Estudio del tiempo de encriptación RSA según la complejidad de las llaves generadas



Ilustración 1,, Breaking RSA encryption with math, Generada por Copilot Designer

Asignatura: Matemáticas: Análisis y Enfoques NS

Número de páginas:

Índice

[1. Introducción 3](#_Toc161904514)

[1.1 Elección del tema 3](#_Toc161904515)

[1.2 Contexto y la importancia de RSA 3](#_Toc161904516)

[1.3. Propuesta de investigación 3](#_Toc161904517)

[2. Marco teórico 4](#_Toc161904518)

[2.1. Algoritmo de cifrado RSA 4](#_Toc161904519)

[2.1.2. Funcionamiento de RSA: 4](#_Toc161904520)

[2.3. Teoría de Números 4](#_Toc161904521)

[2.4. Prueba de Miller–Rabin de Primitividad 4](#_Toc161904522)

[2.4.1 Probables primos fuertes 5](#_Toc161904523)

[2.4.5 Elección de bases 5](#_Toc161904524)

[3. Diseño de programa de encriptación 6](#_Toc161904525)

[4. Resultados 6](#_Toc161904526)

[5. Nube de puntos 7](#_Toc161904527)

[6. Determinación de la precisión de las líneas de tendencia 10](#_Toc161904528)

[7. Predicciones del tiempo de ejecución 12](#_Toc161904529)

[Anexos 13](#_Toc161904530)

[Bibliografía 15](#_Toc161904531)

# 1. Introducción

## 1.1 Elección del tema

Durante mucho tiempo me he interesado en el funcionamiento de los ordenadores, especialmente en cómo se comunican y comparten información, esto me llevo a sumergirme en el campo de la ciberseguridad, donde descubrí el protocolo SSH (Secure Shell), que funciona mediante la generación de dos laves que se usan para “*abrir*” el mensaje, estas dos llaves se generan gracias al algoritmo RSA, que se basa en la complejidad de factorizar números computacionalmente.

## 1.2 Contexto y la importancia de RSA

El algoritmo RSA, nombrado así por sus creadores, Ron Rivest, Adi Shamir y Leonard Adleman, es uno de los algoritmos de cifrado asimétrico más utilizados en el mundo. Fue inventado en 1977 y revolucionó el campo de la criptografía al proporcionar un método seguro con el que enviar información por internet.

La importancia del algoritmo RSA radica en su capacidad para proporcionar un sistema de clave pública y privada que permite a los usuarios cifrar y descifrar datos de manera segura sin necesidad de compartir una clave secreta. Esto es fundamental para la seguridad en internet y en sistemas informáticos, y es por lo que hoy en día se ha convertido en el estándar de encriptación en todo el mundo.

## 1.3. Propuesta de investigación

El propósito de este estudio es investigar cómo la complejidad de las claves utilizadas en el proceso de encriptación RSA impacta en el tiempo computacional necesario para llevar a cabo este proceso. La encriptación RSA, basada en la factorización de números primos, es ampliamente utilizada en la seguridad informática y la comunicación digital debido a su robustez y eficacia.

Objetivos de la investigación:

1. Analizar la relación entre la longitud de las claves RSA y el tiempo de computación: Se busca comprender cómo aumentar la longitud de las claves RSA afecta el tiempo necesario para realizar la encriptación y desencriptación de datos.
2. Validar los resultados con datos experimentales: Se realizarán pruebas utilizando programas diseñados para encriptar datos con claves RSA de diferentes longitudes, con el fin de validar y respaldar los resultados teóricos obtenidos mediante modelización matemática.

# 2. Marco teórico

## 2.1. Algoritmo de cifrado RSA

Basado en la complejidad de la factorización de números primos, RSA se ha convertido en un pilar fundamental para garantizar la confidencialidad en las comunicaciones electrónicas.

## 2.1.2. Funcionamiento de RSA:

1. Generación de Claves:
   1. Eliges dos números primos distintos grandes, y .
   2. Calculas el módulo de ;
   3. Calculas la función totiente de Euler: .
   4. Seleccionas un exponente público , que suele ser un número primo pequeño, como o . debe ser mayor que 1 y menor que .
   5. Calculas el exponente privado , que es el inverso multiplicativo modular del módulo . En otras palabras, .
2. Cifrado:
   1. Conviertes el mensaje en texto plano en una representación numérica , mediante la codificación ASCII, donde es un entero tal que .
   2. Utilizas la clave pública del destinatario para cifrar el mensaje.
   3. Calculas el texto cifrado (mod n).
3. Descifrado:
   1. El destinatario utiliza su clave privada para descifrar el texto cifrado .
   2. El destinatario calcula el mensaje original , y convierte el código ASCII en texto.

## 2.3. Teoría de Números

**[edit. notes] Fuente: chap2 page 63, Handbook of applied criptography**

El algoritmo RSA se basa en la teoría de números, específicamente en la dificultad de factorizar el producto de dos números primos grandes. La factorización es un problema computacionalmente costoso y, hasta la fecha, no existe un algoritmo eficiente conocido que pueda factorizar grandes números en tiempo polinómico.

