

Infraestructura Computacional

# **Seguridad**

Francisco Rueda

Sandra Rueda

- *En este curso se estudian el proceso, las tareas y los criterios relevantes para el diseño de la infraestructura computacional requerida para responder a las necesidades de las organizaciones*

- *En este curso se estudian el proceso, las tareas y los criterios relevantes para el diseño de la infraestructura computacional requerida para responder a las necesidades de las organizaciones*
  - *¿Cómo influyen los requerimientos de seguridad en las características de la infraestructura computacional de una organización?*

# Seguridad

- Confidencialidad
- Integridad
- Disponibilidad

# Motivación

- Escuchamos con frecuencia sobre robos y fraudes cometidos por medio de Internet
  - Muchas compañías dependen de Internet para prestar un mejor servicio

## **Casi dos tercios de los usuarios de Internet son víctimas de fraude, según estudio**

Esto se debe a que las víctimas no están bien informadas y no suelen denunciar los crímenes.

Así lo afirmó el miércoles la empresa de seguridad Symantec, que hizo la investigación. Entre las personas encuestadas para este estudio, bautizado 'Norton Cybercrime report: the human impact' (Informe de Cibercrimen de Norton: el impacto humano), el 65 por ciento dijo haber sido víctima de criminalidad en Internet.

.....

Revista Enter, Septiembre 11 de 2010

<http://blogs.zdnet.com/security/?p=1012>

April 7th, 2008

## **The next big thing? Crimeware-as-a-service**

Posted by Larry Dignan @ 7:49 am

Finjan says Crimeware-as-a-Service (CaaS) is becoming an increasing problem and the ability of law enforcement to track malicious hackers will become increasingly hampered.

On Monday, Finjan's Malicious Code Research Center (MCRC) released its first quarter Web security trends report (registration required) and highlighted CaaS. finjan's release is timed for the RSA security conference in San Francisco.

The gist: "Criminals have started to use online cybercrime services instead of having to deal themselves with the technical challenges of running their own Crimeware server, installing Crimeware toolkits or compromising legitimate websites," says Finjan. In other words, it's point, click and hack.

What makes CaaS a big problem is that the service operators don't necessarily attack anything. These CaaS operators are basically arms dealers that provide customers with anti-forensic attack techniques and the ability to manage bot networks. Finjan has highlighted this trend before, but its report puts a little more meat on its research. posted by Larry Dignan @ 7:49 am

Finjan says Crimeware-as-a-Service (CaaS) is becoming an increasing problem and the ability of law enforcement to track malicious hackers will become increasingly hampered.



# **A través de la banca virtual, delincuentes han logrado robar \$100 mil millones este año**

Esa es una de las nuevas formas de delito que acosan a los colombianos, según la Policía.

El 'paquete chileno' se ha refinado y para 'embolatar' a sus víctimas los cacos se han vuelto expertos en el uso de lo último en tecnología. Las últimas trampas para hurtar dinero hacen parte de la lista de nuevas formas de delito que hoy acosan a los colombianos, según la Policía.

Van desde el fraude electrónico, las falsas ofertas vía teléfono celular (el smishing, trampas enviadas por mensajes de texto), el robo de identidad, hasta la venta ilegal de bases de datos, el espionaje industrial, los ataques con virus en sistemas, hacking o sabotaje y el ciberbulling (ciber-acoso) -que fue el origen del asesinato de una universitaria registrado recientemente en Bogotá- Algunos de esos delitos

El Tiempo Sábado 7 de noviembre de 2009 | eltiempo.com | Nación

y si se hace clic directamente sobre él, en vez de acceder a un formulario, el usuario lo que va hacer, es descargar un archivo ejecutable denominado "Formulario.exe" que muy probablemente contiene un virus, un *keylogger*, troyano, gusano, malware, etc.

Esta modalidad delictiva denominada *phishing* busca que usuarios desprevenidos entreguen información a los delincuentes, principalmente información personal y financiera, como cuentas bancarias y números de tarjetas de crédito. La Policía Nacional NUNCA solicita esta clase de información a la ciudadanía y cualquier requerimiento se realiza por los canales habituales de comunicación.

Con el fin de atender las inquietudes y dudas sobre este y otros incidentes de seguridad Informática, se ha dispuesto....

## Nasdaq fue atacado por ‘hackers’

Piratas informáticos violaron el año pasado la seguridad de la plataforma de negocios de la bolsa de Nasdaq en varias ocasiones. Así lo informó el diario *The Wall Street Journal*, que citó a fuentes que aseguraron que Nasdaq, la bolsa de valores electrónica en EEUU no se vio amenazada. Se señala como posibles motivos el robo de información o intentos por plantear una amenaza a la seguridad nacional a través de un ataque a gran escala

A Nasdaq

.....

.....

**El Tiempo 6 de Febrero de 2011**

## **'Ciberatracos' en todo el país crecieron un 96 por ciento**

Cuando se dice que en el 2010 se robaron en Colombia alrededor de **3.000** millones de pesos por medios electrónicos la cifra puede parecer no muy alta a la luz de la magnitud del dinero que se mueve en el sistema financiero, pero cuando se advierte que esa suma es sólo de los casos que se denuncian, el problema toma otras dimensiones.

.....

.....

**El Tiempo 6 de Febrero de 2011**





# DAVIVIENDA

## **Estimado Cliente.**

Le informamos que su servicio en línea ha sido bloqueado.

Como parte de la seguridad e integridad de nuestros servicios, le enviamos este mensaje de alerta, comunicándole que sus servicios bancarios en línea se encuentran suspendidos debido a que presenta intentos fallidos para acceder a su cuenta.


Esta es una medida preventiva implementada por nuestra entidad para prevenir el acceso no autorizado, evitar la pérdida, mal uso, alteración y hurto de sus datos personales.

Para desbloquear su servicio en línea, acceda a su cuenta de inmediato y desbloquee con la segunda clave de seguridad. El bloqueo se eliminará de manera inmediata y usted podrá seguir disfrutando de todos nuestros servicios.

**Entre aquí para realizar dicho proceso:**



**GRUPO EMPRESARIAL BOLIVAR,  
Av. El Dorado No. 68 C - 61 Bogotá D.C. Colombia  
Conmutador: 3 30 00 00 Fax : 2 85 79 61 Apartado Aereo : 6944  
Nit. 860.034.310 - 7 Código País 1075**



## Atención !

La página a la cual intenta conectarse ha sido detectada como fraudulenta, es una copia de la original en donde se busca capturar su información confidencial, esto es conocido como phishing.

