Algoritmo Rivest-Shamir-Adleman (RSA).

El RSA, llamado así por las siglas de sus creadores (Rivest, Shamir y Adelman), es el algoritmo de clave pública más popular. El algoritmo se puede usar para encriptar comunicaciones, firmas digitales e intercambio de claves. La clave es de tamaño variable, generalmente se usan claves entre 512 y 2048 bits.

El funcionamiento del algoritmo es como sigue:

- **Encriptación**. Para encriptar un mensaje un usuario calcula $c=m^e$ modulo n, donde m es el texto en claro, c es el texto cifrado y (e, n) es la clave pública del destinatario.
- **Desencriptación**. Para desencriptar el mensaje el destinatario calcula c^d modulo n = $(m^e)^d$ modulo n = m^{ed} modulo n = m, donde (d, n) es la clave privada del destinatario. Hay que indicar que la última sustitución es posible por el modo en que hemos escogido los números, ya que d es el producto inverso de e modulo n, por lo que m^{ed}= m.
- **Firmado**. Si el emisor desea enviar el mensaje firmado usa su clave privada para calcular $c=m^d$ modulo n y el destinatario lo valida calculando c^e modulo n = $(m^d)^e$ modulo n = m^{de} modulo n = m, donde (e, n) es la clave pública del emisor.

RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977 por los informáticos y criptógrafos Ron Rivest, Adi Shamir y Leonard Adleman en el MIT. Fue el primer algoritmo creado de su tipo. Utiliza factorización de números enteros y, a diferencia de métodos anteriores de

clave pública como el Diffie y Hellman, es válido tanto para cifrar como para firmar digitalmente.

RSA funciona multiplicando dos números primos para generar un semiprimo, que crea una clave pública. Para que alguien pueda descifrar el mensaje, tendría que determinar los dos números primos utilizados para crear el semiprimo. Con números primos grandes, es extremadamente complejo y requiere mucho tiempo determinar esos dos números.

La base de la seguridad de este algoritmo es el problema de la factorización de números enteros. Se utiliza una representación numérica para los mensajes enviados y el funcionamiento utiliza el producto, conocido, de dos números primos grandes elegidos aleatoriamente y que se mantienen en secreto en todo momento. Actualmente, estos primos son del orden de 10200, y sigue aumentando debido al constante crecimiento en la capacidad de cálculo actual de los ordenadores.

Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave y, una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada. El algoritmo consta de cuatro pasos: generación de claves, distribución de claves, cifrado y descifrado.

El descifrado de RSA es mucho más lento que otros criptosistemas simétricos ya que requiere de más capacidad de procesamiento que otros tipos de algoritmos. Aunque el cifrado de un mensaje amplio es posible, se suele utilizar

para contraseñas relativamente cortas y cifrar con algoritmos simétricos mensajes más largos. RSA suele usarse para transmitir claves compartidas de criptografía simétrica.

Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos. Aunque también se cree que la computación cuántica podría hallar una solución al problema de factorización, existen investigadores que dudan que tales avances vayan a volver obsoletos estos algoritmos. No sólo aumentarán la capacidad de cálculo para descifrarlos sino también para aumentar el orden de los números primos utilizados.