## 2.4. Prueba de Miller–Rabin de Primitividad

**[edit. notes] Pequeño Teorema de Fermat, Fuente:** [**Pequeño teorema de Fermat - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/Peque%C3%B1o_teorema_de_Fermat)

**[edit. notes] Primos fuertes, Fuente:** [**Número primo fuerte - Wikipedia, la enciclopedia libre**](https://es.wikipedia.org/wiki/N%C3%BAmero_primo_fuerte)

**[edit. notes] What are strong primes and are they necessary for the RSA system?:** [**link**](https://web.archive.org/web/20130425010834/http:/www.rsa.com/rsalabs/node.asp?id=2217)

**[edit. notes] A Companion to User’s Guide to Cryptography and Standards:** [**Link**](https://web.archive.org/web/20060925134546/http:/www.isg.rhul.ac.uk/ugcs/Companion_v1.21.pdf)

La prueba de Miller-Rabin de Primitividad es un algoritmo utilizado para determinar si un número dado es probablemente primo. Este algoritmo se basa en los siguientes conceptos matemáticos.

### 2.4.1 Probables primos fuertes

Dado un entero impar , escribimos como , donde y son enteros positivos y **d** es impar, mientras que es par.

Sea a un número entero tal que ; Diremos que es probablemente primo fuerte[[1]](#footnote-2) para la base si se cumple alguna de las siguientes relaciones:

* 1. para algún , .

La idea detrás de la prueba de Miller-Rabin es que cuando es un primo impar, pasa la prueba debido a dos resultados:

1. Por el Pequeño Teorema de Fermat, .
2. Las únicas raíces cuadradas de módulo son y .

Si no es un probable primo fuerte para alguna base , entonces es compuesto, y se llama testigo de la propiedad de que es compuesto. Sin embargo, esta propiedad no es una caracterización exacta de los números primos. Si es compuesto, puede haber una base para la cual sea probable primo fuerte, en cuyo caso se llama un *pseudoprimo* fuerte[[2]](#footnote-3) y se lo denomina un *mentiroso* fuerte. La prueba probabilística de Miller-Rabin se basa en la comprobación para diferentes bases de que un número dado es probable primo fuerte.

### 2.4.5 Elección de bases

Afortunadamente, ningún número compuesto es un *pseudoprimo* fuerte para todas las bases al mismo tiempo. Sin embargo, no se conoce una forma sencilla de encontrar un testigo, una solución es probar todas las bases posibles, pero esto produce un algoritmo determinista ineficiente.

Otra solución es elegir una base al azar. Esto produce una rápida prueba probabilística. Que se basa en que cuando es compuesto, la mayoría de las bases son testigos, por lo que la prueba detectará como compuesto con una probabilidad razonablemente alta, mayor que 0,75.

## 3. Diseño de programa de encriptación

Para poder realizar el estudio del tiempo que se requiere para encriptar, diseñe un programa en Python, que encripta la frase “*Hello World!”*, que es la primera frase que todo programador usa para hacer su primer programa, esto permite realizar las mismas operaciones matemáticas solo variando en números de dígitos de los números primos usados para la encriptación.

Debido al enfoque matemático de este trabajo opte por no hacer el uso de bibliotecas de Python[[3]](#footnote-4) que realizan toda la encriptación de forma automática como *cryptography[[4]](#footnote-5)*, escribiendo un programa simple y altamente documentado que hace uso de “matemática pura” para realizar la encriptación y recoger las medidas de tiempo de computación; El código se puede en centrar en [GitHub](https://github.com/raf181/Trabajo-de-Campo-de-Matematicas/blob/main/Code/rsa_pure_math-(prime%20grab).py).

Debido a la complejidad e ineficiencia de generar los números primos en Python sin hacer uso de bibliotecas de encriptación, opte por desarrollar un programa en el lenguaje de programación Rust[[5]](#footnote-6) y haciendo uso de la prueba de primitividad de Miller–Rabin, esto permite generar los números primos con una longitud deseada. El código se puede encontrar en [GitHub](https://github.com/raf181/Trabajo-de-Campo-de-Matematicas/blob/main/prime-gen/src/main.rs), junto con las listas con las [listas](https://github.com/raf181/Trabajo-de-Campo-de-Matematicas/blob/main/prime-gen/src/main.rs) de primos ya generados.

## 4. Resultados

**[edit. notes] Cambiar colores y traducir los títulos**

Para simplificar la recopilación de datos decidí implementar una función en el programa de Python que guarda los tiempos directamente a un archivo CSV, que permite graficar y realizar los cálculos necesarios. Esto permite realizar una observación previa de las tendencias de los datos y permite enfocar la dirección del estudio.

Los datos originales y sin modificar junto a el Excel se pueden encontrar en [GitHub](https://github.com/raf181/Trabajo-de-Campo-de-Matematicas/blob/main/key_length_results.xlsx), publicados por mí.

