Universidad del Quindío Oct. 4/2003
Ingeniería de Sistemas y Computación
Algoritmos I

Profesor: Leonardo Hernández Rodríguez
leonardohernandez@uniquindio.edu.co
www.geocities.com/leoher314

Introducción a la Criptografía

La criptografía es el arte y la ciencia de la comunicación secreta a través de canales poco seguros.

Como ejemplos de canales poco seguros tenemos el teléfono, Internet y el correo manual. Los llamados sitios seguros en Internet, son sitios que usan criptografía para evitar que terceras personas puedan observar información confidencial, como por ejemplo números de tarjeta de crédito.

Criptografía simétrica

En la criptografía simétrica se usa la misma clave tanto para encriptar como para desencriptar.

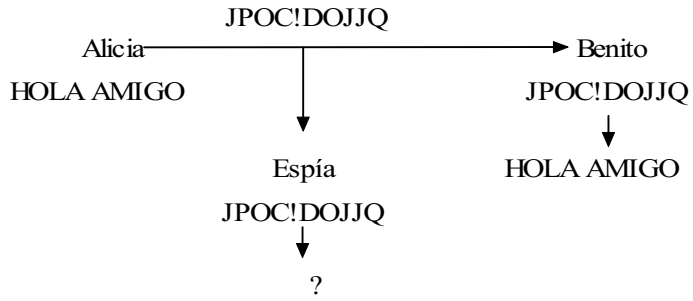
Ejemplo: supongamos que Alicia le va a enviar el mensaje "HOLA AMIGO" a Benito, digamos por e-mail, y que esté mensaje es secreto.

Primero Alicia debe encriptar el mensaje. Una manera de hacer esto, con criptografía simétrica, es la que se muestra en la figura:

Mensaje original:	H	O	L	A		A	M	I	G	O
	2	1	3	2	1	3	2	1	3	2
Mensaje cifrado:	J	P	O	C	!	D	O	J	J	Q

El sistema usa al número 213 como clave, la clave se repite varias veces debajo del mensaje. A partir de cada carácter se realizan desplazamientos de 2, 1 o 3 caracteres en la tabla ASCII obteniendo así el mensaje cifrado.

Alicia envía el mensaje cifrado "JPOC!DOJJQ" a Benito y este, haciendo el proceso inverso, obtiene el mensaje original "HOLA AMIGO".



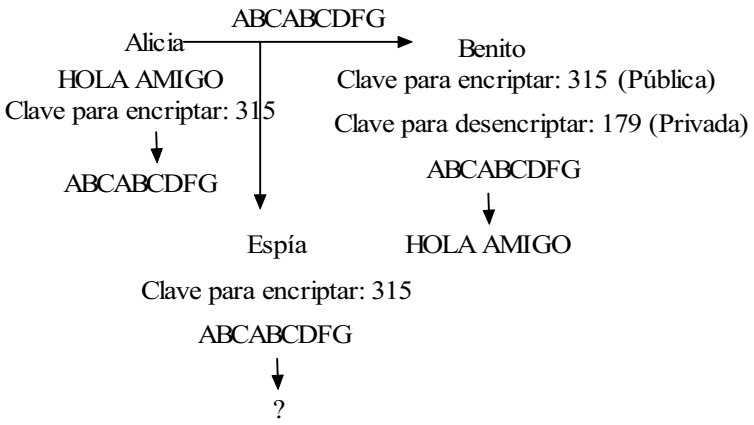
Aquí se requiere un acuerdo previo, Alicia debió dar a Benito la clave, previamente. Ese acuerdo previo es muy peligroso, un espía podría obtener en este momento la clave.

En el sistema de ejemplo, se observa también que es relativamente fácil, para el espía descifrar el mensaje, por ejemplo con un programa de computador basado en un diccionario o usando estadísticas de repetición de cada letra.

Criptografía Asimétrica

En los años 70 se consideró que el acuerdo previo no era necesario (Merkle, 1978 y Diffie y Hellman, 1976). Para evitar el acuerdo previo se usa criptografía asimétrica, la cual utiliza claves diferentes para encriptar y para desencriptar. Esto a primera vista parece imposible, pera ya existen procedimientos matemáticos para lograrlo.

