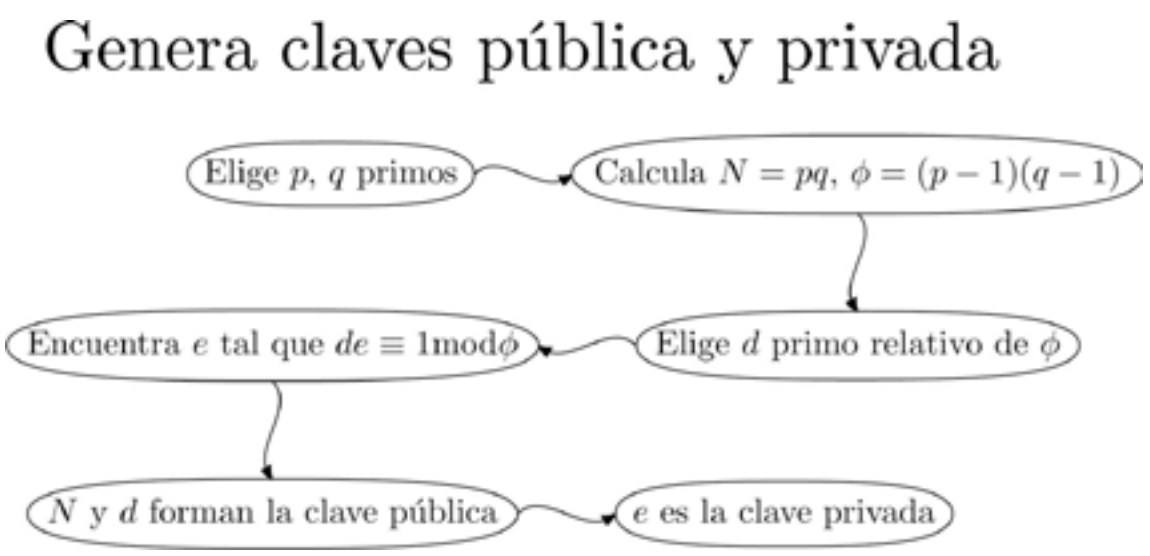
ACADEMIA DE CIENCIAS DE MORELOS, A.C.

¿Comentarios y sugerencias?, ¿Preguntas sobre temas científicos? CONTÁCTANOS: editorial @acmor.org.mx

Me están espiando



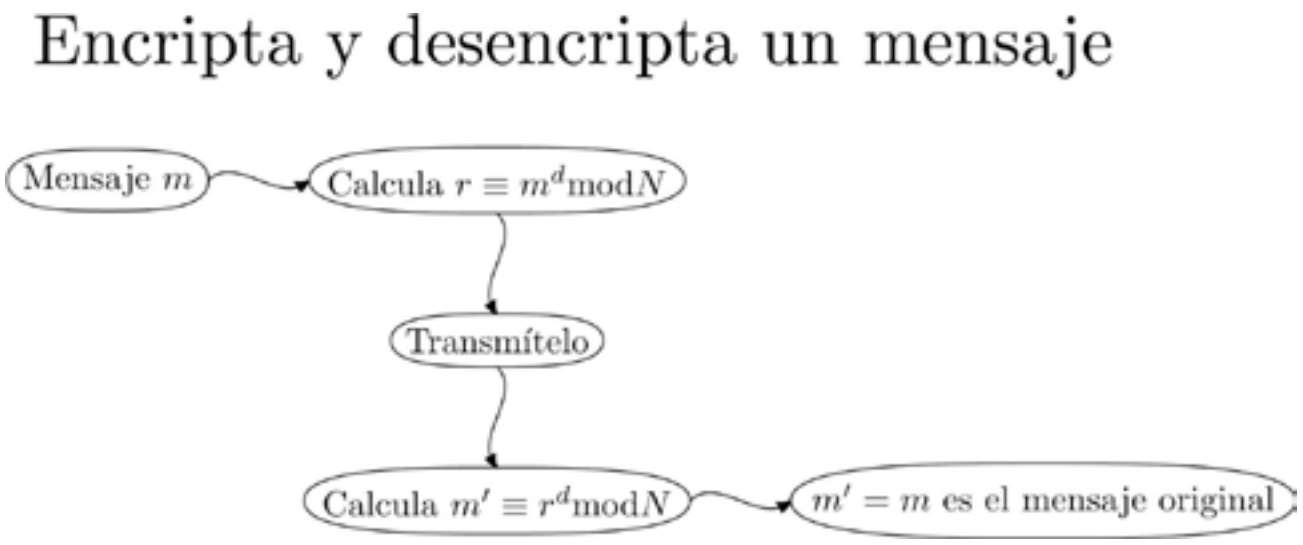
Algoritmo para generar la clave pública y la clave privada.