## 5. Nube de puntos

|  |  |  |  |
| --- | --- | --- | --- |
| **Dígitos (nº)** | **Encriptación (s)** | **Descripción (s)** | **Total (Encriptación + Descripción) (s)** |
| 8 | 0.00000885 | 0.00000806 | 0.00001691 |
| 9 | 0.00000792 | 0.00000725 | 0.00001517 |
| 10 | 0.00000893 | 0.00000818 | 0.00001711 |
| 11 | 0.00001224 | 0.00001111 | 0.00002335 |
| 12 | 0.00001315 | 0.00001220 | 0.00002535 |
| 13 | 0.00001318 | 0.00001218 | 0.00002536 |
| 14 | 0.00001435 | 0.00001305 | 0.00002740 |
| 15 | 0.00001873 | 0.00001760 | 0.00003633 |
| 16 | 0.00001824 | 0.00001728 | 0.00003552 |
| 17 | 0.00001898 | 0.00001891 | 0.00003789 |
| 18 | 0.00002238 | 0.00002145 | 0.00004383 |
| 19 | 0.00002644 | 0.00002575 | 0.00005219 |
| 20 | 0.00002680 | 0.00002646 | 0.00005326 |
| 21 | 0.00003764 | 0.00003717 | 0.00007481 |
| 22 | 0.00004610 | 0.00004431 | 0.00009041 |
| 23 | 0.00004774 | 0.00005340 | 0.00010114 |
| 24 | 0.00004774 | 0.00005340 | 0.00010114 |

Los puntos de las tres series de datos muestran una tendencia polinómica de grado 3. Debido a que las tres series tienen la misma tendencia, polinómica, debido ha esto los siguientes pasos se aplican a todas las series de datos.

La expresión de regresión polinómica general es la siguiente:

El sumatorio de los cuadrados que nos lleva al sistema de ecuaciones es el siguiente:

A través del método de mínimos cuadrados también se pueden determinar polinomios del grado que se desee. En este caso, la recta de regresión polinómica es de grado 3. Por lo tanto, se deberá resolver ecuaciones, ya que también se debe tener en cuenta el término independiente. En nuestro caso , por lo que deberemos resolver un sistema con un total de 4 ecuaciones. El sistema de ecuaciones quedará planteado de la siguiente manera para las tres series de datos:

Donde:

* , es el número de datos.
* , es el timepo de ejecución.
* , es el número de dígitos que formal el numero primo usado para la encriptación.
* , son las incógnitas.

Para realizar, este sistema es necesario usar una tabla de frecuencias con los valores necesarios para resolver los sistemas. En este caso la tabla de frecuencias se presenta de esta manera:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tiempo Total (Encriptación + Descripción) | x = Numero de dígitos; y =Tiempo en segundos | | | | | | | | | | | |
|  | n | y | x |  |  |  |  |  |  |  |  |
|  | 1 | 0.0000169 | 8 | 64 | 512 | 4096 | 32768 | 262144 | 0.00013528 | 0.00108224 | 0.00865792 |
|  | 2 | 0.0000152 | 9 | 81 | 729 | 6561 | 59049 | 531441 | 0.00013653 | 0.00122877 | 0.01105893 |
|  | 3 | 0.0000171 | 10 | 100 | 1000 | 10000 | 100000 | 1000000 | 0.0001711 | 0.001711 | 0.01711 |
|  | 4 | 0.0000233 | 11 | 121 | 1331 | 14641 | 161051 | 1771561 | 0.00025685 | 0.00282535 | 0.03107885 |
|  | 5 | 0.0000253 | 12 | 144 | 1728 | 20736 | 248832 | 2985984 | 0.0003042 | 0.0036504 | 0.0438048 |
|  | 6 | 0.0000254 | 13 | 169 | 2197 | 28561 | 371293 | 4826809 | 0.00032968 | 0.00428584 | 0.05571592 |
|  | 7 | 0.0000274 | 14 | 196 | 2744 | 38416 | 537824 | 7529536 | 0.0003836 | 0.0053704 | 0.0751856 |
|  | 8 | 0.0000363 | 15 | 225 | 3375 | 50625 | 759375 | 11390625 | 0.00054495 | 0.00817425 | 0.12261375 |
|  | 9 | 0.0000355 | 16 | 256 | 4096 | 65536 | 1048576 | 16777216 | 0.00056832 | 0.00909312 | 0.14548992 |
|  | 10 | 0.0000379 | 17 | 289 | 4913 | 83521 | 1419857 | 24137569 | 0.00064413 | 0.01095021 | 0.18615357 |
|  | 11 | 0.0000438 | 18 | 324 | 5832 | 104976 | 1889568 | 34012224 | 0.00078894 | 0.01420092 | 0.25561656 |
|  | 12 | 0.0000522 | 19 | 361 | 6859 | 130321 | 2476099 | 47045881 | 0.00099161 | 0.01884059 | 0.35797121 |
|  | 13 | 0.0000533 | 20 | 400 | 8000 | 160000 | 3200000 | 64000000 | 0.0010652 | 0.021304 | 0.42608 |
|  | 14 | 0.0000748 | 21 | 441 | 9261 | 194481 | 4084101 | 85766121 | 0.00157101 | 0.03299121 | 0.69281541 |
|  | 15 | 0.0000904 | 22 | 484 | 10648 | 234256 | 5153632 | 113379904 | 0.00198902 | 0.04375844 | 0.96268568 |
|  | 16 | 0.0001011 | 23 | 529 | 12167 | 279841 | 6436343 | 148035889 | 0.00232622 | 0.05350306 | 1.23057038 |
|  | 17 | 0.0001011 | 24 | 576 | 13824 | 331776 | 7962624 | 191102976 | 0.00242736 | 0.05825664 | 1.39815936 |
|  | 17 | 0.00077717 | 272 | 4760 | 89216 | 1758344 | 35940992 | 754555880 | 0.014634 | 0.29122644 | 6.02076786 |

