SEGURIDAD INFORMATICA

Criptología

(del Griego Krypto y logos)

El estudio de lo oculto, lo escondido.

"Estudia problemas teoricos en la seguridad en el intercambio de mensajes".

Dos Ramas: **Criptografia**. **Criptoanalisis**.

SEGURIDAD INFORMATICA

CRIPTOLOGÍA

CRIPTOGRAFÍA

Arte de Escribir
Mensajes Secretos

CRIPTOANÁLISIS

Arte de Descifrar
Mensajes Secretos

SEGURIDAD INFORMATICA

SEGURIDAD INFORMATICA

CriptoSIstemas

Definiremos un criptosistema como una quíntupla (M, C, K, E, D), donde:

- M representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto plano, o *plaintext*) que pueden ser enviados.
- C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K representa el conjunto de claves que se pueden emplear en el criptosistema.
- E es el conjunto de *transformaciones de cifrado* o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E_k para cada valor posible de la clave k.
- D es el conjunto de *transformaciones de descifrado*, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

$$D_k(E_k(m)) = m$$

SEGURIDAD INFORMATICA

Criptografia

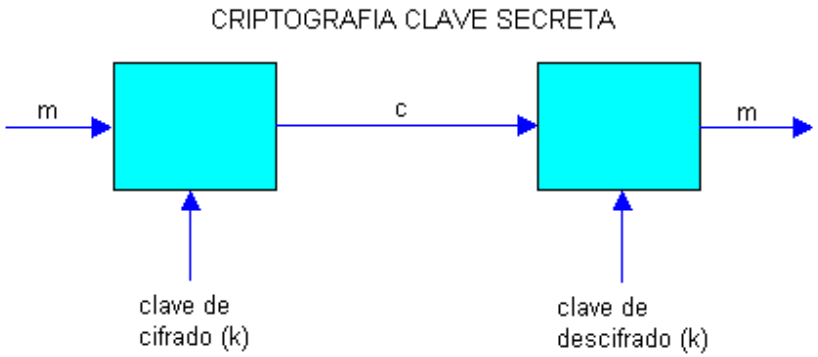
Criptosistema de clave Simetrica o Privada

Emplean la misma clave k tanto para cifrar como para descifrar

.

El problema es que para ser empleados en comunicaciones la clave k debe estar tanto en el emisior como en el receptor.

Como viaja la clave? Es segura?

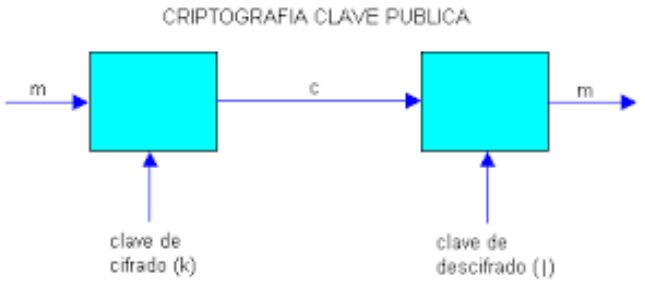


SEGURIDAD INFORMATICA

Criptografia

Criptosistemas Asimetricos o de clave Pública

Emplean una doble clave (k p , k P).
k p se conoce como clave privada
k P se conoce como clave pública.
k P sirve para la transformación E de cifrado.
k p para la transformación D de descifrado.



Estos criptosistemas deben cumplir además que el conocimiento de
La clave pública k P no permita calcular la clave privada k p .

Pueden emplearse para establecer comunicaciones seguras por canales inseguros
(SOLO viaja por el canal la **clave pública**, que sólo sirve para:

- Cifrar.
- Autentificar.

SEGURIDAD INFORMATICA

Otras formas de esconder

Esteganografía:

La idea es el empleo de canales subliminales.

Consiste en ocultar en el interior de una información, aparentemente inocua, otro tipo de información (cifrada o no).

Muy utilizado ya permite burlar diferentes sistemas de control.

Un mensaje cifrado es detectabe y al menos puede ser interrumpido. En cambio un mensaje camuflado es mas invisible.

