^{d4^2} = 2^{d16} \not\equiv -1 \bmod n$$

   Para $r = 4$, usando el mismo procedimiento $(2^d)^{16^2} = 2^{d16^2} \equiv 1082247192662216^2 \bmod n$, lo que implica que:

$$2^{d16^2} \equiv 732905763062490 \bmod n \text{ , lo que implica que } 2^{d16^2} = 2^{d256} \not\equiv -1 \bmod n$$

   Por último para $r = 5$, usando el mismo procedimiento $(2^d)^{256^2} = 2^{d256^2} \equiv 732905763062490^2 \bmod n$, lo que implica que:

$$2^{d256^2} \equiv 162838472074967 \bmod n \text{ , lo que implica que } 2^{d256^2} = 2^{d65536} \not\equiv -1 \bmod n$$

   Por lo tanto, 2 es un testigo en el cúal no se cumple ninguna prueba de primalidad, y se puede decir con seguridad que $n = 1,148,289,976,600,001$ no es un primo, por lo tanto $n$ es compuesto. ■

2. Mediante el algoritmo de **rho de Pollard** para enteros descomponga **n = 7784099**.

   (a) Dé la función semialeatoria empleada.

$$f(x) := x^2 + c \ mod \ p$$

$c$ es un número aleatorio entre $1 \ldots p-1$
$p$ es un número primo

   (b) Número de iteración en el cual fue exitoso el algoritmo y factor encontrado.

Encontramos diferentes resultados en dos ejecuciones:

```
Se encontró una colisión después de 39 intentos.
Encontramos que uno de los divisores de 7784099 es 2791
```

```
Se encontró una colisión después de 125 intentos.
Encontramos que uno de los divisores de 7784099 es 2789
```

   (c) Descifre el siguiente mensaje RSA, el cual esta en unicode:

   Llave públicaRSA=(7784099 , 7), mensaje cifrado= 6308199
   Llave públicaRSA=(7784099 , 11), mensaje cifrado= 5536286
   Llave públicaRSA=(7784099 , 13), mensaje cifrado= 159060
   Llave públicaRSA=(7784099 , 19), mensaje cifrado= 6724396
   Llave públicaRSA=(7784099 , 23), mensaje cifrado= 26176
   Llave públicaRSA=(7784099 , 29), mensaje cifrado= 1117219
   Llave públicaRSA=(7784099 , 37), mensaje cifrado= 6925326
   Llave públicaRSA=(7784099 , 43), mensaje cifrado= 7550806
   Llave públicaRSA=(7784099 , 47), mensaje cifrado= 1525454
   Llave públicaRSA=(7784099 , 49), mensaje cifrado= 4142333

El mensaje descifrado en `RSA.py` es:
"*Es rutina.*"

3. Mediante el algoritmo de la criba cuadrática, descomponga $n = 4245221$ y descifre el mensaje en RSA que se proporciona más adelante.

   (a) Dé las cotas de base e intervalo, escriba la base

   (b) Proporcione las $i$ de $q(i)$ con las cuales se obtiene la solución $x, y$ tales que $(x - y, n) = d$ donde $d$ es un factor primo de $n$. Describa de manera clara y metódica como obtiene $y$.

   **Solución 3a y 3b**:

   Considerando el código adjunto `RSA.py`, que imprime en consola el proceso íntegro del algoritmo (incluyendo la obtención de $y$), tenemos que:

$$S = \{-1, 2, 5, 7, 17, 31, 37\}$$
$$m = 2060$$
$$T = \{1, 2, 3, 8\}$$
$$x = (2061 \times 2064 \times 2099 \times 2489) \ mod \ 4245221 = 3374328$$
$$l_0 = 0 \quad l_1 = 3 \quad l_2 = 5 \quad l_3 = 1 \quad l_4 = 1 \quad l_5 = 1 \quad l_6 = 1$$
$$y = (-1^0 \times 2^3 \times 5^5 \times 7^1 \times 17^1 \times 31^1 \times 37^1) \ mod \ 4245221 \ = 3412537$$
$$d = mcd(x - y, n) = mcd(-38209, 4245221) = 2011$$

   (c) Descifrar el siguiente mensaje cifrado en RSA:

   Llave pública RSA = (4245221, 7), mensaje cifrado = 2787825.
   Llave pública RSA = (4245221, 11), mensaje cifrado = 2055284.
   Llave pública RSA = (4245221, 13), mensaje cifrado = 2061537.
   Llave pública RSA = (4245221, 17), mensaje cifrado = 4003203.
   Llave pública RSA = (4245221, 19), mensaje cifrado = 3833015.
   Llave pública RSA = (4245221, 23), mensaje cifrado = 504464.
   Llave pública RSA = (4245221, 29), mensaje cifrado = 1181333.
   Llave pública RSA = (4245221, 31), mensaje cifrado = 3063352.
   Llave pública RSA = (4245221, 37), mensaje cifrado = 1145481.
   Llave pública RSA = (4245221, 41), mensaje cifrado = 899155.
   Llave pública RSA = (4245221, 43), mensaje cifrado = 1046164.
   Llave pública RSA = (4245221, 47), mensaje cifrado = 1315170.
   Llave pública RSA = (4245221, 49), mensaje cifrado = 1878863.
   Llave pública RSA = (4245221, 53), mensaje cifrado = 2088416.
   Llave pública RSA = (4245221, 59), mensaje cifrado = 2571920.
   Llave pública RSA = (4245221, 61), mensaje cifrado = 2621019.
   Llave pública RSA = (4245221, 71), mensaje cifrado = 155090.