Tabla 1, Tabla con los cálculos necesarios para realizar el sistema con los datos de la serie de tiempo total. Fuente: Creación Propia

Las tablas con los datos de encriptación y desencriptación se pueden encontrar en [Anexos](#_Anexos) como tabla 2 y 3.

Por lo tanto, de las tablas obtenemos lo siguientes sistemas los siguientes sistemas:

|  |  |
| --- | --- |
| Sistema de tiempo total |  |
| Sistema de tiempo de desencriptación |  |
| Sistema de tiempo de encriptación |  |

Para resolver estas ecuaciones usare una ecuación matricial

Donde son los coeficientes y las incógnitas; Debido a las propiedades de las matrices no se pueden dividir, por lo tanto, multiplicaremos a ambos lados por la matriz inversa de A, y de esta manera en el lado izquierdo de la incógnita se queda la llamada identidad, que su valor es 1.

|  |  |
| --- | --- |
| Sistema de tiempo total |  |
| Sistema de tiempo de desencriptación |  |
| Sistema de tiempo de encriptación |  |

Que, resuelto una vez resuelto mediante Excel, resulta en:

|  |  |  |  |
| --- | --- | --- | --- |
| Resultados de las incógnitas de los sistemas | | | |
|  | Total | Desencriptación | Encriptación |
| B0 |  |  |  |
| B1 |  |  |  |
| B2 |  |  |  |
| B3 |  |  |  |

*O expresado en forma de función:*

|  |  |
| --- | --- |
| modelo de regresión de tiempo total |  |
| *modelo de regresión de tiempo de descripción* |  |
| *modelo de regresión de tiempo de encriptación* |  |

## 6. Determinación de la precisión de las líneas de tendencia

**[edit. notes]** ▷ Coeficiente de determinación (R cuadrado) ([probabilidadyestadistica.net](https://www.probabilidadyestadistica.net/coeficiente-de-determinacion-r-cuadrado/))

Para poder observar la precisión de la línea de tendencia se debe calcular el **coeficiente de determinación**, cuyo símbolo es , que mide la bondad de ajuste de un modelo de regresión. El coeficiente de determinación muestra lo bien que se ajusta un modelo de regresión a un conjunto de datos. El valor de debe estar entre 0 y 1, cuanto mas cercano a uno mas precisa es el modelo de regresión de las variables que se están estudiando.

Y se calcula mediante la siguiente formula:

Donde:

* , es el coeficiente de determinación.
* , es la varianza residual.
* es la varianza de la variable dependiente Y.
* , es el valor de la variable dependiente de la observación i.
* es el valor aproximado por el modelo de regresión para la observación i.
* , es la media de la variable dependiente de todas las observaciones.

Para resolver la ecuación necesitamos los siguientes datos:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Datos para resolver del modelo de regresión del tiempo total | | | | |
|  | x | y | Predicción de la curva = Ŷ |  |  |
|  | 8 | 1.69100E-05 | 1.57649E-05 | 2.554452E-10 | 1.311320E-12 |
|  | 9 | 1.51700E-05 | 1.75492E-05 | 1.998745E-10 | 5.660385E-12 |
|  | 10 | 1.71100E-05 | 1.92809E-05 | 2.552272E-10 | 4.712719E-12 |
|  | 11 | 2.33500E-05 | 2.10870E-05 | 4.888338E-10 | 5.121008E-12 |
|  | 12 | 2.53500E-05 | 2.30946E-05 | 5.755917E-10 | 5.086747E-12 |
|  | 13 | 2.53600E-05 | 2.54306E-05 | 5.694944E-10 | 4.987422E-15 |
|  | 14 | 2.74000E-05 | 2.82220E-05 | 6.625414E-10 | 6.757510E-13 |
|  | 15 | 3.63300E-05 | 3.15959E-05 | 1.188279E-09 | 2.241199E-11 |
|  | 16 | 3.55200E-05 | 3.56791E-05 | 1.116979E-09 | 2.531351E-14 |
|  | 17 | 3.78900E-05 | 4.05987E-05 | 1.260381E-09 | 7.337235E-12 |
|  | 18 | 4.38300E-05 | 4.64818E-05 | 1.688863E-09 | 7.031815E-12 |
|  | 19 | 5.21900E-05 | 5.34552E-05 | 2.405469E-09 | 1.600649E-12 |
|  | 20 | 5.32600E-05 | 6.16460E-05 | 2.463511E-09 | 7.032432E-11 |
|  | 21 | 7.48100E-05 | 7.11811E-05 | 4.987590E-09 | 1.316872E-11 |
|  | 22 | 9.04100E-05 | 8.21877E-05 | 7.323154E-09 | 6.760679E-11 |
|  | 23 | 1.01140E-04 | 9.47926E-05 | 9.132472E-09 | 4.028990E-11 |
|  | 24 | 1.01140E-04 | 1.09123E-04 | 8.972070E-09 | 6.372554E-11 |
|  | n=17 | 0.0007772 | 0.0007772 | 4.354578E-08 | 3.160952E-10 |

