INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

MATEMÁTICAS COMPUTACIONALES

PROYECTO FINAL

---

# Fundamentos Matemáticos del Criptosistema de Llave Pública RSA

---

*Autores*

Alejandro Chavez Campos
Luis Enrique Neri Pérez
Rudolf Josef Fanchini Reyes
Sonia Leilani Ramos Nuñez

Julio 2019

# 1 Fundamentos Matemáticos del RSA

## 1.1 Generación de Primos

Este es el resultado de multiplicar dos números y es fácil determinar si un número es primo o no.

Se puede generar un número random por medio, de una lista de números aleatorios y a partir de esa lista, se recorre hasta encontrar un número primo. El número de candidatos a probar es de orden $ln(x)$, donde $x$ es un número del tamaño deseado.

## 1.2 Multiplicar es fácil

Las maneras de encontrar la multiplicación de dos números grandes es fácil, usando el método de multiplicar un número, por cada dígito y posteriormente sumar cada uno de los distintos resultados.

## 1.3 Factorizar es difícil

Un determinado número, es complicado obtener los factores primos. El método más rápido para encontrar es mucho más eficiente que probar con todos los factores posibles una vez, y sus $\sqrt{(n)}$ pasos, y en términos de recursos empleados, puede ser de un año, y costo generado US $10 millones, y número de tamaño 2048-bit puede un billón veces más complicado.

Métodos recientes son todavía más rápidos no serán descubiertos en próximos años.

## 1.4 Encriptación

La encriptación de hace la siguiente manera:

$$c = Encrypt(m) = m^e \mod (n)$$

Donde la entrada $m$ es el mensaje, la salida $c$ es el texto resutante. En práctica, el mensaje $m$ es comúnmenrte, una aproximación de la llave a compartir. El mensaje actual es encriptado con la llave pública usando un algoritmo tradicional de encriptación.

La decriptación es la siguiente operación:

$$m = Decrypt(c) = c^d \mod (n)$$

La relación entre los exponente $e$ y $d$, aseguran que la encriptación y desencriptación son operaciones inversas, y así de esta forma, obtener el mensaje original $m$ después de la operación. Sin la llave privada, es decir, obtener los factores primos, sería muy difícil obtener $m$ usando $c$. En otro aspecto, $n$ y $e$ pueden ser públicos sin comprometer la seguridad.

La firma digital puede ser aplicando la decriptación de la siguiente forma:

$$s = Sign(m) = m^d \mod (n)$$

Y esta firma puede ser verificada, aplicando la operación de encriptación y comparando el resultado con la recuperación del mensaje.

$$m = Verify(s) = s^e \mod (n)$$

# 2 Vulnerabilidades del RSA

- Si se está cifrando con un exponente de cifrado bajo y valores pequeños para m, entonces: $m^e <$ mod $n$. Esto significa que puede descifrar fácilmente tomando la raíz del texto cifrado sobre los enteros.
- Si los números primos utilizados para la generación de claves no son realmente aleatorios, algunas de las claves privadas podrían determinarse fácilmente a través de la factorización prima en un tiempo práctico utilizando la clave pública. Un ejemplo de una violación que aprovechó esta vulnerabilidad fue la vulnerabilidad de ROCA que afectó a los productos fabricados por Infineon TPM.
- En redes, en la aplicación TSL de RSA, un atacante puede ingresar a un servidor vulnerable y consultar textos cifrados modificados para recibir verdadero o falso de acuerdo con la validez del texto cifrado. Una vez que el atacante encuentre un texto cifrado válido, intentará descifrarlo. Esta vulnerabilidad se conoce desde hace mucho tiempo y aún se explota. Es conocida como la vulnerabilidad de Bleichenbacher.