**Por su seguridad hemos restringido el acceso a ese sitio.**

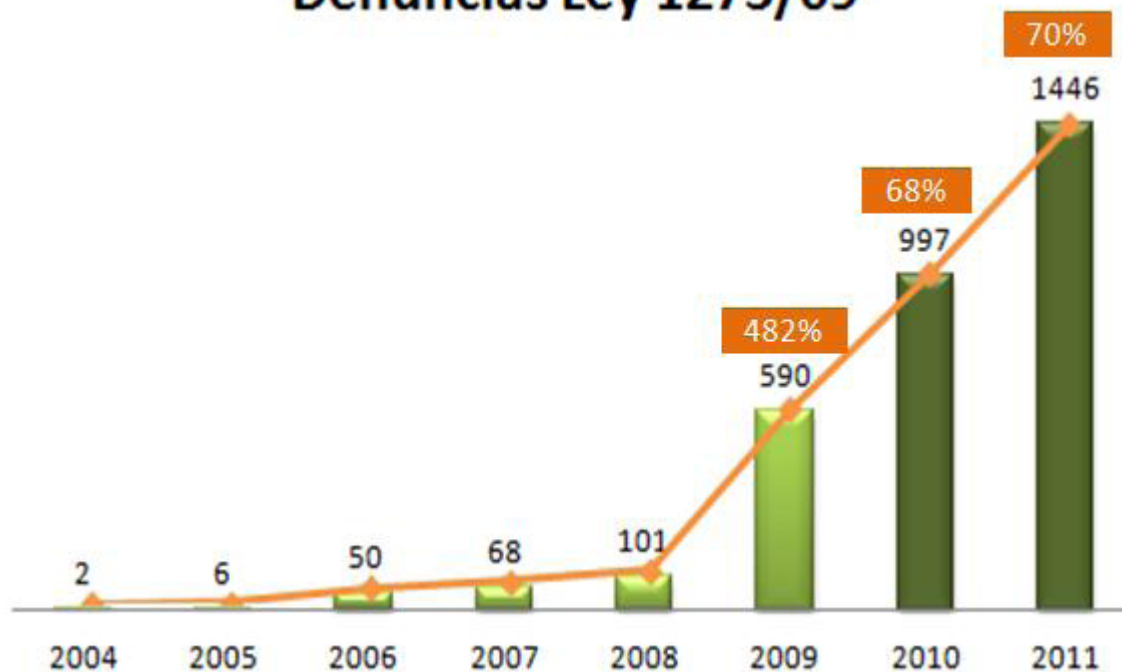
Para mayor información sobre el phishing y asuntos de seguridad informática en general, visite nuestra [Zona de Seguridad](#).



© ETB S.A. ESP. Todos los derechos reservados.



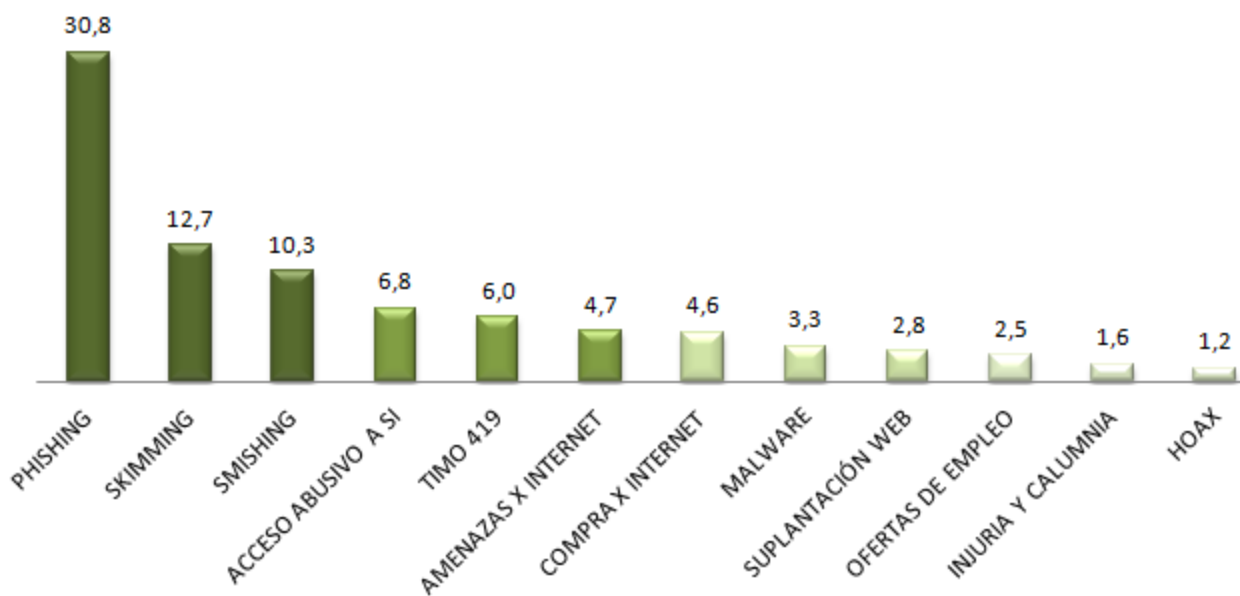
## Denuncias Ley 1273/09



Coronel Fredy Bautista, 2 Foro de Computación móvil Uniandes, 2012



### CAI Virtual denuncias recibidas - %



Coronel Fredy Bautista, 2 Foro de Computación móvil Uniandes, 2012

# Estadísticas

	2009-2010*
<b>Prevalencia:</b> Empresas afectadas por el fraude	94%
<b>Áreas de pérdida frecuente:</b> Porcentaje de empresas que informaron pérdidas por este tipo de fraude	Fraude de vendedores, proveedores o de adquisición (24%) Robo, pérdida o ataques de información (21%) Conflictos de interés de la gerencia (18%) Fraude de regulación o cumplimiento (15%)
<b>Enfoque de la Inversión:</b> Porcentaje de empresas que invierten en la prevención de este tipo de fraude	PI y programa de monitoreo de marcas (91%) Monitoreo de reputación (85%) Capacitación del personal (82%) Sistemas de gestión de riesgos (76%) Controles financieros (73%) Seguridad de TI (73%) Controles de la gerencia (73%) Investigación de antecedentes del personal (73%) Seguridad de activos físicos (70%) Due diligence (70%)
<b>Aumento en la Exposición:</b> Empresas en las que la exposición al fraude ha aumentado	88%
<b>Mayores Motores del Aumento de la Exposición:</b> Factor más generalizado que lleva a mayor exposición al fraude y porcentaje de empresas afectadas	Alta rotación de personal (42%)

\*Encuestados insuficientes en el 2009 para proporcionar datos comparativos.

Informe Global sobre Fraude, Kroll - Economist Intelligence Unit, 2010-2011 - Colombia

# Estadísticas

Gráfico 1. Porcentaje de empresas que reportan fraudes indicados en los últimos 12 meses

	2010	2009
Robo, pérdida o ataques de información	27.3%	18%
Robo de activos físicos o inventario	27.2%	28%
Conflictos de interés de la gerencia	19%	20%
Fraude de vendedor, proveedor o adquisiciones	15%	12%
Fraude o robo financiero interno	13%	14%
Mala gestión financiera	13%	12%
Violación de reglamentación o cumplimiento	12%	17%
Corrupción y soborno	10%	12%
Robo de propiedad intelectual, piratería o falsificación	10%	8%
Lavado de dinero	6%	3%

Informe Global sobre Fraude, Kroll - Economist Intelligence Unit, 2010-2011 - [Global](#)

# Medidas Preventivas

- Virus
- Phishing
- Robos de información
- Suplantación
- ...

