CRIPTOSISTEMAS DE CLAVE PÚBLICA
¿Son seguras tus comunicaciones?

M.Ángeles Lozano

Tutor:Albert Masip-Álvarez

INTRODUCCIÓN

Actualmente tenemos toda la información en formato digital
esto nos facilita la rapidez, transporte y uso de los datos.
Pero al mismo tiempo también nos crea problemas con la seguridad en nuestras comunicaciones.

Para averiguar que grado de seguridad tienen, vamos a estudiar el criptosistema de mayor difusión y relevancia : la RSA

OBJETIVO

El objetivo del trabajo es ver como se generan las claves para cifrar y descifrar los mensajes que utilizamos a diario ,tanto en redes sociales como para gestiones administrativas .Y asi garantizar su fiabilidad mediante la firma digital

METODOLOGIA

Se han consultado los datos en libros y en la web.Tambiéh se ha consultado a los gestores de la firma digital de Greintec (Gremi de instaladores de Terrassa y Comarca)

CONCLUSIONES

En la sociedad digital en la que vivimos,casi todas nuestras actividades las gestionamos vía internet.
Gracias a la criptografía. tenemos cierto grado de seguridad en nuestras comunicaciones.
Pero como usuarios,bien por falta de conocimientos o por despreocupación, cada día nos llegan noticias de hackeos de datos o intentos de estafas.
Por tanto aún queda mucho que hacer en cuanto a seguridad .

RESULTADOS

La criptografía nos está facilitando la vida: como aplicación la Firma Digital.

Gracias a ella las gestiones que hacemos a diario ,son más rápidas y seguras ; al mismo tiempo cuidamos al planeta con el ahorro de papel.

¿Cómo funcionan las claves RSA?

Algoritmo de cifra asimétrica RSA

En febrero de 1978 Ron Rivest, Adi Shamir y Leonard Adleman proponen un algoritmo de cifra de clave pública: RSA

Pasos del algoritmo

1. Cada usuario elige un grupo $n = p*q$ (pueden y de hecho son distintos)
2. Los valores p y q no se hacen públicos.
3. Cada usuario calcula $\phi(n) = (p-1)(q-1)$.
4. Cada usuario elige una clave pública e de forma que $1 < e < \phi(n)$ y que cumpla con la condición: $\text{mcd}[e, \phi(n)] = 1$.
5. Cada usuario calcula la clave privada $d = \text{inv}[e,\phi(n)]$.
6. Se hace público el grupo n y la clave e.
7. Se guarda en secreto la clave d. También guardará p y q puesto que en la operación de descifrado usará el Teorema del Resto Chino.

Cifra: $C = N^{eR} \bmod n_R$ Firma: $C = h(M)^{dE} \bmod n_E$

REFERENCIAS

Fuster A;De la Guia D; Hernández LL;Montoya F (2003) : Técnicas Criptográficas de Protección de Datos .Ed .Ra-Ma
https://es.m.wikipedia.org/wiki/Criptografia
foto1: https://www.ionos.es/digitalguide/servidors/seguridad/clav3-rsa
foto2:https://tutorialesenlinea.es/257-claves-rsa/amp.html