- Es posible utilizar el método de fracción continua para exponer claves privadas de pequeño tamaño.
- También en mensajes suficientemente pequeños, ya que el algoritmo es bien conocido, uno puede simplemente intentar cifrar todos los mensajes de tal tamaño hasta que se encuentre un texto cifrado que coincida.
- De manera similar, si el atacante desea conocer un exponente privado y conoce un texto en claro y un texto cifrado, puede intentar cada clave posible en los textos cifrados hasta que adquiera el texto en claro conocido.
- Es posible atacar al interceptar la clave pública y cambiar sus valores. Una vez que el usuario final recibe la clave defectuosa, le pedirá al usuario inicial que envíe el mensaje nuevamente, esta vez será con la clave correcta. El atacante ahora tiene el texto cifrado defectuoso y el correcto más los exponentes y el módulo público.
- Y, por supuesto, la falta de fiabilidad humana siempre es un factor, las claves privadas y los números base para la generación siempre pueden filtrarse.

# 3 Breve descripción de las reivindicaciones de la patente US-4405829

Esta invención se refiere a comunicaciones, más particularmente a sistemas y métodos de comunicaciones criptográficas. Es importante que la sustancia de las comunicaciones particulares pase de un remitente a un destinatario deseado sin partes intermedias, es decir, interpretar el mensaje transferido.

Una serie de técnicas de codificación y decodificación criptográficas están disponibles para proporcionar un cierto grado de privacidad y autenticación; En general, el sistema criptográfico está adaptado para ser transferido a mensajes entre ubicaciones remotas. Este sistema y método criptográfico y de comunicación incluye un canal de comunicaciones acoplado a al menos un terminal con un dispositivo de codificación y otro con un dispositivo de decodificación; un mensaje que se transfiere se cifra en el terminal de codificación cuando primero se codifica el mensaje como un número $M$ en un conjunto predeterminado, y luego se aumenta ese

número a una primera potencia predeterminada y finalmente se calcula el resto, o el resto, $C$, este el residuo $C$ es el texto cifrado. El mensaje original se descifra en el terminal de decodificación de manera similar elevando el texto cifrado a una segunda potencia predeterminada. Cuando el texto cifrado exponencial se divide por el producto de los dos números primos predeterminados asociados con el recibido, es $M$ y esto corresponde al texto codificado original. A continuación, se resume lo que se explica en las reivindicaciones:

Un sistema de comunicación criptográfica comprende muchos componentes.

- Canal de comunicaciones.
- Un sistema acoplado a un canal específico, este canal está adaptado para transformar la señal de una palabra conocida como M en un texto cifrado. La forma en que M se transforma es cuando M corresponde a un número representativo de un mensaje.
- La decodificación se acopla a dicho canal y se adapta para recibir C desde el canal y para transformar C al mensaje M 'recibido.

Los medios de transformación comprenden:

- Este sistema tiene una serie de registros donde almacenamos el componente recibido.
- La señal a transformar, esta señal se almacena en un primer registro.
- Cuando el sistema recibe la segunda señal digital representativa del exponente de la relación de equivalencia, esta equivalencia se almacena en un segundo registro.
- Tenemos un tercer registro donde recibimos la señal digital representativa del módulo de equivalencia.
- Una exponenciación por red de cuadratura y multiplicación repetidas, aquí están los tres registros.

Transferencia de señales de mensaje $M_i$, con $k$ terminales, cada terminal se caracteriza por una clave de codificación. Así mismo, los medios de codificación para transformar dicha etiqueta de señal de palabra de mensaje cada bloque corresponde a un número representativo de una parte del mensaje firmado.

Las señales de palabras de texto cifrado de dicho primer terminal al segundo, esta segunda terminal incluye medios para descodificar dichas señales de palabras de texto cifrado firmadas.

Codificación y decodificación: medios de codificación acoplados a dicho canal y adaptados para transformar una señal de palabra de mensaje de transmisión y transmitir en el canal. Medios de decodificación acoplados a dicho canal y adaptados para recibir Mbs del canal correspondiente y transformar mbs del mensaje $M'$.

Codificación: cuando el sistema comienza a codificar significa que el primer terminal está adaptado para transformar dicha señal de palabra de mensaje $MA$ en una señal de palabra de texto cifrado firmada.

Un método para establecer comunicaciones criptográficas comprende el paso de:

- Codificación de la señal de la palabra del mensaje digital M al texto cifrado.