Tabla 2,Tabla con los datos necesarios para realizar los cálculos del coeficiente de correlación del modelo de regresión de tiempo de computación total. Fuente: Creación Propia

Las tablas con los datos de encriptación y desencriptación se pueden encontrar en [Anexos](#_Anexos) como tabla 3 y 4.

**[edit. notes] Cambiar notación científica de excel a real y añadir las tablas para las otras dos series añadir encabezado y fuente**

Que calculado mediante Excel resulta en:

|  |  |
| --- | --- |
| coeficiente de determinación del modelo de regresión de tiempo total |  |
| *coeficiente de determinación del modelo de regresión de tiempo de descripción* |  |
| *coeficiente de determinación del modelo de regresión de tiempo de encriptación* |  |

Esto resultados indican la alta fiabilidad de los modelos de regresión de todas las series de datos, esta exactitud nos permite realizar predicciones de los tiempos de computación con números primos mas grandes, esto nos permite analizar el tiempo esperado que tendremos que esperar al encriptar información.

## 7. Predicciones del tiempo de ejecución

Gracias a la exactitud de las rectas de regresión nos permite estimar los valores y observar su exactitud comparándolas con los valores reales y observar como el margen de error evoluciona.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Serie | x | Predicción | real | error |
| Total | 25 | 5.8656E-05 |  | 5.8656E-05 |
| 26 | 6.6154E-05 |  | 6.6154E-05 |
| 27 | 7.4401E-05 |  | 7.4401E-05 |
| 28 | 8.3435E-05 |  | 8.3435E-05 |
| 29 | 9.3296E-05 |  | 9.3296E-05 |
| 30 | 1.0402E-04 |  | 1.0402E-04 |
| Desencriptación | 25 | 6.6650E-05 |  | 6.6650E-05 |
| 26 | 7.7314E-05 |  | 7.7314E-05 |
| 27 | 8.9335E-05 |  | 8.9335E-05 |
| 28 | 1.0280E-04 |  | 1.0280E-04 |
| 29 | 1.1780E-04 |  | 1.1780E-04 |
| 30 | 1.3443E-04 |  | 1.3443E-04 |
| Encriptación | 25 | 1.2531E-04 |  | 1.2531E-04 |
| 26 | 1.4347E-04 |  | 1.4347E-04 |
| 27 | 1.6374E-04 |  | 1.6374E-04 |
| 28 | 1.8624E-04 |  | 1.8624E-04 |
| 29 | 2.1110E-04 |  | 2.1110E-04 |
| 30 | 2.3845E-04 |  | 2.3845E-04 |

**[edit. notes] Finalizar cálculos y añadir conclusión del apartado**

# 8. Análisis del crecimiento de los médelos de regresión

Para poder comprender la evolución del tiempo, es esencial comprender el crecimiento de las funciones mediante el análisis de puntos máximos para ver si hay un punto donde el tiempo de procesamiento deja de crecer.

Ya que todas las funciones de los modelos de regresión son iguales polo que el proceso es el mismo

Primero analizare el máximo, mediante derivada:

1. Se deriva de la función
   1. Con la derivada primera también calcule la pendiente para ver si siempre hay un crecimiento, dado que si es siempre positivo, crece siempre.

Y todos los modelos de regresión cumplen esto, por lo que todos los modelos presentan un crecimiento siempre.

1. Después se iguala la derivada a cero, y se resuelve para obtener x, para obtener los puntos críticos.

Y definiré los puntos críticos como .

1. Después utilice la segunda derivada para clasificar las soluciones entre puntos de inflexión o máximos y mínimos, donde:
   1. Si , entonces la función tiene un mínimo en
   2. Si , entonces la función tiene un máximo en
   3. Si , la prueba no es concluyente, por lo que se resultara a hacer un análisis gráfico, mediante GeoGebra.