# Medidas Preventivas

- Niveles:
  - Directivo
    - Organizacional y de procesos
  - Operativo
    - Medidas técnicas y controles

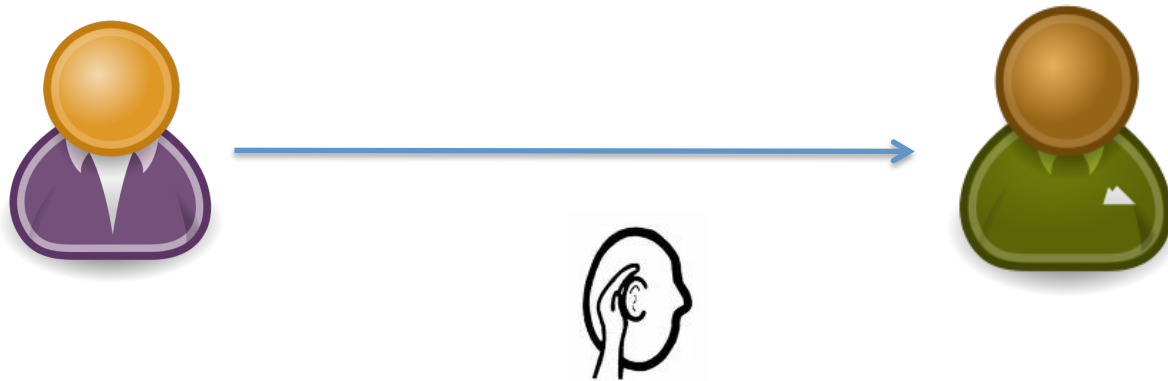
# Nivel Directivo

- Política
- Análisis e implementación de políticas enmarcados en metodologías y estándares
  - ISO 27001
  - Circular 052

# Principales Problemas

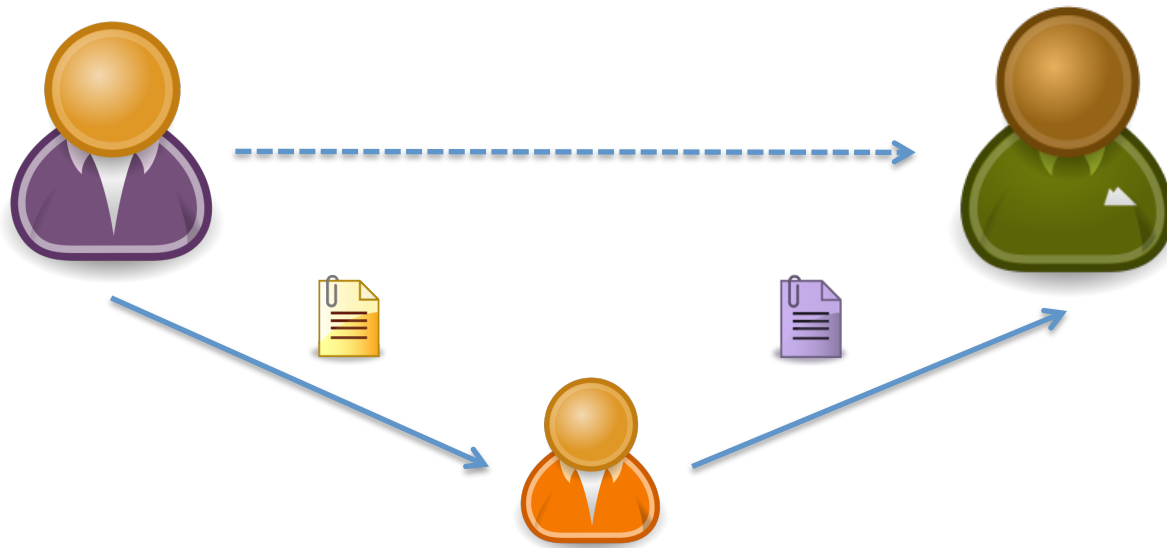
- Espionaje
- Adulteración
- Suplantación
- Repudio

# Espionaje

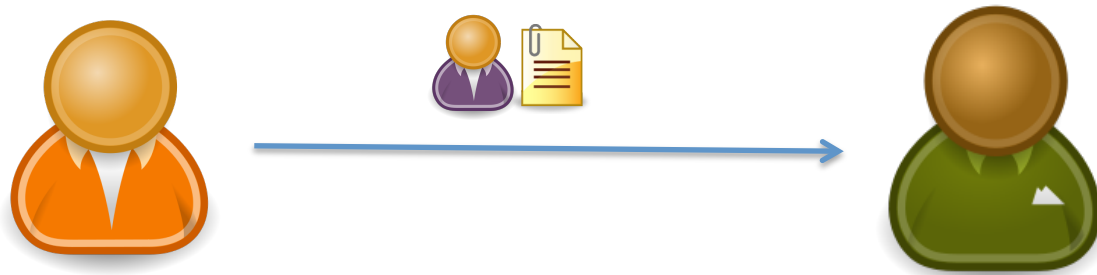




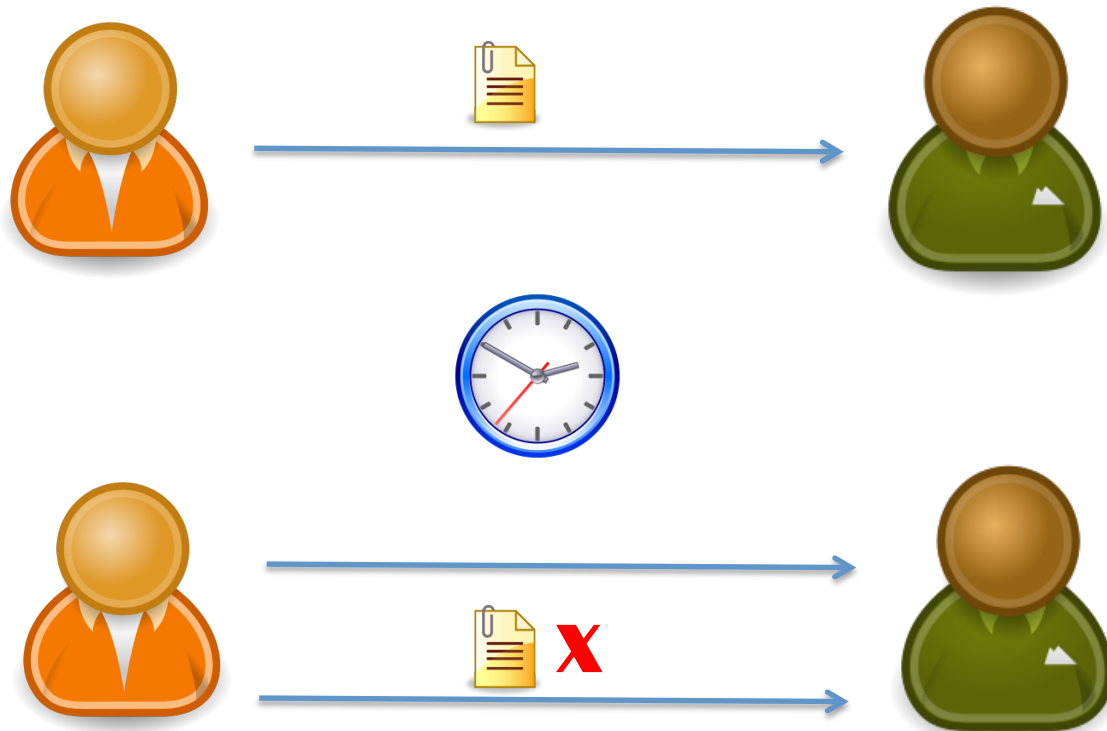
# Adulteración



# Suplantación



# Repudio



# Implementación

- Criptografía
  - Algoritmos de cifrado simétrico
  - Algoritmos de cifrado asimétrico

# Cifrado Simétrico

- Se usa la misma llave para cifrar y para descifrar



# Cifrado Simétrico

- El algoritmo es público pero la llave es secreta
- Solo las dos partes que se quieren comunicar conocen la llave
- Las llaves deben ser largas para evitar que las descubran
  - Un ataque de fuerza bruta explora todos los valores posibles de una llave