El mensaje se envía como texto plano, pero entremezclado con cantidades ingentes de basura.

La técnica se la conoce como chaffing and winnowing, que vendría a traducirse como llenar de paja y separar el grano de la paja.

Creado por RIVEST en 1998 para como desafío a la política restrictiva del Gobierno de los EE.UU.

Criptologia

Criptoanálisis:

La idea es comprometer la seguridad de un criptosistema.

2 Formas: hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación.

No es criptoanálisis el descubrimiento de un algoritmo secreto de cifrado.

Suponemos por el contrario que ***los algoritmos siempre son conocidos.***

SEGURIDAD INFORMATICA

Criptologia

Criptoanálisis:

Algunas estimaciónes probabilisticas de vocales y conectores
En castellano...

espacio	0.164
e	0.094
a	0.088
o	0.062
s	0.055
i	0.051
n	0.051
r	0.048
l	0.041
d	0.040
c	0.034
t	0.033
u	0.027
m	0.020
p	0.020
b	0.010
g	0.010
v	0.007
y	0.007
f	0.006
q	0.006
h	0.005
j	0.003
z	0.003
x	0.002
ñ	0.001
k	0.000
w	0.000

	frecuencia
de	0.0659
la	0.0351
a	0.0319
el	0.0270
en	0.0259
y	0.0258
que	0.0238
los	0.0157
del	0.0133
se	0.0111
las	0.0103
por	0.0098
con	0.0075
un	0.0073
su	0.0064
una	0.0063
no	0.0058
para	0.0057
al	0.0055
es	0.0053
lo	0.0042
pero	0.0017
ya	0.0012
hasta	0.0011

SEGURIDAD INFORMATICA

CriptoSIstemas

El cuadrado de Polibio:

Inventado hacia 150 a. C. por el historiador Polibio, el cuadrado de Polibio fue utilizado principalmente por nihilistas rusos encerrados en las prisiones zaristas. Se trata de un algoritmo trivial, donde cada letra del alfabeto es reemplazada por las coordenadas de su posición en un cuadrado.Tomamos un cuadrado de Polibio con lugares cuadrados.

Es posible extenderlo a 36 para agregar cifras y signos de puntuación.

En este caso, pondremos la I y la J juntas para poder entrar en 25 lugares.

Carlos → 131142313443

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

SEGURIDAD INFORMATICA

CriptoSIstema

Un metodo de los Confederados:

Es un tipo de sustitución polialfabética. Básicamente, se escoge una clave, que se va "sumando" al texto llano para dar lugar al texto cifrado. Eso de sumar significa que hacemos como si las letras fuesen números. Si hacemos B=2 y C=3, entonces B+C=2+3=5=E.

La Frase: HOY ES EL DIA
La clave:FE

H	O	Y		E	S		E	L		D	I	A
F	E	F		E	F		E	F		E	F	E
N	T	E		J	Y		J	P		I	Ñ	F

El criptograma:NTE JY JP IÑF

SEGURIDAD INFORMATICA

CriptoSIstemas
Criptografía Clasica

Cifrados Monoalfabéticos:

Sin desordenarlos símbolos dentro del mensaje, establecen una correspondencia única para todos ellos en todo el texto.

Es decir, si al símbolo A le corresponde el símbolo D, esta correspondencia se mantiene a lo largo de todo el mensaje.

El sistema Caesar: (Cesar, por Julio Cesar)

Alfabeto A= Zm (enteros modulo m).

f(x)= ax+b, a<>0

1/f(x)=x-b).

Caesar utiliza (1,b) es decir a=1.

SEGURIDAD INFORMATICA

Clasica

CESAR CON SALTO Y PALABRA:

Consiste en utilizar un salto y una palabra Clave.