Transformando dicho mensaje firmado, la palabra MA de la señal, uno o más mensajes de la palabra de bloque de señal firmado MAS, cada señal de la palabra de bloque MAS" corresponde a un número representativo de una parte de dicha señal de palabra del mensaje firmado MA en el rango 0MAB"nB -1 y transforma cada una de dichas señales de palabra de bloque de mensaje firmado en una CA de señal de palabra de texto cifrado firmada.

Uno de dichos medios de transformación comprende los pasos de:

- Recibir y almacenar una primera señal digital en un primer registro, siendo dicha primera señal digital representativa de dicha palabra a transformar.

- Recibir y almacenar una segunda señal digital en un segundo registro, siendo dicha segunda señal digital representativa del exponente de la relación de equivalencia que define dicha transformación.

Ahora bien, para clarificar un poco más lo que se explica en las reivindicaciones, a continuación se explica de qué habla cada reivindicación y está dividido por cada reivindicación independiente por sus dependientes.

En primera instancia, para las reivindicaciones 1 y 2, se describe en qué consiste el sistema, que consta de un canal de comunicaciones, un medio de codificación acoplado a dicho canal y adaptado para transformar una señal de palabra de mensaje de transmisión $M$ en una señal de palabra de texto cifrado $C$ y para transmitir $C$ en dicho canal, donde $M$ corresponde a un número representativo de un mensaje y $0 \leq M \leq n-1$ donde $n$ es un número compuesto de la forma $n = p \cdot q$ donde $p$ y $q$ son números primos, y donde $C$ corresponde a un número representativo de una forma cifrada de dicho mensaje.

De las reivindicaciones 3 a 7, se habla sobre la transferencia de señales de mensaje que se caracteriza por tener terminales y una clave de codificación y decodificación. Se transmite de una terminal a otro y en la de llegada se debe tener los medios para descodificar el mensaje. Así mismo, de las reivindicaciones 8 a 12 se habla de como un bloque de palabras cifradas se puede traducir por medio de las terminales a un bloque de palabras decodificadas, es decir traduce las entradas por el mensaje deseado.

Por otra parte, en las reivindicaciones 13 a 24 habla sobre un sistema de comunicaciones que tiene una pluralidad de terminales acoplados por un canal de comunicaciones, que incluye un primer terminal terminal por una clave de codificación asociada y una clave de decodificación, e incluye un segundo terminal, en el que dicho primer terminal comprende: medios de codificación acoplados a dicho canal y adaptados para transformar una señal $MA$ de palabra de mensaje de transmisión en una $MA$ de señal de palabra de mensaje firme y para transmitir $MA$ en dicho canal. El segundo terminal comprende medios de decodificación acoplados a dicho canal y adaptados para recibir $MA$ de dicho canal y para transformar $MA$ en una señal de mensaje de recepción $MA$.

Las reivindicaciones 25-32 que consisten en codificar una señal de mensaje digital MA para su transmisión desde un primer terminal $(i = A)$ a una segunda terminal $(i = B)$, dicha etapa de codificación incluye la subetapa de transformar dicha señal de palabra de mensaje $MA$ a una señal de palabra de mensaje firmada $MA's$. Así mismo, en transformar dicha señal de palabra de mensaje $MA$ en una o más señales de palabra de bloque de mensaje $MA''$, cada señal de palabra de bloque $MA''$ corresponde a un número representativo de una parte de dicha señal de palabra de mensaje $MA$ en el rango $0 \leq MA'' \leq nB-1$, transformando cada una de dichas señales de palabra de bloque de mensaje $MA''$ a una señal de palabra de

texto cifrado $CA$, $CA$ correspondiente a un número representativo de una forma codificada de dicha señal de palabra de bloque de mensaje $MA$".