# Tamaño de la Llave

Año	A. Simétrico	Hash	A. Asimétrico
2000	70	140	952
2002	72	144	1028
2004	73	146	1108
2006	75	150	1191
2008	76	152	1279
2010	78 → 112	156 → 256	1369 → 2048
2020	86	172	1881
2030	93	186	2495

Swaminatha 2003 –  
NIST Recommendation for Key Management 2012

# Tamaño de Llave

- Tiempo requerido con ensayos exhaustivos para descifrar una llave

Tam. Llave	Llaves	Tiempo (1)	Tiempo (2)
32 bits	$2^{32}$	35.8 min	.15 ms
56 bits	$2^{56}$	1142 años	10.01 h
128 bits	$2^{128}$	$5.4 \times 10^{24}$ años	$0.4 \times 10^{18}$ años
168 bits	$2^{168}$	$5.9 \times 10^{36}$ años	$9 \times 10^{30}$ años

**(1) Suponiendo 1 operación por  $\mu s$**

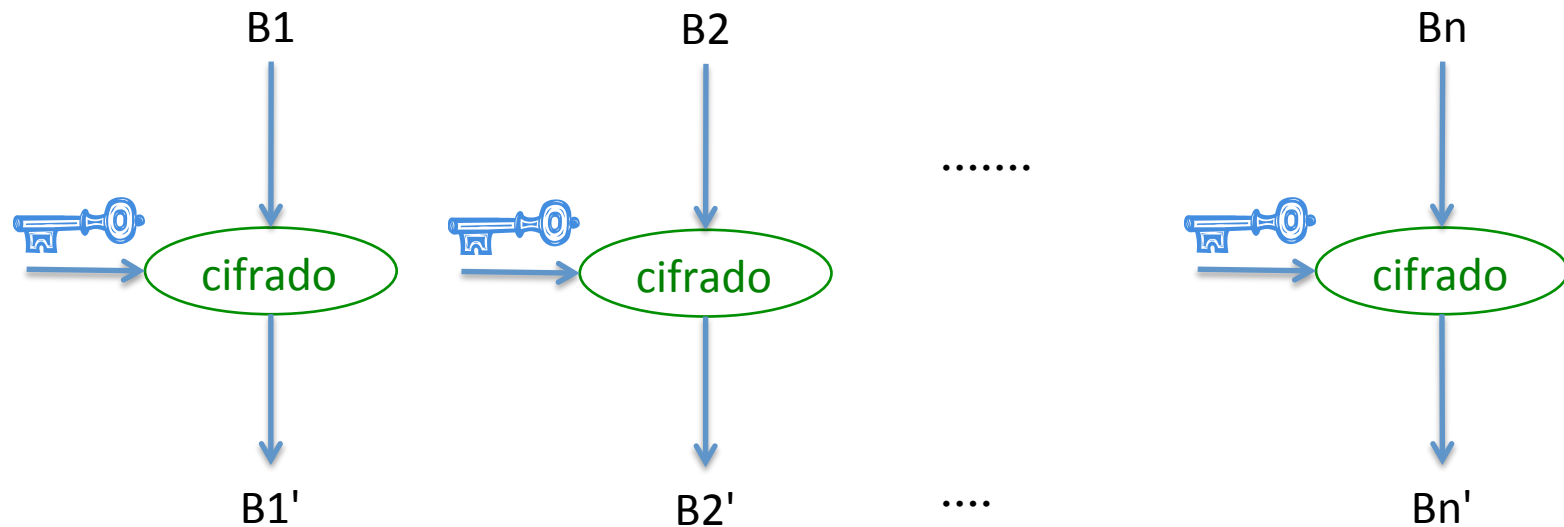
**(2) Suponiendo  $10^6$  operaciones por  $\mu s$**

[Stallings]



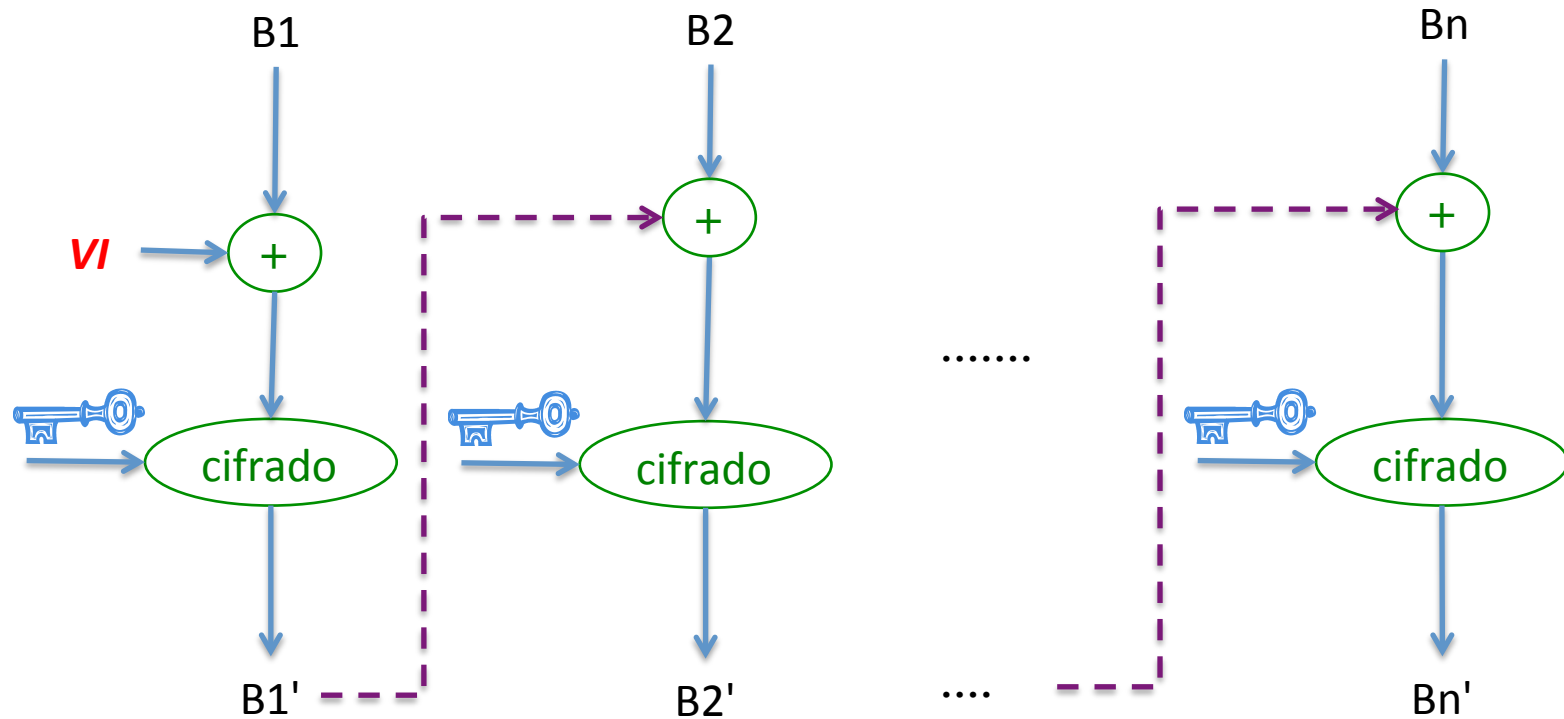
# Cifrado por Bloques

- ECB (Electronic Codebook)