A partir de la posición del salto escrbir la palabra, sin repetir caracteres y completar

0	1	2	3	4	5	6	7	8	9	0	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
					M	U	R	C	I	E	L	A	G	O												
T	V	W	X	Y	M	U	R	C	I	E	L	A	G	O	B	D	F	H	J	K	N	Ñ	P	Q	R	S

SEGURIDAD INFORMATICA

Clasica

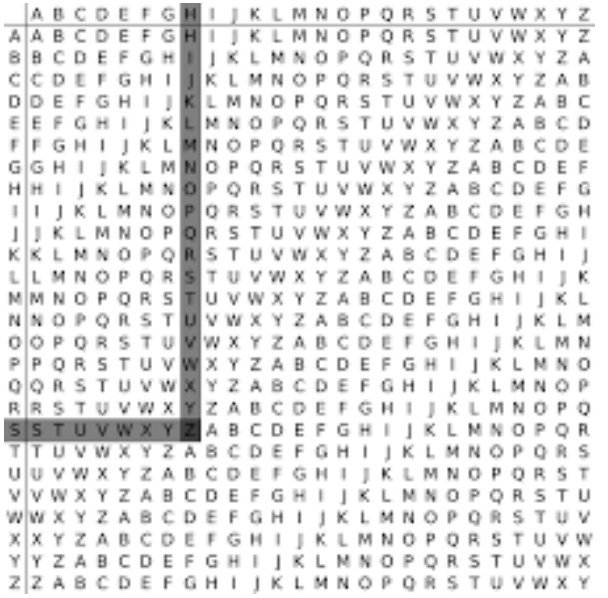
Cifrados Polialfabéticos:

La sustitución aplicada a cada carácter varía en función de la posición que ocupe éste dentro del texto plano.

En realidad corresponde a la apliación cíclica
de n cifrados monoalfabéticos.Sin desordenarlos símbolos dentro del mensaje, establecen una

El sistema Vigénere: (Criptografo Frances):

Matriz de 26x 26. (a..z). desplazada de a 1 por fila.
clave= palabra de K letras >=1.
1) Una frase a encriptar y la clave.
2) Dividir la frase en grupos de k letras.
3) Repetir la clave por gupos de palabras de k letras.
4) Armar criptograma fila= frase, columna=clave.(letras)



SEGURIDAD INFORMATICA

Criptografía

Cifrados de Transposición:

La idea es no sustituir unos símbolos por otros, sino que cambia su orden dentro del texto.

La Frase: "EL AMIGO DE MI AMIGO ES MI AMIGO"
La clave: Rotación 3,2,5,1,4

1	2	3	4	5
E	L		A	M
I	G	O		D
E		M	I	
A	M	I	G	O
	E	S		M
I		A	M	I
G	O			

APLICAMOS ROTACIÓN {32514}

3	2	5	1	4
	L	M	E	A
O	G	D	I	
M			E	I
I	M	O	A	G
S	E	M		
A		I	I	M
	O		G	

El Criptograma : " LMEAOGDI M EIIMOAGSEM A IIM O G "

Los espacios valen!!!

SEGURIDAD INFORMATICA

Criptografía 2da Guerra

Máquinas de Rotores. La Máquina ENIGMA:

Se trataba de un instrumento, parecido a una máquina de escribir. Quien deseara codificar un mensaje sólo tenía que teclearlo y las letras correspondientes al mensaje cifrado se irían iluminando en un panel.
El destinatario copiaba dichas letras en su propia máquina y el mensaje original aparecía de nuevo.

La clave la constituían las posiciones iniciales de tres tambores o rotores

SEGURIDAD INFORMATICA

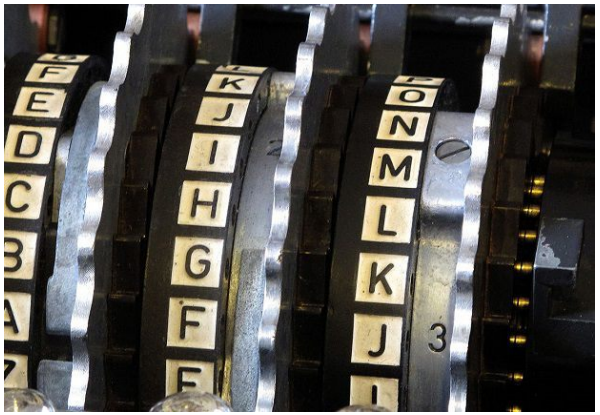
La Máquina ENIGMA:

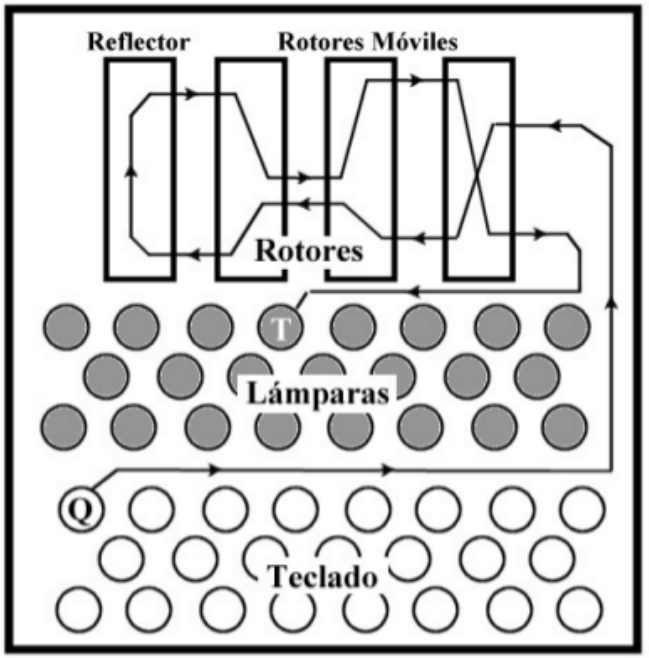
Enigma era el nombre de una máquina que disponía de un mecanismo de cifrado rotatorio, que permitía usarla tanto para cifrar como para descifrar mensajes.

Durante la guerra: Le aplicaron varias mejoras, como incluir un pequeño sistema previo de permutación de letras, llamado Stecker.

Incorporar rotores intercambiables

Se podían elegir y colocar en cualquier orden tres de entre cinco disponibles





SEGURIDAD INFORMATICA

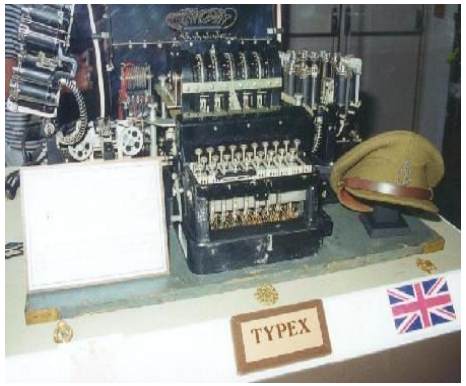
Criptografía 2da Guerra

Otras Máquinas de Rotores:

Enigma fue la Estrella pero existieron otras maquinas de rotores en esa epoca **SIGABA** (USA) **TYPEX** (GB) ambas blanqueadas en el año 2000. Japon por su parte tuvo codigo RED y **PURPLE**.

SIGABA

TIPEX



PURPLE

Criptografía Moderna

Algoritmos Simétricos de Cifrado

La gran mayoría de los algoritmos de cifrado simétricos se apoyan en los conceptos de confusión y difusión inicialmente propuestos por Shannon.

Para conseguir algoritmos fuertes sin necesidad de almacenar tablas enormes es intercalar:

- **Connfusión** (sustituciones simples, con tablas pequeñas)
- **Difusión** (permutaciones).

En muchos casos el criptosistema no es más que un paso simple de sustitución-permutación repetido n veces, como ocurre con **DES**

SEGURIDAD INFORMATICA

Criptografía Moderna

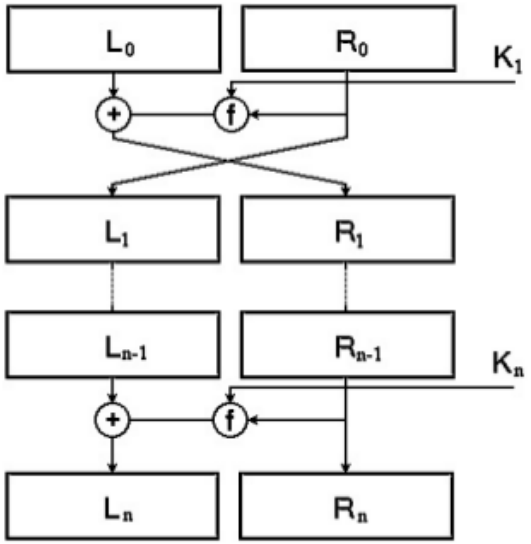
Redes de Feistel

Muchos de los cifrados de producto tienen en común que dividen un bloque de longitud **n** en dos mitades, **L y R.**