W. Luis Mochán Backal
Investigador del Instituto de Ciencias Físicas de la UNAM
Miembro de la Academia de Ciencias de Morelos

-Me están espiando.
-¡Estás paranoico!
-¿Qué, no has escuchado las noticias? La Agencia Nacional de Seguridad de Estados Unidos (NSA por sus siglas en inglés) ha espiado a nuestro presidente, a nuestro ex presidente, a la presidenta de Brasil, a la canciller de Alemania...
-Sí, pero ellos son importantes, no como tú.
-Importante o no, me espían. No lo permitiré.
-¿Cómo sabes que te espían?
-Lo sospechaba desde hace muchos años, antes de que Edward Snowden mostrara que la NSA ha obtenido información de ciudadanos en todo el mundo. Alguna vez falló la conexión vía internet entre mi casa y mi oficina, a pocos kilómetros de distancia. La falla podría haber estado en mi casa, en algún lugar de la UNAM, en la red telefónica... Para averiguarlo corrí *traceroute*.
-¿Corriste a donde?
-A ningún lugar. Mandé ejecutar en mi computadora un programa cuyo propósito es trazar las rutas que siguen los mensajes para llegar de una computadora a otra. El protocolo de comunicación TCP/IP de Internet prevee que los mensajes viajen saltando de una a otra computadora hasta llegar a su destino. Así te puedes comunicar con computadoras en cualquier lugar del mundo sin que tengan que estar conectadas todas entre sí.
-Y ¿que contestó tu programa?
-Dejame buscar... ¡aquí está!: 1 192.168.0.1 (192.168.0.1) 4.268 ms 4.319 ms 5.219 ms / 2 10.149.0.1 (10.149.0.1) 14.624 ms 15.589 ms 18.725 ms...
-¡Parale! No entiendo nada. ¿Qué son esos números?
-Unos números representan la dirección electrónica de alguno de los nodos que se encuentra en el camino. Por ejemplo, 192.168.0.1 es el *ruteador* de mi casa, 10.149.0.1 es una dirección interna de mi proveedor de internet. A veces obtengo el nombre del nodo además de los números que lo identifican. Los demás números corresponden aproximadamente al tiempo que tardan mis mensajes en llegar a cada nodo. Por ejemplo, 5.219ms significa poco más de cinco milisegundos. Para recorrer los cuatro kilómetros desde Bellavista hasta Chamilpa en Cuernavaca, mis mensajes se iban primero a pasear a Nueva York, Nueva Jersey, Texas, etc., antes de llegar a la ciudad de México, a Ciudad Universitaria y finalmente al Campus Morelos de la UNAM.
-¡Todo un paseo internacional! Parece ser poco eficiente.
-¡Es ridículo! Cada nodo debería tener una *tabla de ruteo* que le indica cuál es el camino menos congestionado que debería emplearse para que cada mensaje llegue a su destino lo antes posible y con el menor costo. Estas tablas se deben actualizar conforme cambia el tráfico en la red.
-Pues en México esas tablas ¡no están muy optimizadas!
-No le di mucha importancia al asunto, sino hasta hace poco, cuando leí algunos artículos recientes del periodista Glenn Greenwald detallando la enorme maquinaria de espionaje informático montada por el gobierno estadounidense.
-Y ¿entonces?
-La semana pasada, cuando me enteré del espionaje contra decenas de líderes mundiales, volví a checar mi red y encontré que mis mensajes ahora se van a Madrid y luego a Dallas.
-Y eso ¿cómo lo sabes?
-Por ejemplo, en el reporte de traceroute venía el nodo llamado if-12-7.tcore2.DT8-Dallas.as6453.net cuya dirección es 66.110.56.138. El nombre delata que está situado en Dallas, pero para confirmarlo ejecuté *whois*.
-Que ejecutaste ¿a quién?
-Whois es el nombre de un programa que interroga las bases de datos de internet y te dice quién registró qué nodo y dónde. Resulta que la dirección 66.110.56.138 está registrada como un nodo en Dallas perteneciente a *TATA Communications Ltd.*, una compañía de telecomunicaciones basada en Mumbai, India. Ese nodo recibió mis mensajes desde el nodo 213.140.52.126 en Madrid perteneciente a *Telefónica Internacional*. Los mensajes fueron enviados a España desde un nodo en la Ciudad de México registrado por la compañía *Telefónica* (México).
-¡Vaya labor detectivesca! ¿Y esos programas?
-Traceroute y whois son programas totalmente legales, del *dominio público*, gratuitos, libres y de *código abierto* que cualquiera puede conseguir e instalar en su computadora; yo encontré los míos preinstalados en mi sistema operativo *Linux/Debian*.
-Entonces ¿tú crees que algún proveedor de internet saca tus mensajes del país para espiar su contenido?
-Seguramente no solamente *mis* mensajes, sino los de muchos, y quizás los de *todos* los usuarios de internet en México.
-¿Y no será que esos nodos están en México, aunque registrados en el extranjero?