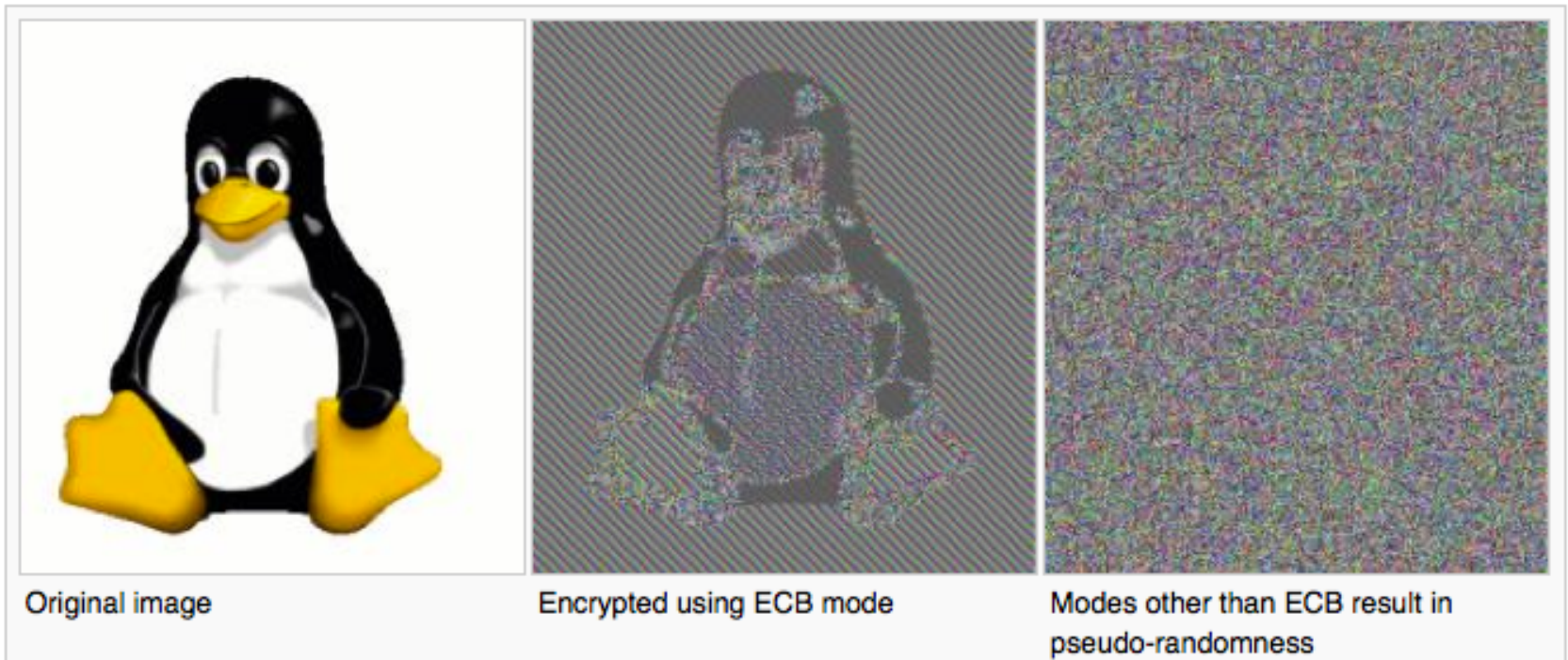


# Cifrado por Bloques

- CBC (Cipher-block chaining)



# ECB vs. CBC



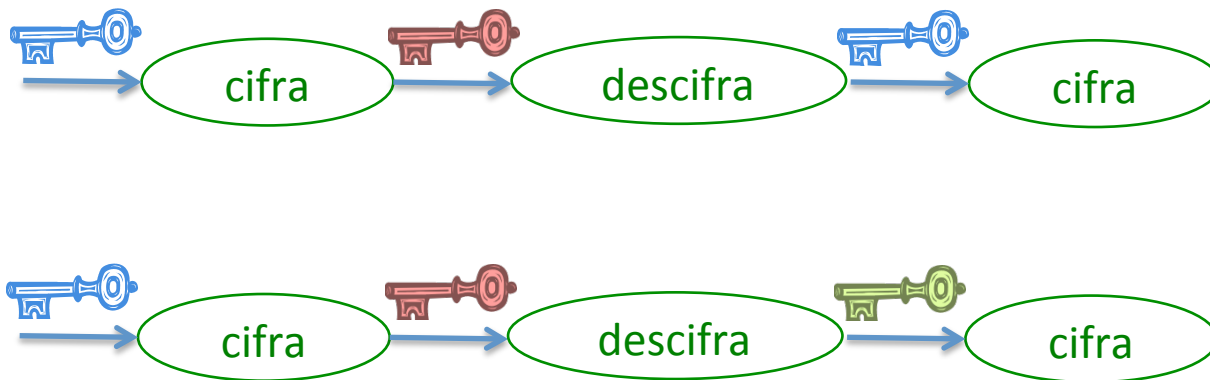
[[http://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation](http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)]

# Cifrado por Bloques

- Data Encryption Standard – DES
  - Amplia difusión
  - Maneja bloques de 64 bits y llaves de 56 bits
  - DES ya fue vulnerado por lo que no se considera seguro en la actualidad
    - Aunque en algunos contextos puede ser apropiado

# Cifrado por Bloques

- 3DES
  - Llaves de 168 bits ( $56 \times 3$ )
  - Trabaja en tres fases



# Cifrado por Bloques

- AES
  - Llaves de 128, 192 y 256
  - Bloques de 128 bits
- Blowfish
  - Llaves de 32 a 448 bits
- RC5
  - Llaves de hasta 2040 bits

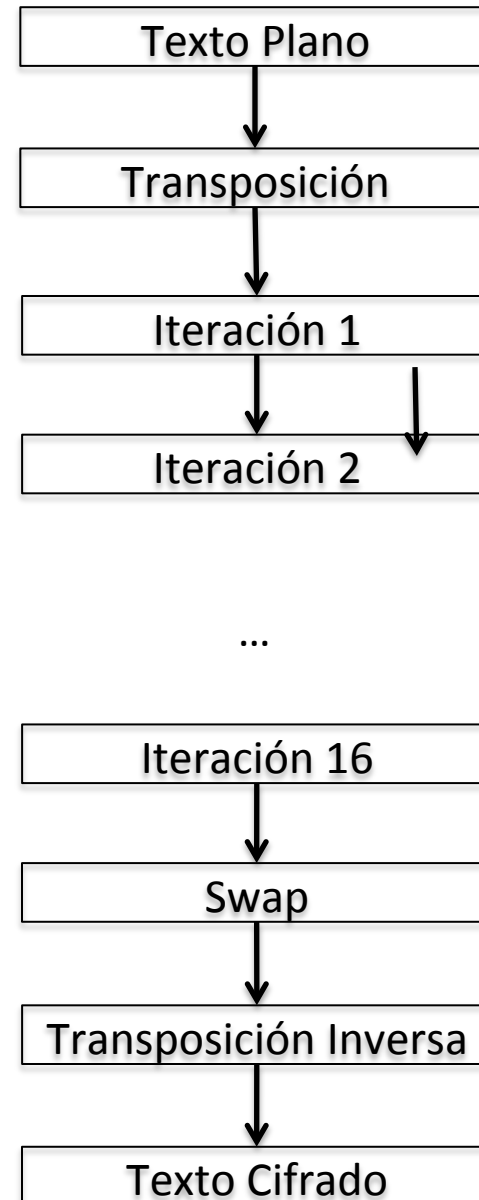
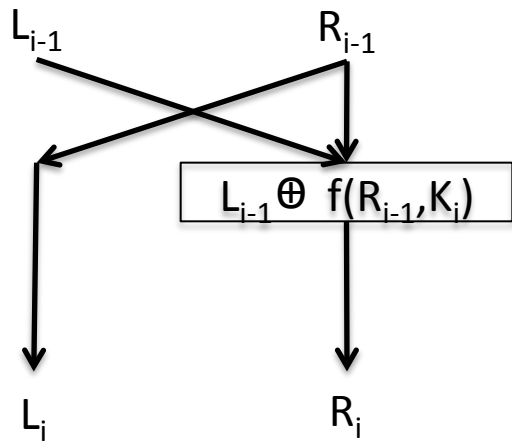
# Algoritmos de Cifrado por Bloques