1) Selecionar cadena, **N** de **64** o **128** bits dividir en **L** y **R**, de igual longitud (**N/2**)

2) Se toma una función, **F**, y una clave **Ki**

3) Se realizan una serie de operaciones con F y Ki y con **L** o **R** (solo uno de ellas)
La cadena obtenida intercambia por la cadena sin operar y se Hace nueva ronda

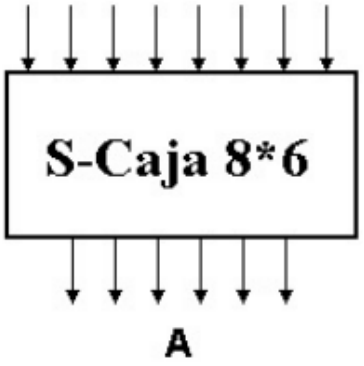


Utilizados por DES, Lucifer, FEAL, CAST, Blowfish,

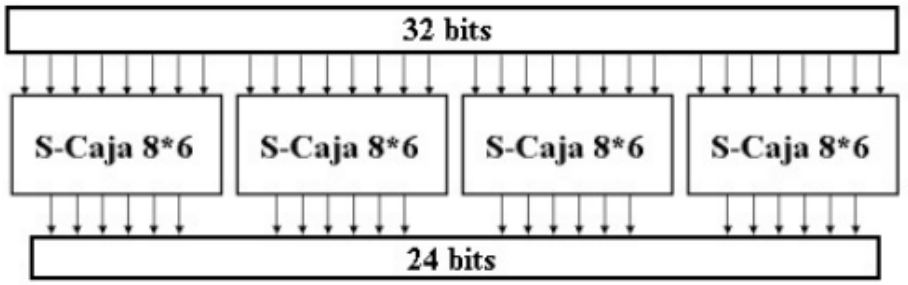
Criptografía Moderna

Cifrados con Estructura de Grupo

Como para poder construir buenos algoritmos de producto, intercalaremos sustituciones sencillas (confusión), con tablas pequeñas, y permutaciones (difusión). Estas tablas pequeñas de sustitución se denominan de forma genérica **S-Cajas.**



A



B

Se divide el bloque original en trozos de m bits y cada uno de ellos se sustituye por otro de n bits.

SEGURIDAD INFORMATICA

Criptografía Moderna

Criptosistema de clave secreta: (DES)

Data Encryption Standard.

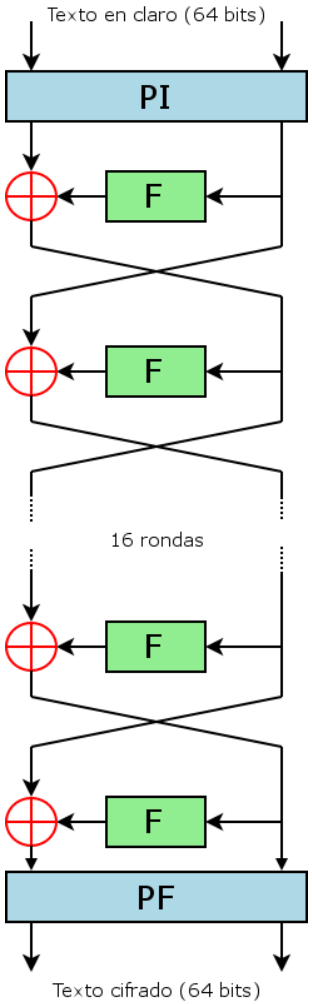
El original trabaja con 64 bit de cifrado. 56 de clave y 8 de paridad.

Divide la informacion en grupos de 64 bits.

