Criptografía y Cifrado de Información 2021

Lab 07

23.septiembre.2021

En este laboratorio implementaremos funciones para calcular el máximo divisor común de dos enteros, los coeficientes en la propiedad de Bezout, inversos módulo n, y generación de primos usando el Test de Fermat.

1. Implementar el algoritmo de Euclides para calcular el máximo común divisor de los siguientes números:

   - $a = 1036$, $b = 240$;
   - $a = 22896$, $b = 192$;
   - $a = 689161$, $b = 378851$.

2. Implementar el algoritmo de Euclides extendido para calcular los coeficientes x y y que producen el máximo divisor común $(a, b) = ax + by$ para los siguientes números:

   - $a = 1036$, $b = 240$;
   - $a = 8753$, $b = 3354$;
   - $a = 2021$, $b = 43$.

3. Hallar, cuando sea posible, el inverso de a módulo n, para los siguientes números:

   - $a = 47$, $n = 2020$;
   - $a = 31$, $b = 1234$;
   - $a = 65$, $b = 17316$.

4. Implemente el Test de primalidad de Fermat (utilice $k = 5$ repeticiones del test).
   (Agregar el código de la función que ejecuta el test, sólo de la función, en su tarea impresa. Esta función no debería ser mayor a 15 líneas de código.

   Luego, evalúe en su test si los siguientes números son primos o no:

   $$1317, 2709, 3257, 3911, 4279, 5497, 6311, 7223, 8431, 9203.$$

   Compare con una tabla de primos para indicar si su test da la respuesta correcta (aquí la respuesta correcta se entiende que en el caso de n ser primo, el test responde que n es probablemente primo).
   Una tabla de primos puede encontrarse en `https://primes.utm.edu/lists/small/10000.txt`.

   (Sugerencia: para que el cálculo de las potencias sea eficiente, puede implementar el método de potenciación binaria).

5. Usando el Test de primalidad de Fermat, construya un generador de primos aleatorios. Para ello, el usuario debe ingresar la longitud de los primos a generar (por ejemplo n el número de dígitos), y el número k de primos a generar.

   Utilice su algoritmo para generar 5 primos aleatorios de 10 dígitos.