Las reivindicaciones 33 a 36 habla de un sistema de comunicaciones, un medio de codificación para transformar una señal $M$ de palabra de mensaje de transmisión en una señal $C$ de palabra de texto cifrado donde $M$ corresponde a un número representativo de un mensaje y $0 \leq M \leq n-1$ donde n es un número compuesto, y donde $C$ corresponde a un número representativo de una forma cifrada de dicho mensaje. Los medios de codificación están adaptados para transformar $M$ a $C$ mediante el desempeño de una primera sucesión ordenada de operaciones invertibles en $M$, al menos una de dichas operaciones es exponencial, un medio de descodificación adaptado para transformar $C$ a $M$ por el desempeño de una segunda sucesión ordenada de operaciones invertibles en $C$, en donde cada una de las operaciones invertibles de dicha segunda sucesión es la inversa de una correspondiente de dicha primera sucesión, y en donde el orden de dichas operaciones en dicha segunda sucesión se invierte con respecto al orden de operaciones correspondientes en dicha primera sucesión.

Finalmente, las reivindicaciones 37 a 40 hablan sobre un método para establecer comunicaciones criptográficas que comprende el paso de codificar una señal de palabra de mensaje digital $M$ a una señal de palabra de texto cifrado $C$, donde $M$ corresponde a un número representativo de un mensaje y $0 \leq M \leq n-1$ donde n es un número compuesto y donde $C$ corresponde a un número representativo de una forma codificada de la palabra de mensaje $M$, en donde dicha etapa de codificación comprende la etapa de transformar dicha señal de palabra de mensaje $M$ a dicha señal de palabra de texto cifrado $C$.

Los medios de transformación comprenden los pasos de recibir y almacenar una primera señal digital en un primer registro, siendo dicha primera señal digital representativa de la palabra a transformar, recibir y almacenar una segunda señal digital en un segundo registro, siendo representativo del exponente de la relación de equivalencia que define dicha transformación, recibiendo y almacenando una tercera señal digital en un tercer registro, siendo dicha señal representativa del módulo de la relación de equivalencia que define dicha transformación, y exponiendo dicha primera señal digital mediante repetición la cuadratura y la multiplicación utilizando dichas segunda y tercera señales digitales.

Dicha etapa de exponenciación incluye los pasos intermedios de:

A) Recibir y almacenar una primera señal multiplicadora en un registro de salida, y aplicar dicha primera señal multiplicadora a una primera línea de entrada multiplicadora,

B) Seleccionar sucesivamente cada uno de los bits de dicha segunda señal digital como un selector multiplicador

C) Para cada uno de dichos selectores multiplicadores, seleccionando como segunda señal multiplicadora el contenido de dicho registro de salida o el contenido de dicho primer registro, y para aplicar dicha segunda señal multiplicadora a una segunda línea de salida multiplicadora, dicha selección depende de la valor binario de los bits sucesivos de dicha segunda señal digital,

D) Para cada uno de dichos selectores multiplicadores, generando dicha primera señal multiplicadora en un módulo multiplicador en respuesta a la primera y segunda señales multiplicadoras en dichas primera y segunda líneas de entrada de multiplicador, y para transferir dicha primera señal multiplicadora generada a dicho registro de salida.

   La primera señal del multiplicador es inicialmente representativa del binario 1 y, a continuación, es representativa del producto en módulo de dichos primer y segundo multiplicadores, donde el módulo de dicho producto en módulo corresponde a dicha tercera señal digital.

# 4 Aplicaciones del RSA en la industria

## 4.1 Cifrado de Código

El código fuente encriptado depende del interés de aquellos que desean proteger su propiedad intelectual mientras distribuyen sus programas de manera segura. RSA se puede usar para ofuscar (hacer que los archivos sean más difíciles de leer) elementos importantes en el código fuente, como cadenas o El usuario recibirá una clave pública que utilizará para descifrar el código para ejecutar el programa. La palabra ofuscado se usa porque cualquier persona con suficiente tiempo y habilidad puede revertirla, ya que el programa en sí mismo es capaz de descifrar el código, por eso esta técnica de ofuscación es a veces controvertida entre los ingenieros de software.

El cifrado de archivos se basa en digitalizar primero los archivos, cosa que es compatible con muchos lenguajes de programación como C#. El archivo se cifra y se devuelve a su forma de texto.