Para cada grupo:

- aplica permutacion inicial fijo IP.”desordena”
- divide en 2 grupos de 32
- para c/ subgrupo: Aplica 16 veces “vueltas”, el algoritmo de cifrado compuesto de Permutaciones, substituciones y operacines

- Utilizado desde la decada del 70 Aprobado 1976.
- Remplazado en el 2002 poe el AES Advanced Encryption Standard.
- Violado por fuerza bruta en 1998 Muchos usuarios de DES utilizan 3DES. (aplicar 3 veces DES)



SEGURIDAD INFORMATICA

Criptografía Moderna

Criptosistema de clave secreta: (IDEA)

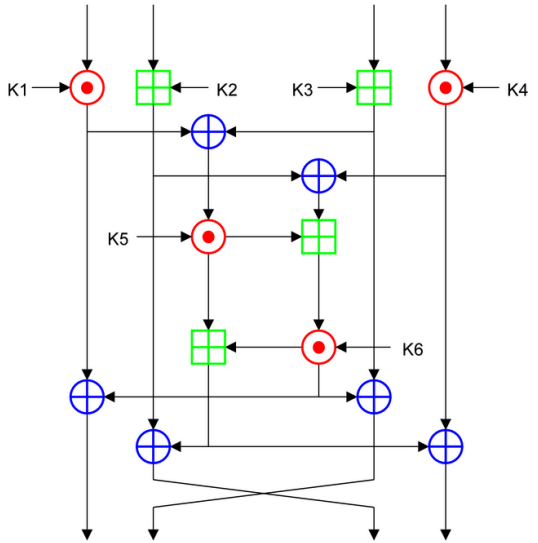
International Data Encryption Algorithm

Trabaja con bloques de 64 bits de longitud y emplea una clave de 128 bits.

IDEA es un algoritmo bastante seguro, y hasta ahora se ha mostrado resistente a multitud de ataques, entre ellos el criptoanálisis diferencial.

Se basa en los conceptos de confusión y difusión, haciendo uso de las siguientes operaciones:

- XOR.
- Suma módulo 2 16 .
- Producto módulo 2 16 + 1



El algoritmo IDEA consta de ocho rondas.

SEGURIDAD INFORMATICA

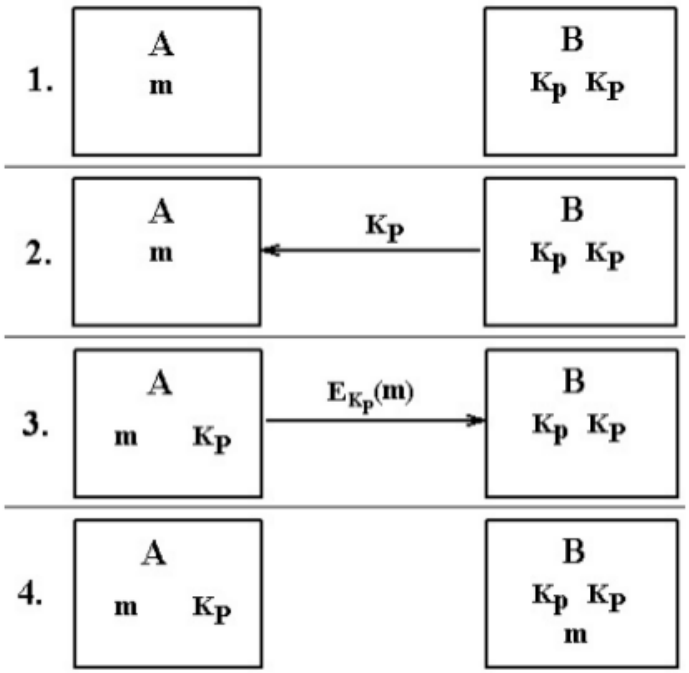
Criptografía de Llave Pública

Algoritmos Asimétricos de Cifrado

Constan de dos claves diferentes en lugar de una, **K p** y **K P** , denominadas: clave privada y clave pública.

Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar.

Dependiendo de la aplicación que le demos al algoritmo, la clave pública será la de cifrado o viceversa.