## Comparación de algoritmos por bloques en un Pentium

Algoritmo	Ciclos de reloj por ronda	Rondas	Ciclos de reloj por byte
Blowfish	9	16	18
RC5	12	16	23
DES	18	16	45
3DES	18	48	108

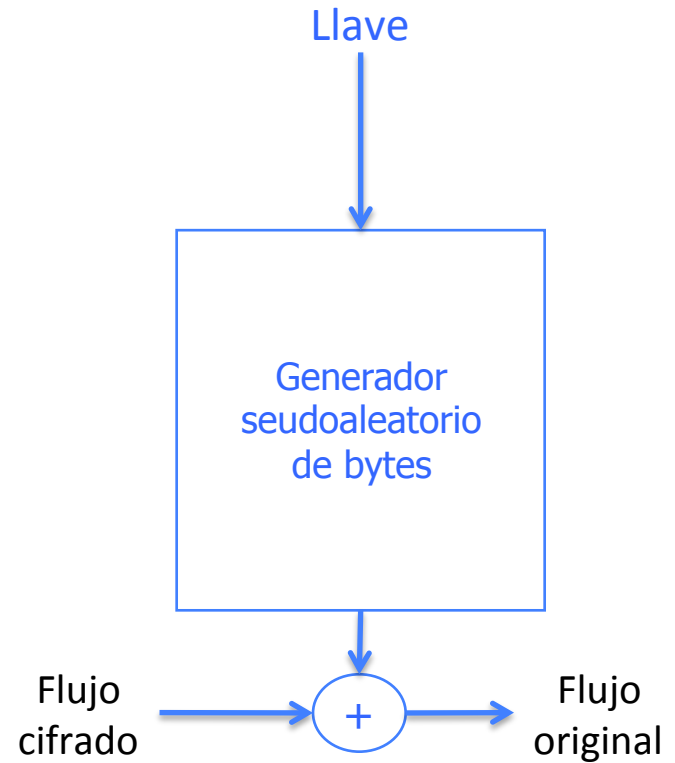
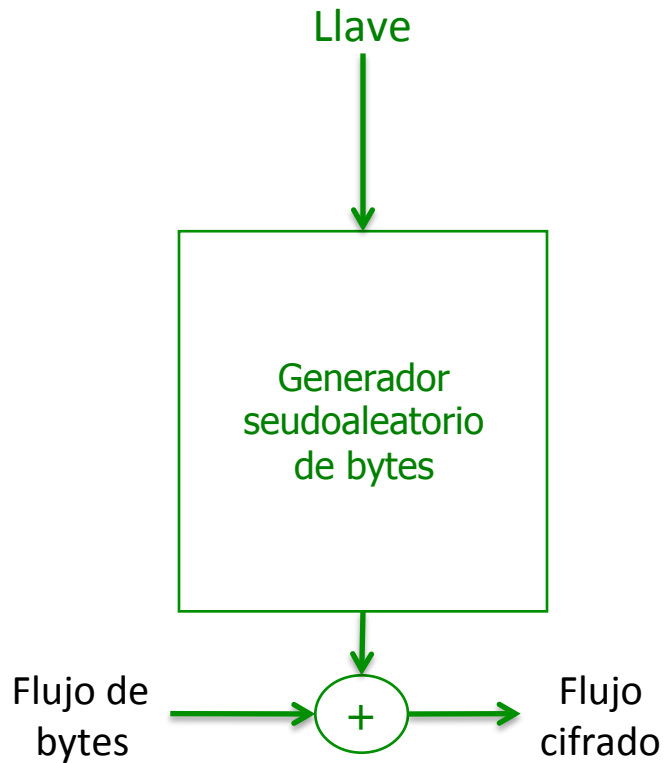
[Stallings 2003]

# Rondas DES





# Cifrado por Flujo



# Velocidad

Comparación de velocidad de algoritmos simétricos  
-por bloques y por flujo-  
en un Pentium II

Algoritmo	Tamaño de Llave	Velocidad (Mbps)
DES	56	9
3DES	168	3
RC4	Variable	45

[Stallings]

# Cifrado Simétrico

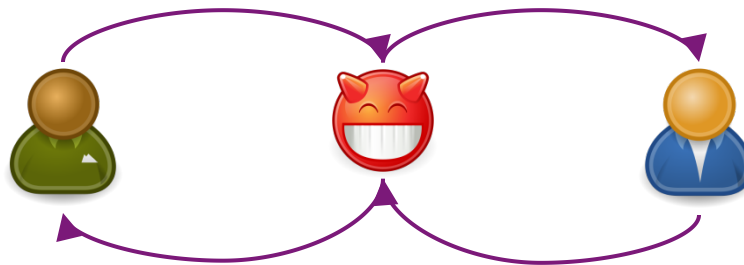
- Las partes deben
  - usar un mecanismo seguro para acordar la llave
  - almacenar la llave para evitar que otros tengan acceso

# Diffie-Hellman

- Algoritmo para acordar una llave compartida con un medio inseguro
  - Escoja un número primo  $p$  y una base  $g$  ( $<p$ )
  - Cada individuo escoge un valor  $x$  ( $<p-1$ )
  - Cada individuo genera  $y$  y comunica:
    - $y = g^x \bmod p$
  - Cada individuo genera la llave secreta  $z$ :
    - $z = y^x \bmod p$
  - Ejercicio con el vecino
    - siga los pasos con  $p=7$  y  $g=4$

# Diffie-Hellman

- El protocolo no autentica
  - Como no autentica, es posible el ataque conocido como hombre en el medio (man in the middle)
  - El hombre en el medio negocia llaves con cada participante. Los participantes creen que están negociando una llave entre ellos



# Cifrado Simétrico

- Aunque no tanto como en el caso del cifrado asimétrico, hay una cierta sobrecarga asociada con el cifrado simétrico, lo cual es especialmente crítico en dispositivos con recursos limitados
  - Teléfonos celulares y dispositivos móviles en general
  - Batería, memoria, capacidad de cómputo

# Dispositivos con Recursos Limitados

- Los dispositivos poco potentes pueden ayudarse de otros (pero de todas maneras es importante conocer los costos de procesamiento de los algoritmos)