Después analice de la función las asíntotas horizontales, mediante límites para determinar si las funciones presentan un límite de crecimiento. El estudio de limites no presento ningún límite de donde el tiempo de computación resulta en una línea prácticamente vertical.

Como la función solo es válida de , solo considerade los máximos de 8 a . Todas las funciones tienen un cambio de sentido en x=0, pero dado que no se pueden calcular un numero con un numero de dígitos negativos se ha obviado por completo; y dado que la dado que ninguna de las funciones presenta un máximo se puede decir que el tiempo

# Conclusion

# Anexos

* Generador de números primos (Rust): [Archivo](https://github.com/raf181/Trabajo-de-Campo-de-Matematicas/blob/main/prime-gen/src/main.rs)
* Encriptado con matemáticas puras (Python): [Archivo](https://github.com/raf181/Trabajo-de-Campo-de-Matematicas/blob/main/Code/rsa_pure_math-(prime%20grab).py)
* Excel: [archivo](https://github.com/raf181/Trabajo-de-Campo-de-Matematicas/blob/main/key_length_results.xlsx), vista previa [key\_length\_results.xlsx (live.com)](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fraw.githubusercontent.com%2Fraf181%2FTrabajo-de-Campo-de-Matematicas%2Fmain%2Fkey_length_results.xlsx&wdOrigin=BROWSELINK)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tiempo de desencriptación | x = Numero de dígitos; y =Tiempo en segundos | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | 1 | 0.0000081 | 8 | 64 | 512 | 4096 | 32768 | 262144 | 0.0000645 | 0.0005158 | 0.0041267 |
|  | 2 | 0.0000072 | 9 | 81 | 729 | 6561 | 59049 | 531441 | 0.0000652 | 0.0005872 | 0.0052852 |
|  | 3 | 0.0000082 | 10 | 100 | 1000 | 10000 | 100000 | 1000000 | 0.0000818 | 0.0008180 | 0.0081800 |
|  | 4 | 0.0000111 | 11 | 121 | 1331 | 14641 | 161051 | 1771561 | 0.0001222 | 0.0013443 | 0.0147874 |
|  | 5 | 0.0000122 | 12 | 144 | 1728 | 20736 | 248832 | 2985984 | 0.0001464 | 0.0017568 | 0.0210816 |
|  | 6 | 0.0000122 | 13 | 169 | 2197 | 28561 | 371293 | 4826809 | 0.0001583 | 0.0020584 | 0.0267595 |
|  | 7 | 0.0000131 | 14 | 196 | 2744 | 38416 | 537824 | 7529536 | 0.0001827 | 0.0025578 | 0.0358092 |
|  | 8 | 0.0000176 | 15 | 225 | 3375 | 50625 | 759375 | 11390625 | 0.0002640 | 0.0039600 | 0.0594000 |
|  | 9 | 0.0000173 | 16 | 256 | 4096 | 65536 | 1048576 | 16777216 | 0.0002765 | 0.0044237 | 0.0707789 |
|  | 10 | 0.0000189 | 17 | 289 | 4913 | 83521 | 1419857 | 24137569 | 0.0003215 | 0.0054650 | 0.0929048 |
|  | 11 | 0.0000214 | 18 | 324 | 5832 | 104976 | 1889568 | 34012224 | 0.0003861 | 0.0069498 | 0.1250964 |
|  | 12 | 0.0000257 | 19 | 361 | 6859 | 130321 | 2476099 | 47045881 | 0.0004892 | 0.0092957 | 0.1766192 |
|  | 13 | 0.0000265 | 20 | 400 | 8000 | 160000 | 3200000 | 64000000 | 0.0005292 | 0.0105840 | 0.2116800 |
|  | 14 | 0.0000372 | 21 | 441 | 9261 | 194481 | 4084101 | 85766121 | 0.0007806 | 0.0163920 | 0.3442314 |
|  | 15 | 0.0000443 | 22 | 484 | 10648 | 234256 | 5153632 | 113379904 | 0.0009748 | 0.0214460 | 0.4718129 |
|  | 16 | 0.0000534 | 23 | 529 | 12167 | 279841 | 6436343 | 148035889 | 0.0012282 | 0.0282486 | 0.6497178 |
|  | 17 | 0.0000534 | 24 | 576 | 13824 | 331776 | 7962624 | 191102976 | 0.0012816 | 0.0307584 | 0.7382016 |
|  | 17 | 0.0003878 | 272 | 4760 | 89216 | 1758344 | 35940992 | 754555880 | 0.0073529 | 0.1471617 | 3.0564727 |

Tabla 3, Tabla con los cálculos necesarios para realizar el sistema con los datos de la serie de tiempo de desencriptación. Fuente: Creación Propia