-Si así fuera, ¿por qué no registrarlos en el país en donde se encuentran? ¿Qué querrán ocultar?
-Me parece que estás sufriendo un ataque de *conspiranoya*, enfermedad común en esta época, en que todos creemos ser víctimas de alguna conspiración.
-Quizás, pero ya me empecé a cuidar, encriptando mis mensajes y pidiendo a mis corresponsales que encripten los suyos para que nadie pueda entender nuestras comunicaciones más que aquellos a quienes van dirigidas.
-¡Qué divertido! De pequeño me gustaba inventar códigos para mandar mensajes secretos, aunque cuando los interceptaban siempre descubrían el código.
-Seguramente es porque no sabías *teoría de números*.
-Claro que sí conocía los números; era el más rápido para hacer operaciones aritméticas.
-La teoría de *números* estudia las propiedades de los números, las cuales en ocasiones son fantásticas.
-¿Y eso qué tiene que ver con criptografía y los mensajes secretos?
-Se pueden aprovechar dichas propiedades para hacer códigos seguros, virtualmente irrompibles y con claves que se pueden compartir públicamente.
-No puede ser. Si publicas tu clave, ya no sería secreta.
-El truco consiste en tener *dos* claves, una pública y otra secreta. Tus amigos pueden usar la clave pública para enviarte mensajes cifrados que nadie, ni siquiera ellos, pueden descifrar si no tienen tu clave secreta.
-¿Y cómo funciona esto?
-Te daré un ejemplo, el código RSA: Empiezas con dos números *primos p* y *q*, calculas su producto *N=pq* y su *totiente f=(p-1)×(q-1)*, escoges un número *2<d<f* que sea *primo relativo* de *f* y buscas un número *e* tal que su producto *ed* sea congruente con 1 módulo *f*. Entonces, *N* y *d* serán el código público y *e* será tu clave secreta. Para enviarte un mensaje *m*, basta elevarlo a la potencia *d*, dividir el resultado entre *N* y transmitirte el residuo *r*. Para leer el mensaje elevarías *r* a la potencia *e*, dividirías el resultado entre *N* y eso es todo, el residuo sería el mensaje original *m*. Todos los espías del mundo podrían ver el mensaje cifrado *r* y podrían conocer los números *d* y *N*, pero ello no les permitiría conocer el contenido *m* del mensaje.
-¿Que qué? No entendí nada. ¿Me lo puedes barajear más despacio?
-Déjame darte un ejemplo. Considera los números primos 5 y 11.
-¿Primos de quién?
-De nadie, primos viene de primarios. Son números que no se pueden escribir como producto de otros números que no sean 1 y ellos mismos. Por ejemplo, seis no es primo pues 6=3×2, pero cinco sí es primo. Ahora multiplica los dos números primos que escogimos,
-...55,
-réstale 1 a cada uno,
-...4 y 10,
-y multiplícalos,
-...40.
-Bien, ya tenemos *N=55* y *f=40*. Fíjate que 40=2×2×2×5, los factores primos de 40 son por lo tanto 2 y 5. Escoge ahora un número cualquiera menor que 40 que no sea múltiplo de 2 ni de 5.
- ...3.
-Perfecto. Tomemos *d=3*. Ahora busquemos un número *e* tal que su producto con *d* deje residuo 1 al dividirlo entre 40. Como '40' termina en cero, el producto *d×e* debe terminar en 1. Para que 3 multiplicado por algo termine en 1, ese algo debe terminar en 7, así que las únicas posibilidades son *e=7, 17, 27* o *37*.
-Dejame checar... ya. De esas posibilidades, la correcta es *e=27* pues 3×27=81, que dividido entre 40 da 2 y sobra 1.
-Perfecto. Entonces mi clave secreta será *e=27* y mi clave pública consistirá de los números *N=55* y *d=3*.
-Y ¿cómo se usa?
-Imagínate que me quieres mandar un número secreto menor a 55, sin que nadie más se entere de cuál es, por ejemplo *m=35*. Lo primero que debes hacer es multiplicarlo por sí mismo *d=3* veces, *m×m×m=42875*. Luego divides el resultado entre *N=55*, obteniendo 779 y sobran *r=30*. Tu me mandarías el mensaje cifrado 30 y nadie sospecharía que el mensaje original era 35.
-¿Y tú cómo sabrías qué número te quise enviar?
-Cuando reciba el 30 lo multiplicaría por sí mismo *e=27* veces, *r×r×r...*
-¡Qué flojera! Mejor saco mi calculadora científica... ¡Ya está! 7.63e39.
-No. Ese es un número *aproximado*. Necesitamos el resultado *exacto*. Déjame sacar mi calculadora de precisión infinita... ¡Ya está! 76255974849870000000000000000000000000000. Para terminar, lo dividiré entre 55 para obtener el cociente 1386472269997636363636363636363636363 y el residuo 35 que ¡es el número que me querías mandar!
-Parece un proceso muy engorroso.
-Es un proceso muy fácil para una computadora.
-Y ¿sirve para cualquier número?
-Sí, siempre y cuando sea menor que N=55. Pruébalo.
-¿Cómo sabes que siempre funciona?
-Se puede demostrar para todos los mensajes usando, por ejemplo, el pequeño teorema de Fer-