Lo interesante es que para garantizar la protección del código, los criptógrafos están desarrollando una técnica para cifrar la ejecución del código fuente, utilizando cifrado homomórfico en lugar de RSA. En el cifrado homomórfico, si se realiza una operación matemática con datos cifrados, no es necesario descifrar la salida, lo que hace casi imposible realizar un seguimiento de la salida del software.

## 4.2 Autenticación de clave púplica para SSH

La autenticación de clave pública proporciona una fuerza criptográfica que incluso las contraseñas extremadamente largas pueden ofrecer. Además de publicarse, una autenticación auténtica permite a los usuarios implementar el inicio de sesión único en los servidores SSH a los que se conectan. Permite el inicio de sesión automatizado y sin contraseña, lo que es un importante habilitador para los procesos de automatización seguros que se ejecutan en las redes empresariales de forma global.

La criptografía de clave pública gira en torno a un par de conceptos clave:

***Criptografía asimétrica - Algoritmos***
Los algoritmos más comunes utilizados para la autenticación de clave pública son RSA y DSA. A diferencia de los algoritmos de cifrado de clave secreta o simétrica, los algoritmos de cifrado de clave pública funcionan con dos claves separadas. Estas dos claves forman un par específico del usuario.

***Par de llaves - públicas y privadas***
Las implementaciones de SSH incluyen utilidades fácilmente utilizables para que los usuarios creen la clave ellos mismos.

Cada par de claves SSH incluye dos claves:

Una *clave pública* que se copia a los servidores SSH. Cualquier persona con una copia de la clave pública puede cifrar datos que solo puede leer la persona que posee la clave privada correspondiente. Cuando el servidor

SSH recibe una clave pública de un usuario y considera que la clave es confiable, marca como clave autorizada.

Una *clave privada* que permanece exclusivamente con el usuario como prueba de la identidad del usuario. Solo un usuario que posea la clave privada que corresponde a la clave pública en el servidor podrá autenticarse con éxito. Las claves privadas utilizadas para la autenticación del usuario se denominan claves de identidad.

***Manejo de la clave privada***

Para la mayoría de los casos dirigidos por el usuario, la protección cuidadosa de la privacidad de la clave privada se logra mediante el cifrado de la clave privada con una frase de contraseña.

Siempre que se necesite una clave privada, el usuario debe proporcionar la frase de contraseña para que la clave privada pueda ser desencriptada. El manejo de frases de paso se puede automatizar con un agente de SSH.

# 5 Referencias


RSA. (2012). RSA distributed credential protection.
Recuperado de: https://www.emc.com/collateral/software/white-papers/h11013-rsa-dcp-0812-w p.pdf

Ylönen, T. (2017). SSH PROTOCOL. SSH Communications Security.
Recuperado de: https://www.ssh.com/ssh/protocol/

Caicedo Ortíz, H. (2010). Algoritmo de factorización para un computador cuántico (pp. 2-4). Distrito Federal.
Recuperado de http://www.lajpe.org/may10/16$_{H}ernando_{C}aicedo.pdf$

Hong, W. (2007). RSA Cryptosystem and Its Applications. Clayton College State University.
Recuperado de: http://archives.math.utk.edu/ICTCM/VOL17/C052/paper.pdf

Killeen, R. (2001) "Possible Attacks on RSA." RSA: Hacking and Cracking, Conan Kileen/Trinity College Dublin.
Recuperado de: www.members.tripod.com/irish$_{r}onan/rsa/attacks.html$.

Schneier, B. (1996) “ Applied Cryptography” New Nork. - Chichester : Valley, ISBN: 0-471-12845-7

SSH Communications Security, Inc. (2017) “Public Key Authentication for SSH”. SSH.com.
Recuperado de: https://www.ssh.com/ssh/public-key-authentication

Kaliski, Burt. “The Mathematics of the RSA Public-Key Cryptosystem”.
Recuperado de: http://www.mathaware.org/mam/06/Kaliski.pdf