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tiempo de Encriptación | x = Numero de dígitos; y =Tiempo en segundos | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | 1 | 8.06E-06 | 8 | 64 | 512 | 4096 | 32768 | 262144 | 7.08E-05 | 0.000566 | 0.004531 |
|  | 2 | 7.25E-06 | 9 | 81 | 729 | 6561 | 59049 | 531441 | 7.13E-05 | 0.000642 | 0.005774 |
|  | 3 | 8.18E-06 | 10 | 100 | 1000 | 10000 | 100000 | 1000000 | 8.93E-05 | 0.000893 | 0.00893 |
|  | 4 | 1.11E-05 | 11 | 121 | 1331 | 14641 | 161051 | 1771561 | 0.000135 | 0.001481 | 0.016291 |
|  | 5 | 1.22E-05 | 12 | 144 | 1728 | 20736 | 248832 | 2985984 | 0.000158 | 0.001894 | 0.022723 |
|  | 6 | 1.22E-05 | 13 | 169 | 2197 | 28561 | 371293 | 4826809 | 0.000171 | 0.002227 | 0.028956 |
|  | 7 | 1.31E-05 | 14 | 196 | 2744 | 38416 | 537824 | 7529536 | 0.000201 | 0.002813 | 0.039376 |
|  | 8 | 1.76E-05 | 15 | 225 | 3375 | 50625 | 759375 | 11390625 | 0.000281 | 0.004214 | 0.063214 |
|  | 9 | 1.73E-05 | 16 | 256 | 4096 | 65536 | 1048576 | 16777216 | 0.000292 | 0.004669 | 0.074711 |
|  | 10 | 1.89E-05 | 17 | 289 | 4913 | 83521 | 1419857 | 24137569 | 0.000323 | 0.005485 | 0.093249 |
|  | 11 | 2.14E-05 | 18 | 324 | 5832 | 104976 | 1889568 | 34012224 | 0.000403 | 0.007251 | 0.13052 |
|  | 12 | 2.57E-05 | 19 | 361 | 6859 | 130321 | 2476099 | 47045881 | 0.000502 | 0.009545 | 0.181352 |
|  | 13 | 2.65E-05 | 20 | 400 | 8000 | 160000 | 3200000 | 64000000 | 0.000536 | 0.01072 | 0.2144 |
|  | 14 | 3.72E-05 | 21 | 441 | 9261 | 194481 | 4084101 | 85766121 | 0.00079 | 0.016599 | 0.348584 |
|  | 15 | 4.43E-05 | 22 | 484 | 10648 | 234256 | 5153632 | 113379904 | 0.001014 | 0.022312 | 0.490873 |
|  | 16 | 5.34E-05 | 23 | 529 | 12167 | 279841 | 6436343 | 148035889 | 0.001098 | 0.025254 | 0.580853 |
|  | 17 | 5.34E-05 | 24 | 576 | 13824 | 331776 | 7962624 | 191102976 | 0.001146 | 0.027498 | 0.659958 |
|  | 17 | 0.000389 | 272 | 4760 | 89216 | 1758344 | 35940992 | 754555880 | 0.007281 | 0.144065 | 2.964295 |

Tabla 4, Tabla con los cálculos necesarios para realizar el sistema con los datos de la serie de tiempo de encriptación. Fuente: Creación Propia

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Datos para resolver del modelo de regresión del tiempo de desencriptación | | | | |
|  | x | y | Predicción de la curva = Ŷ |  |  |
|  | 8 | 8.06000E-06 | 7.25112E-06 | 5.826976E-11 | 6.542790E-13 |
|  | 9 | 7.25000E-06 | 8.38378E-06 | 4.565483E-11 | 1.285468E-12 |
|  | 10 | 8.18000E-06 | 9.36913E-06 | 5.819973E-11 | 1.414019E-12 |
|  | 11 | 1.11100E-05 | 1.02956E-05 | 1.103419E-10 | 6.631740E-13 |
|  | 12 | 1.22000E-05 | 1.12518E-05 | 1.331284E-10 | 8.990033E-13 |
|  | 13 | 1.21800E-05 | 1.23262E-05 | 1.312154E-10 | 2.137885E-14 |
|  | 14 | 1.30500E-05 | 1.36073E-05 | 1.500520E-10 | 3.105416E-13 |
|  | 15 | 1.76000E-05 | 1.51835E-05 | 2.791190E-10 | 5.839554E-12 |
|  | 16 | 1.72800E-05 | 1.71434E-05 | 2.647639E-10 | 1.866649E-14 |
|  | 17 | 1.89100E-05 | 1.95754E-05 | 3.153645E-10 | 4.428050E-13 |
|  | 18 | 2.14500E-05 | 2.25682E-05 | 4.049134E-10 | 1.250294E-12 |
|  | 19 | 2.57500E-05 | 2.62101E-05 | 5.860385E-10 | 2.116570E-13 |
|  | 20 | 2.64600E-05 | 3.05896E-05 | 6.081457E-10 | 1.705379E-11 |
|  | 21 | 3.71700E-05 | 3.57953E-05 | 1.229512E-09 | 1.889667E-12 |
|  | 22 | 4.43100E-05 | 4.19157E-05 | 1.750951E-09 | 5.732503E-12 |
|  | 23 | 5.34000E-05 | 4.90393E-05 | 2.551799E-09 | 1.901586E-11 |
|  | 24 | 5.34000E-05 | 5.72545E-05 | 2.503210E-09 | 1.485709E-11 |
|  | n=17 | 0.0003878 | 0.0003878 | 1.118068E-08 | 7.155974E-11 |