ACADEMIA DE CIENCIAS DE MORELOS, A.C.

¿Comentarios y sugerencias?, ¿Preguntas sobre temas científicos? CONTÁCTANOS: editorial @acmor.org.mx



Algoritmos para encriptar y para desencriptar un mensaje.

mat que dice que si *p* es un número primo entonces cualquier número *a* elevado a la potencia *p* veces es congruente con...

-Dejemos la demostración para otro día. Pero, ¿qué interés tendríamos en enviar números?

-Todo mensaje, desde una carta de amor hasta una declaración de guerra, un texto en cualquier lenguaje, el audio de una sinfonía o el video de una ópera trágica, puede *codificarse* y convertirse en números para después *decodificarse*.

-Pero esos serían inmensos.

-Claro, pero se pueden partir en números pequeños, como cuando dictas tu número telefónico leyendo fragmentos de tres o cuatro cifras a la vez.

- Y este esquema ¿es en verdad seguro?

-Sí. Ni con todo el poder de cómputo del mundo podrías hallar los factores primos de un número. Es un problema intrínsecamente difícil; se cree que es un problema *NP-completo*.

-No me impresionas demasiado. Cualquier persona sabe que 55 es el producto de 5 por 11 y con esa información podrían repetir nuestros cálculos, hallar tu clave privada y espiarte.

-Claro, pero usé los números pequeños 5 y 11 sólo para que me entendieras. En la práctica se usan números con más de seiscientas cifras decimales. La dificultad para factorizar un número crece *exponencialmente* con su tamaño, más rápido que cualquier *polinomio*.

-Pero quién puede andar multiplicando, dividiendo y sacando residuos de números de 600 dígitos.

-Nuestras computadoras. Hay programas gratuitos, libres y abiertos para construir parejas de claves secretas y públicas seguras, hay sitios que permiten distribuir tus claves públicas a todos tus conocidos y desconocidos por igual, a todo aquel interesado en comunicarse contigo, y todos los clientes de correo electrónico tienen facilidades para encriptar el correo que mandas y para desencriptar los mensajes que recibes. Yo empleo el programa *gpg* cuyas siglas significan *Gnu Privacy Guard*, o sea, guardián de la privacía del proyecto GNU y que corre bajo el sistema operativo Linux. Hay versiones para otros sistemas operativos, como el programa *Gpg4win*.

-Y a todo esto, ¿a quién le envías mensajes cifrados?