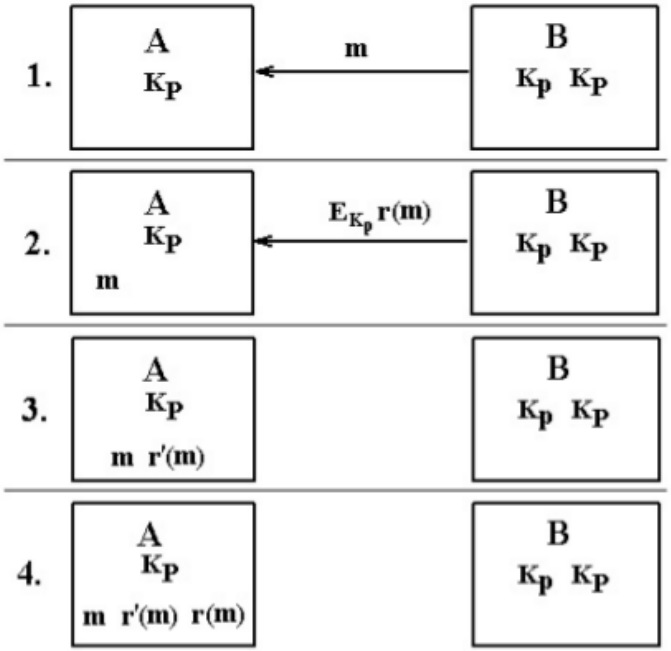
SEGURIDAD INFORMATICA

Criptografía de Llave Pública

Autentificación

La segunda aplicación de los algoritmos asimétricos es la autentificación de mensajes, con ayuda de funciones resumen

Las Fnciones de Resumenpermiten obtener una firma a partir de un mensaje.



SEGURIDAD INFORMATICA

Criptografía de Llave Pública

El Algoritmo RSA

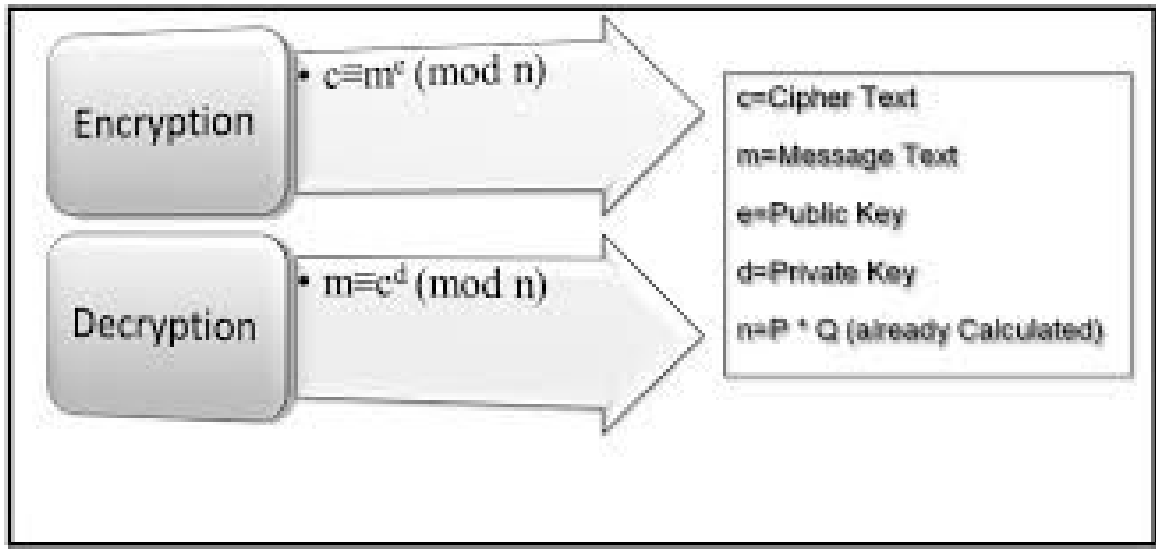
Su nombre proviene de sus inventores:

Ron Rivest, Adi Shamir y Leonard Adleman.

Desde su nacimiento nadie ha conseguido probar o rebatir su seguridad, pero se le tiene como uno de los algoritmos asimétricos más seguros.