Tabla 5,Tabla con los datos necesarios para realizar los cálculos del coeficiente de correlación del modelo de regresión de tiempo de descripción. Fuente: Creación Propia

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Datos para resolver del modelo de regresión del tiempo de encriptación | | | | |
|  | x | y | Predicción de la curva = Ŷ |  |  |
|  | 8 | 8.85E-06 | 8.5137E-06 | 6.970904E-11 | 1.130978E-13 |
|  | 9 | 7.92E-06 | 9.1653E-06 | 5.447715E-11 | 1.550813E-12 |
|  | 10 | 8.93E-06 | 9.9117E-06 | 6.967173E-11 | 9.637153E-13 |
|  | 11 | 1.224E-05 | 1.0791E-05 | 1.346811E-10 | 2.098684E-12 |
|  | 12 | 1.315E-05 | 1.1843E-05 | 1.550865E-10 | 1.709056E-12 |
|  | 13 | 1.318E-05 | 1.3104E-05 | 1.539872E-10 | 5.728815E-15 |
|  | 14 | 1.435E-05 | 1.4615E-05 | 1.819886E-10 | 7.005083E-14 |
|  | 15 | 1.873E-05 | 1.6412E-05 | 3.155800E-10 | 5.371884E-12 |
|  | 16 | 1.824E-05 | 1.8536E-05 | 2.941112E-10 | 8.737704E-14 |
|  | 17 | 1.898E-05 | 2.1023E-05 | 3.148263E-10 | 4.174473E-12 |
|  | 18 | 2.238E-05 | 2.3913E-05 | 4.398805E-10 | 2.351418E-12 |
|  | 19 | 2.644E-05 | 2.7245E-05 | 6.168943E-10 | 6.479185E-13 |
|  | 20 | 2.68E-05 | 3.1056E-05 | 6.236591E-10 | 1.811481E-11 |
|  | 21 | 3.764E-05 | 3.5386E-05 | 1.264407E-09 | 5.082419E-12 |
|  | 22 | 4.61E-05 | 4.0272E-05 | 1.912407E-09 | 3.396893E-11 |
|  | 23 | 4.774E-05 | 4.5753E-05 | 2.029380E-09 | 3.947963E-12 |
|  | 24 | 4.774E-05 | 5.1868E-05 | 1.997101E-09 | 1.704112E-11 |
|  | n=17 | 0.0003894 | 0.0003894 | 1.062785E-08 | 9.729947E-11 |

Tabla 6,Tabla con los datos necesarios para realizar los cálculos del coeficiente de correlación del modelo de regresión de tiempo de encriptación. Fuente: Creación Propia

# Bibliografía

1. Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. <https://cacr.uwaterloo.ca/hac/>
   1. [chap2.pdf (uwaterloo.ca)](https://cacr.uwaterloo.ca/hac/about/chap2.pdf)
   2. [chap4.pdf (uwaterloo.ca)](https://cacr.uwaterloo.ca/hac/about/chap4.pdf)
   3. [chap8.pdf (uwaterloo.ca)](https://cacr.uwaterloo.ca/hac/about/chap8.pdf)
2. colaboradores de Wikipedia. (2023, 29 septiembre). Test de primalidad de Miller-Rabin. Wikipedia, la Enciclopedia Libre. <https://es.wikipedia.org/wiki/Test_de_primalidad_de_Miller-Rabin>
3. Estadística, P. Y. (2023, March 1). Mínimos cuadrados. Probabilidad Y Estadística. <https://www.probabilidadyestadistica.net/minimos-cuadrados/>
4. ▷El Método de mínimos cuadrados: definición y ejemplos☑ - Mi Profe. (2022, February 22). Mi Profe. <https://miprofe.com/minimos-cuadrados/>

1. En matemáticas, un número primo fuerte es un número primo con ciertas propiedades. La definición de primo fuerte es diferente en criptografía y en la teoría de números. Fuentes: [Link](https://es.wikipedia.org/wiki/N%C3%BAmero_primo_fuerte) [↑](#footnote-ref-2)
2. Los pseudoprimos son aquellos números que, sin ser primos, verifican el test de base . Fuente: [link](https://es.wikipedia.org/wiki/N%C3%BAmero_pseudoprimo) [↑](#footnote-ref-3)
3. Welcome to Python.org. (2024, March 13). Python.org. [Link](https://www.python.org/) [↑](#footnote-ref-4)
4. cryptography. (2024, febrero 24). PyPI. [Link](https://pypi.org/project/cryptography/) [↑](#footnote-ref-5)
5. Rust, el lenguaje de programación. (n.d.). [Link](https://www.rust-lang.org/es) [↑](#footnote-ref-6)