-He ahí mi problema. Mis claves pueden emplearse para enviarme mensajes a mí. Para que yo pueda enviarte un mensaje cifrado a tí, tú debes tener tus claves y hacerme llegar tu clave pública. Para que el sistema sea útil, necesitamos que mucha gente lo use. Mientras más lo hagan, más útil será. Para ello debemos *promoverlo*. Quizás las escuelas, centros de investigación y otras instituciones académicas sean los mejores lugares para empezar. Además de permitirte cifrar mensajes para ocultarlos de la vista de espías y metiches, el sistema también te serviría para firmar tus mensajes, certificando que son tuyos y evitando que otros manden mensajes a tu nombre pretendiendo que provienen de tu cuenta de correo. Seas o no blanco de espías o malandrines, te conviene tener una clave secreta para firmar mensajes y que tus contactos tengan tu clave pública por si algún día requieren enviarte información delicada, como podría ser el saldo de tu cuenta de banco. Por todo esto *te invito a que obtengas tus claves, que uses el software criptográfico y que corras la voz*.

Bibliografía.

1. Para aprender sobre el protocolo TCP/IP de internet puede consultar la página http://en.wikipedia.org/wiki/Internet_protocol_suite.

2. Para aprender más sobre la historia de la criptografía puede consultar los artículos ¿Cómo evitar ser incluido en el portal de WikiLeaks? Historia breve de la criptografía de L. Enrique Sucar y Edgar A. Sucar publicado en la Unión de Morelos el 28 de marzo de 2012 y disponible en la dirección http://acmor.org.mx/descargas/11_mar_28_criptografia.pdf, así como el artículo Breve Historia de la Criptografía: Segunda Parte de L. Enrique Sucar y Edgar A. Sucar publicado en La Unión de Morelos el 21 de mayo de 2012 y disponible en http://www.acmor.org.mx/descargas/12_may_21_criptografia.pdf.

3. El protocolo criptográfico RSA es discutido en http://en.wikipedia.org/wiki/RSA_(algorithm).

4. Para conocer los programas del Gnu Privacy Guard puede ingresar a su página http://www.gnupg.org/.

5. Para aprender sobre el proyecto GNU y sobre el software libre puede consultar su página http://www.gnu.org/.

Para actividades recientes de la Academia y artículos anteriores puede consultar: www.acmor.org.mx

PREMIOS 2013
ACMor – La Unión

Premio al **Ensayo Científico Juvenil**

Quiénes pueden participar:
Estudiantes inscritos en una secundaria o en una institución de educación media superior, pública o privada, del Estado de Morelos.

Qué se necesita:
- Ser alumno inscrito en una secundaria o en una institución de educación media superior del Estado de Morelos, pública o privada, que cuente con reconocimiento oficial.
- Escribir un ensayo científico original, con una extensión entre 10,000 y 15,000 caracteres (contando espacios) firmado con un pseudónimo, sobre cualquier tema de las áreas de Matemáticas, Química, Física o Biología.
- Cumplir con todos los requisitos y entregar la documentación descrita en las reglas de la convocatoria.

Fecha límite:
02 noviembre 2013

Premios:
Se elegirá un ganador de nivel secundaria y otro de nivel de educación media superior. Cada premio consistirá de $ 10,000.00 M.N., un diploma y la publicación del ensayo.

Resultado:
El resultado se dará a conocer el día 02 de diciembre de 2013 en la página de la ACMor. Los ganadores serán contactados vía electrónica o telefónica para dar a conocer el fallo del jurado.

Premio al **Profesor Distinguido**

Quiénes pueden participar:
Profesores que impartan clases en una secundaria o en una institución de educación media superior, pública o privada, del Estado de Morelos y se hayan distinguido por su labor en la promoción de la ciencia.

Qué se necesita:
- Ser profesor en una secundaria o en una institución de educación media superior, pública o privada, del Estado de Morelos.
- Haber desarrollado recientemente actividades sobresalientes que promuevan el desarrollo científico de los jóvenes del Estado de Morelos.
- Cumplir con todos los requisitos y entregar la documentación descrita en las reglas de la convocatoria.

Fecha límite:
02 de noviembre de 2013

Premios:
El premio consistirá de $ 10,000.00 M.N. y un diploma.

Resultado:
El resultado se dará a conocer el día 02 de diciembre de 2013 en la página de la ACMor. El ganador será contactado vía electrónica o telefónica para dar a conocer el fallo del jurado.

Academia de Ciencias de Morelos, A.C.
La Unión de Morelos
Más información en: www.acmor.org.mx