RSA se basa en la dificultad para:

Factorizar grandes números.



SEGURIDAD INFORMATICA

Criptografía de Llave Pública

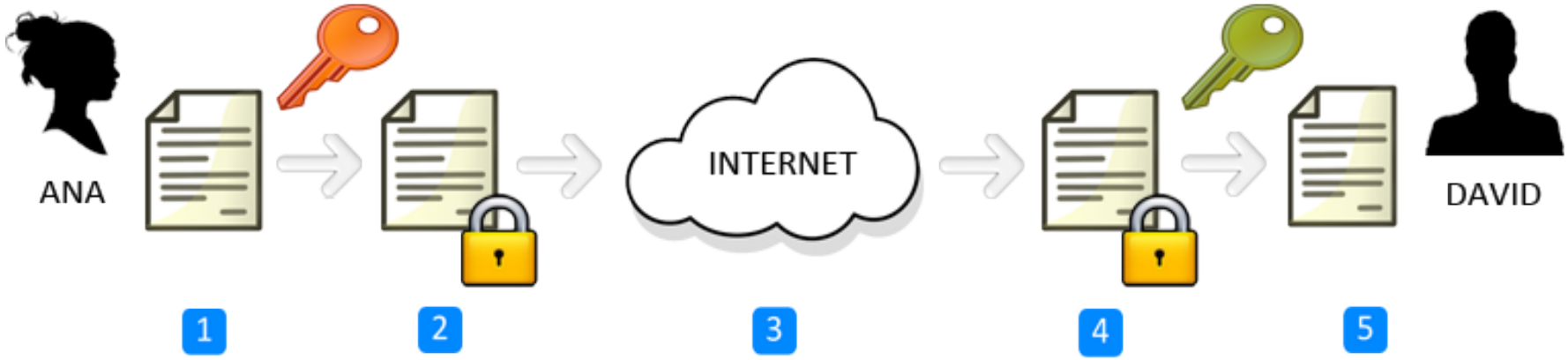
Otros Algoritmos de Clave publica:

- **Codificación de ElGamal**
  - Cifrado basado en Logaritmo Discreto
- **Algoritmo de Rabin**
  - **raices cuadradas módulo un número compuesto**
- **DSA (Digital Signature Algorithm)**
  - **Firma digital**

SEGURIDAD INFORMATICA

Criptografía de Llave Pública

Ejemplo de cifrado de mensaje: Ana envía un mensaje a David



1- Ana redacta un mensaje
2- Ana cifra el mensaje con la clave pública de David
3- Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4- David recibe el mensaje cifrado y lo descifra con su clave privada
5- David ya puede leer el mensaje original que le mandó Ana

SEGURIDAD INFORMATICA

Criptografía de Llave Pública

Ejemplo firma digital de clave asimétrica: David envía un mensaje a Ana

1- David redacta un mensaje
2- David firma digitalmente el mensaje con su clave privada
3- David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4- Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la clave pública de David
5- Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente

SEGURIDAD INFORMATICA

Criptografía de Llave Pública

La propagación de la confianza: (Puede darse como)

- **Infraestructura de clave pública o PKI.**
  - Entidades emisoras de certificados (Autoridades de certificación o CA del inglés Certification Authority)
- **Establecimiento de una web de confianza.**
  - No hay nodos aparte de los usuarios.
  - Los usuarios recogen claves públicas de otros usuarios y aseguran su autenticidad.
- **criptografía basada en identidad.**
  - PKG (acrónimo de Private Key Generator)
  - Hay un Generador que reparte las Caves Publicas y privada a quien corresponda.
- **Criptografía basada en certificados.**
  - En este modelo el usuario posee una clave privada y otra pública.
  - La clave pública la envía a una Autoridad de certificación que basándose en criptografía basada en identidad genera un certificado que asegura la validez de los datos.
- **criptografía sin certificados.**
  - KGC (acrónimo de Key Generator Center) es una clave parcial.
  - La clave privada completa se genera a partir de la clave privada parcial y un valor generado aleatoriamente por el usuario

SEGURIDAD INFORMATICA