Volvamos otra vez al caso en que Alicia desea enviarle a Benito el mensaje "HOLA AMIGO" y que este mensaje es secreto. Con criptografía asimétrica, se seguirá el procedimiento que se ilustra en la figura:



1. Benito, con algún procedimiento matemático establece las dos claves: la clave para encriptar y la clave para desencriptar. En el apartado siguiente se explicará uno de estos sistemas matemáticos: el sistema criptográfico RSA.

Supongamos que la claves son:
Clave para encriptar: 315
Clave para desencriptar: 179

2. Benito publica la clave para encriptar, 315, digamos en un sitio web. Cualquier persona puede ver esta clave, hasta el espía.

Benito guarda en secreto la clave para desencriptar

3. Alicia encripta el mensaje original "HOLA AMIGO", usando la clave para encriptar 315, la cual observó en el sitio web. Supongamos que el mensaje encriptado, con algún procedimiento matemático como el que veremos más adelante, queda: "ABCABCDFG".

4. Alicia envía el mensaje encriptado "ABCABCDFG" a Benito, y esto lo interpreta utilizando la clave para desencriptar 179, que solo él conoce.

5. El espía intercepta el mensaje encriptado "ABCABCDFG" pero no lo puede interpretar porque no conoce la clave para desencriptar 179, solo conoce la clave para encriptar 315, porque la obtuvo del sitio web.

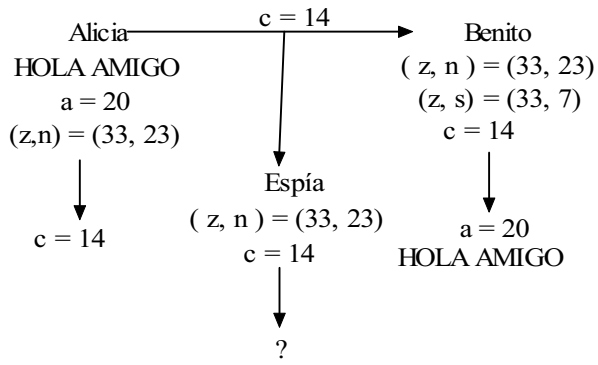
Como se ve, nunca se necesitó que Alicia y Benito tuvieran un acuerdo previo.

Sistema criptográfico RSA o de clave pública

El sistema criptográfico RSA es un sistema asimétrico inventado en 1978. RSA son las iniciales de sus inventores Rivest, Shamir y Adleman. RSA elimina, por consiguiente, la necesidad de un acuerdo previo.

Las claves son pares de números:
Clave para encriptar: *(z, n)*
Clave para desencriptar: (z, s)

La claves tienen la primera componente igual, pero la segunda diferente, por lo que en conjunto son diferentes. Veamos el procedimiento para que Alicia le envíe a Benito el mensaje secreto "HOLA AMIGO".



1. Con los pasos siguientes Benito halla z, n y s, con lo que quedan determinadas la llave para encriptar y la llave para desencriptar.

a) Se escogen dos números primos p y q de 100 cifras. Para el ejemplo tomaremos dos pequeños:

$p = 3$
$q = 11$

b) Se halla $z = p \times q$

$$z = p \times q = 3 \times 11 = 33$$

c) Se halla $\phi = (p - 1)(q - 1)$

$$\phi = (p - 1)(q - 1) = 2 \times 10 = 20$$

d) Se escoge n talque $1 \leq n \leq z - 1$ y que n no tenga factores comunes con ϕ.

Es decir debemos escoger un número n talque $1 \leq n \leq 32$ y que no sea divisible ni por 2 ni por 5, ya que $\phi = 20 = 2^2 \times 5$.

Escogeremos $n = 23$

Hubiera servido $n = 9$, pero no $n = 10$,

e) Se halla s, tal que $1 \leq s \leq z - 1$ y ns mod $\phi = 1$.

Debemos hallar s talque $23s \bmod 20 = 1$, Esto requiere de un teorema matemático, pero por simplicidad lo hallaremos por ensayo y error, haciendo que s tome los valores 1, 2, 3, …

$s = 1$ $23 \times 1 \bmod 20 = 3$
$s = 2$ $23 \times 2 \bmod 20 = 6$
$s = 3$ $23 \times 3 \bmod 20 = 9$
$s = 4$ $23 \times 4 \bmod 20 = 12$
$s = 5$ $23 \times 5 \bmod 20 = 15$

$s = 6$ $23 \times 6 \bmod 20 = 18$
$s = 7$ $23 \times 7 \bmod 20 = 1$

Por lo que $s = 7$.