# Desempeño

## Desempeño de algoritmos simétricos 2.1 GHz Pentium 4

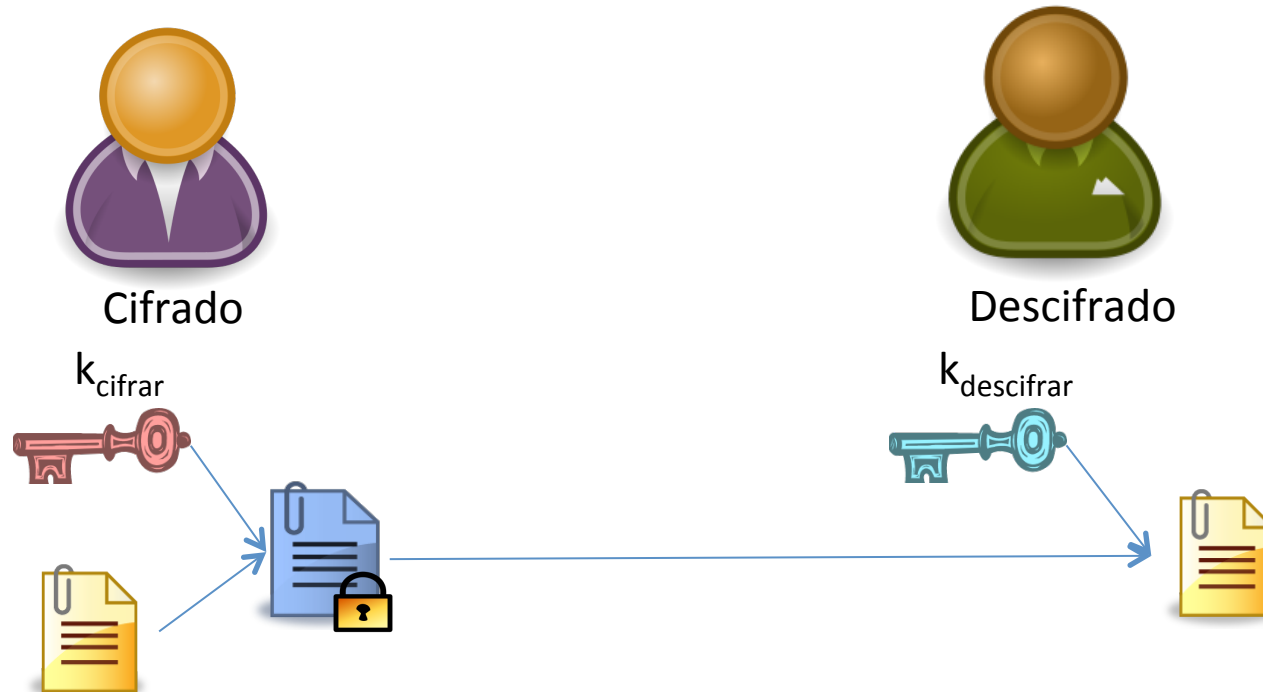
Algoritmo	Tamaño de Llave	Velocidad (Mbytes/s)
DES	56	21.340
3DES	112	9.848
AES	128	61.010
AES	192	53.145
AES	256	48.229

[Coulouris]



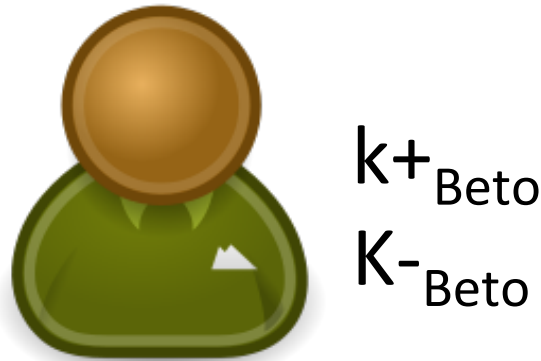
# Cifrado Asimétrico

- Llaves diferentes para cifrar y descifrar



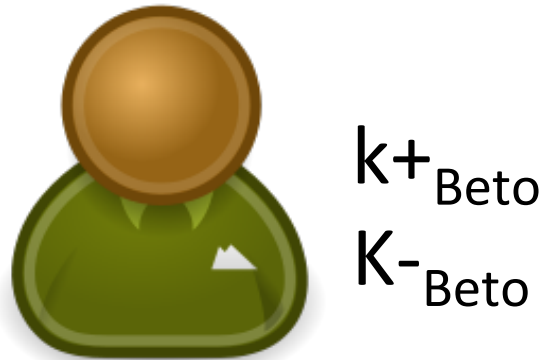
# Cifrado Asimétrico

- Cada entidad tiene dos llaves:
  - Llave pública ( $k^+$ )
  - Llave privada ( $k^-$ )
- Lo que se cifra con una llave pública solo puede ser descifrado con la llave privada correspondiente y viceversa



# Cifrado Asimétrico

- Solo el propietario conoce su llave privada  $K^-$
- Quienes quieran pueden obtener la llave pública  $K^+$



# Cifrado Asimétrico

$$M' = M^E \bmod N$$



Llave = (E,N)

$$M = M'^D \bmod N$$



Llave = (D,N)

# RSA

- Algoritmo para generación de llaves
  - Se basa en propiedades de aritmética módulo  $n$ 
    - Escoja dos número primos  $p$  y  $q$  grandes
    - Calcule  $n = p * q$
    - Escoja  $e$  tal que  $e$  es un primo relativo de  $\phi(n)$ 
      - $\phi(n) = (p-1)*(q-1)$
      - $d = e^{-1} \bmod \phi(n)$  o  $d * e \bmod \phi(n) = 1$
  - Ejemplo
    - $p = 3, q = 11$  y  $e = 7$

$$d = 3$$

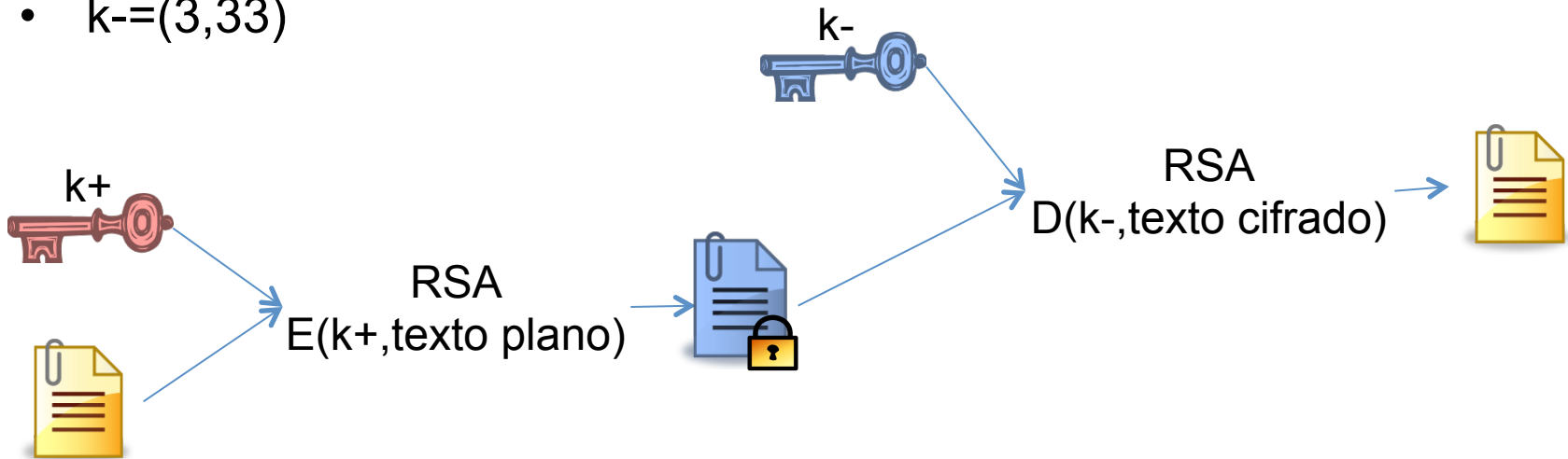
$$n = 33$$

$$\phi(n) = 20$$

Usamos números  
pequeños, solamente para  
facilitar los cálculos

# RSA

- $k^+ = (7, 33)$
- $k^- = (3, 33)$



$$E(\{7, 33\}, 4) = 4^7 \bmod 33 = 16384 \bmod 33 = 16$$

$$D(\{3, 33\}, X) = 16^3 \bmod 33 = 4096 \bmod 33 = 4$$

$$(y^e)^d = y \bmod n$$

# Llaves

- Se usan primos mayores a  $10^{100}$
- Solo el dueño conoce la llave privada
- Cualquiera puede obtener la llave pública
- Cualquiera de las dos sirve para cifrar y se debe descifrar con la otra
- Conviene usar algoritmos de cifrado asimétricos solo cuando sea necesario pues son más costosos en tiempo de cómputo