   **Solución**: Considerando el código adjunto `RSA.py`, y que $p = 2011$ y $q = 2111$, notamos que el mensaje descifrado es "*¡Bien descifrado!*".

   (d) Verifique si la firma digital RSA $firma = 1107437$ del mensaje $m = 1550905$ con parámetros $(4245221, 7)$ es válida.

   **Solución**: Considerando que $k = (n = 4245221, p = 2011, q = 2111, a = 1211743, b = 7)$, basta comprobar dos cosas:

   i. $y = Sig_k(x) = x^a \ mod \ n$ debe ser igual a la $firma$.
   **Comprobación**: $x^a \ mod \ n = 1550905^{1211743} \ mod \ 4245221 = 1107437 = firma$.

   ii. $Ver_k(x, y) =$ `verdadero` lo cual se da $\iff x \equiv y^b \ mod \ n$.
   **Comprobación**: $x \equiv y^b \ mod \ n \iff 1550905 \equiv 1107437^7 \ mod \ 4245221 \iff$
   $1550905 \equiv 1550905 \ mod \ 4245221$.

   Por lo tanto, la firma digital RSA dada es válida. ■

4. El siguiente mensaje fue cifrado con el algoritmo de ElGamal con llave pública = $(2011, 17, 19)$, mediante el algoritmo de cálculo de índices con la base $B = \{2, 3, 5, 7, 11\}$ encuentre el índice de 19 base 17 módulo 2011.

   (a) Dé las ecuaciones ya solucionadas para cada índice.

   (b) Dé la iteración en la cual se obtiene el índice de 19 base 17 módulo 2011.

   **Solución 4a y 4b**:

   Considerando el código adjunto `ElGamal.py`, obtenemos el siguiente sistema de ecuaciones:

$$
\begin{aligned}
1801 &= 2log_{17}(3) + 2log_{17}(5) + log_{17}(7) \ mod\ 2010 \\
1908 &= 3log_{17}(2) + log_{17}(5) + log_{17}(11) \ mod\ 2010 \\
906 &= log_{17}(3) + log_{17}(5) + log_{17}(7) \ mod\ 2010 \\
379 &= log_{17}(2) + log_{17}(5) + 2log_{17}(7) \ mod\ 2010 \\
653 &= 6log_{17}(2) + log_{17}(3) \ mod\ 2010
\end{aligned}
$$

   De donde se obtiene la siguiente solución:

$$
log_{17}(2) = 1165 \qquad log_{17}(3) = 1703 \qquad log_{17}(5) = 1202 \qquad log_{17}(7) = 11 \qquad log_{17}(11) = 1231
$$

   Y con la cual obtenemos $log_{17}(19)$ al desarrollar la siguiente relación:

$$
\begin{aligned}
&\beta \times \alpha^k \ mod\ p \\
&19 \times 17^{1014} \ mod\ 2011 = 90 = 2^1 \times 3^2 \times 5^1 \\
\implies &log_{17}(19) = (log_{17}(2) + 2log_{17}(3) + log_{17}(5) - 1014) \ mod\ 2010 = 739
\end{aligned}
$$

   Así, la llave privada es $a = 739$.

   (c) Descifre el mensaje: (891, 260), (1070, 1838), (91, 934), (1547, 1835), (156, 761), (641, 1542), (842, 1820), (237, 1757), (7, 1215), (119, 1898).

   **Solución**: Considerando el código adjunto `ElGamal.py`, que obtiene la llave privada por fuerza bruta (aunque ya **no** es realmente necesario hacerlo de esta manera, pues el cálculo de índices nos da la llave privada), notamos que el mensaje descifrado es "*¡Muy Bien!*".

   (d) Verifique la siguiente firma digital ElGamal $s_k(33, 7) = (\gamma = 156, \delta = 477)$, con llave pública = $(2011, 17, 19)$; ¿es válida la firma?

   **Solución**: Considerando que $k = (p = 2011, \alpha = 17, a = 739, \beta = 19)$, basta comprobar tres cosas:

   i. $\gamma = \alpha^k \ mod\ p$.
   **Comprobación**: $156 = 17^7 \ mod\ 2011 \iff 156 = 410338673 \ mod\ 2011 \iff 156 = 156$.

   ii. $\delta = (x - a\gamma)k^{-1} \ mod\ (p-1)$.
   **Comprobación**: $477 = (33 - 739 \times 156)7^{-1} \ mod\ (2011 - 1) \iff 477 = (33 - 115284)1723 \ mod\ 2010 \iff 477 = -115251 \times 1723 \ mod\ 2010 \iff 477 = -198577473 \ mod\ 2010 \iff 477 = 477$.

   iii. $Ver_k(x, (\gamma, \delta))$ = `verdadero` lo cual se da $\iff \beta^\gamma \gamma^\delta \equiv \alpha^x \ mod\ p$.
   **Comprobación**: $\beta^\gamma \gamma^\delta \equiv \alpha^x \ mod\ p \iff 19^{156}156^{477} \equiv 17^{33} \ mod\ 2011 \iff 100 \times 1753 \equiv 343 \ mod\ 2011 \iff 175300 \equiv 343 \ mod\ 2011 \equiv 343 \equiv 343 \ mod\ 2011$.

   Por lo tanto, la firma digital ElGamal dada es válida. ■