En este momento quedan determinadas las claves para encriptar y para desencriptar:

Clave para encriptar $(z, n) = (33, 23)$
Clave para desencriptar $(z, s) = (33, 7)$

Como dijimos antes, Benito publica la clave para encriptar y oculta la clave para desencriptar. Cualquiera puede conocer la clave para encriptar, hasta el espía.

2. Alicia encripta el mensaje, usando la llave que publicó Benito y envía el mensaje encriptado a Benito.

El mensaje se encripta con la fórmula $c = a^n \bmod z$, donde a es el mensaje original en caracteres ASCII, $0 \leq a \leq z - 1$, c es el mensaje encriptado y z y n conforman la clave para encriptar ya conocida.

Para facilitar la explicación supongamos que el mensaje “HOLA AMIGO” en caracteres ASCII equivale a $a = 20$. En realidad sería un número mucho más largo. Entonces:

$$c = a^n \bmod z = 20^{23} \bmod 33$$

23 $20 \bmod 33 = \boxed{20}$
11 $20^2 \bmod 33 = \boxed{4}$
5 $4^2 \bmod 33 = \boxed{16}$
2 $16^2 \bmod 33 = 25$
1 $25^2 \bmod 33 = \boxed{31}$

$20 \times 4 \bmod 33 = 14$
$14 \times 16 \bmod 33 = 26$
$26 \times 31 \bmod 33 = 14$

Luego $c = 14$.

Alicia envía el mensaje encriptado $c = 14$ a Benito.

3. Benito descifra el mensaje con la fórmula: $a = c^s \bmod z$, donde c es el mensaje encriptado que recibió de Alicia y s y z conforman la llave para desencriptar que Benito estableció en el paso 1.

$a = c^s \bmod z = 14^7 \bmod 33$

7 $\quad 14 \bmod 33 = \boxed{14}$
3 $\quad 14^2 \bmod 33 = \boxed{31}$
1 $\quad 31^2 \bmod 33 = \boxed{4}$

$14 \times 31 \bmod 33 = 5$
$5 \times 4 \bmod 33 = 20$

Luego a = 20.

Como supusimos que 20 era “HOLA AMIGO” en códigos ASCII, en este momento Benito ha descifrado el mensaje.

4. Veamos la situación del espía.

La situación del espía es la siguiente:

- Conoce la clave para encriptar $z = 33$ y $n = 23$ porque Benito publicó estos valores.
- Conoce el mensaje encriptado $c = 14$ porque lo interceptó.

El espía no puede descifrar el mensaje con la fórmula $a = c^s \bmod z$, ya que no conoce s, porque el valor de s fue guardado en secreto por Benito.

Aparentemente el espía podría descifrar el mensaje con los siguientes pasos:

a) Descomponer $z = 33$ en sus factores primos, hallando $p = 3$ y $q = 11$.

b) Hallar $\phi = (p - 1)(q - 1) = 2 \times 10 = 20$

c) Hallar la parte faltante de la llave para desencriptar $s = 7$, ya que, en este momento, s es la única variable desconocida en la ecuación $ns \bmod \phi = 1$.

d) Hallar el mensaje original en códigos ASCII:

$$a = c^s \bmod z = 14^7 \bmod 33 = 20.$$

El secreto está en que el paso a) en la realidad es imposible. Recordemos que en la realidad p y q son primos de 100 cifras y z podría tener 199 o 200 cifras. Descomponer un número de 200 cifras en sus factores primos es imposible con la tecnología actual, demoraría un tiempo muy superior a la edad del universo.

La seguridad del sistema RSA no ha sido demostrada matemáticamente. Cabe la posibilidad de que alguien invente o haya inventado una manera de violarlo. Aún así, el sistema RSA es considerado como una de las mejores invenciones en la historia de la criptografía.

Ejercicios:

Dados los números primos p, q, la segunda parte de la llave para encriptar n y el mensaje original en códigos ASCII a, halle la segunda parte de la llave para desencriptar s y el mensaje encriptado c.

Resuelva en clase el ejercicio número 1), los demás son para practicar en la casa.

					Respuesta	
#	p	q	n	a	s	c
1)	5	11	49	8		
2)	3	7	17	19	5	10
3)	5	11	23	37	7	53
4)	11	13	47	21	23	109
5)	7	11	13	26	37	75