# Cifrado Simétrico y Asimétrico

Cifrado con llave secreta o simétrica	Cifrado con llaves pública-privada o asimétricas
Es rápido	Es lento
Supone que las dos entidades involucradas (y solo ellas) conocen la llave secreta	No requiere secretos compartidos
Requiere un mecanismo previo para acordar la llave	Requiere un mecanismo para obtener la llave pública



# Desempeño

Algoritmos simétricos  
2.1 GHz Pentium 4

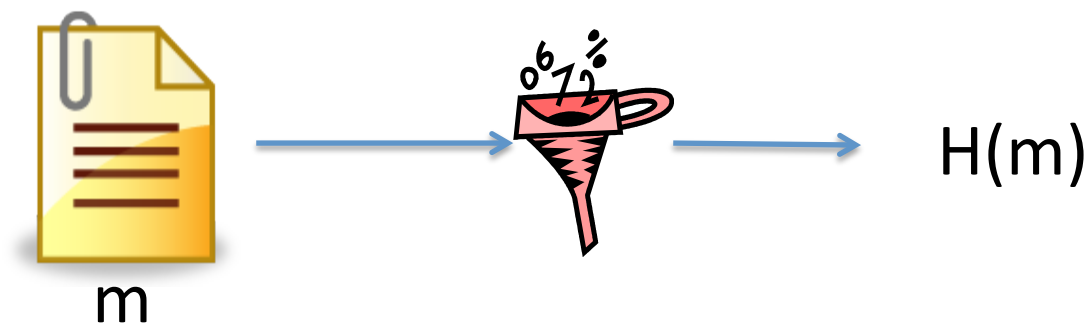
Algoritmo	Tamaño de Llave	Velocidad (Mbytes/s)
DES	56	21.340
3DES	112	9.848
AES	128	61.010
AES	192	53.145
AES	256	48.229

Los algoritmos asimétricos no se usan para cifrar, en general, pero si para firmar.

Algoritmo	Tamaño de Llave	Tiempo de Respuesta
RSA	1024	160 Bits Hash 0.18 ms

# Resumen Digital (digest)

- Una función de resumen, también conocida como función de hash o digest, toma un mensaje de longitud arbitraria y calcula un número de longitud fija



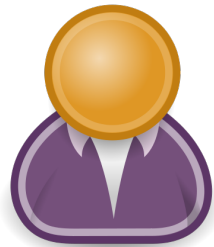
# Propiedades de la Función

- Es fácil calcular  $H(m)$
- Dado  $H(m)$ , no es fácil calcular  $m$ .
  - Aunque si se conoce el dominio de la función es posible evaluar  $H(m)$  para todos los valores posibles de  $m$
  - *Es difícil encontrar el inverso*
- Es computacionalmente difícil encontrar  $m_1$  y  $m_2$  tal que  $H(m_1) = H(m_2)$



# Uso

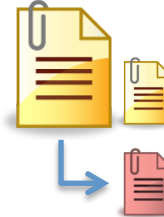
- Integridad de datos



$M + H(M)$

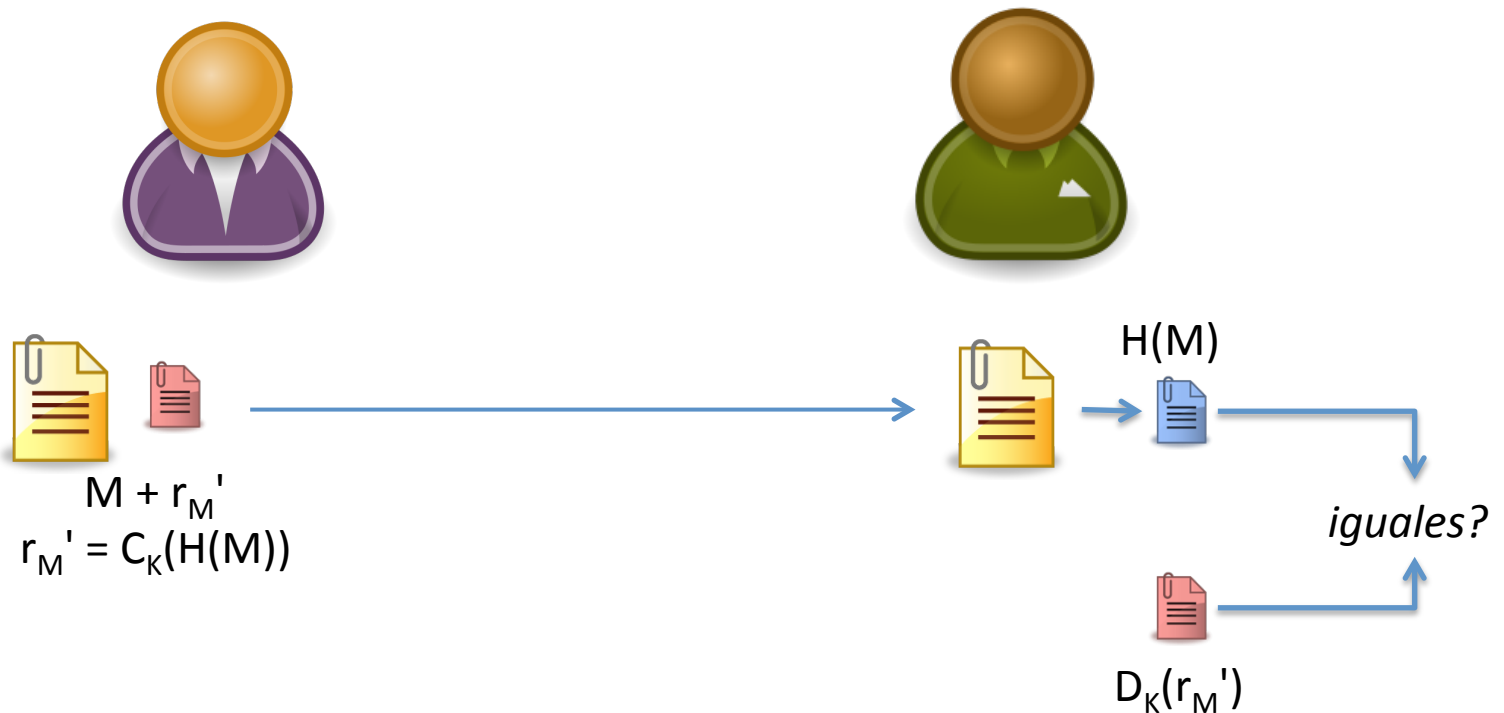


$H(M)$  recibido =  
 $H(M)$  calculado ?

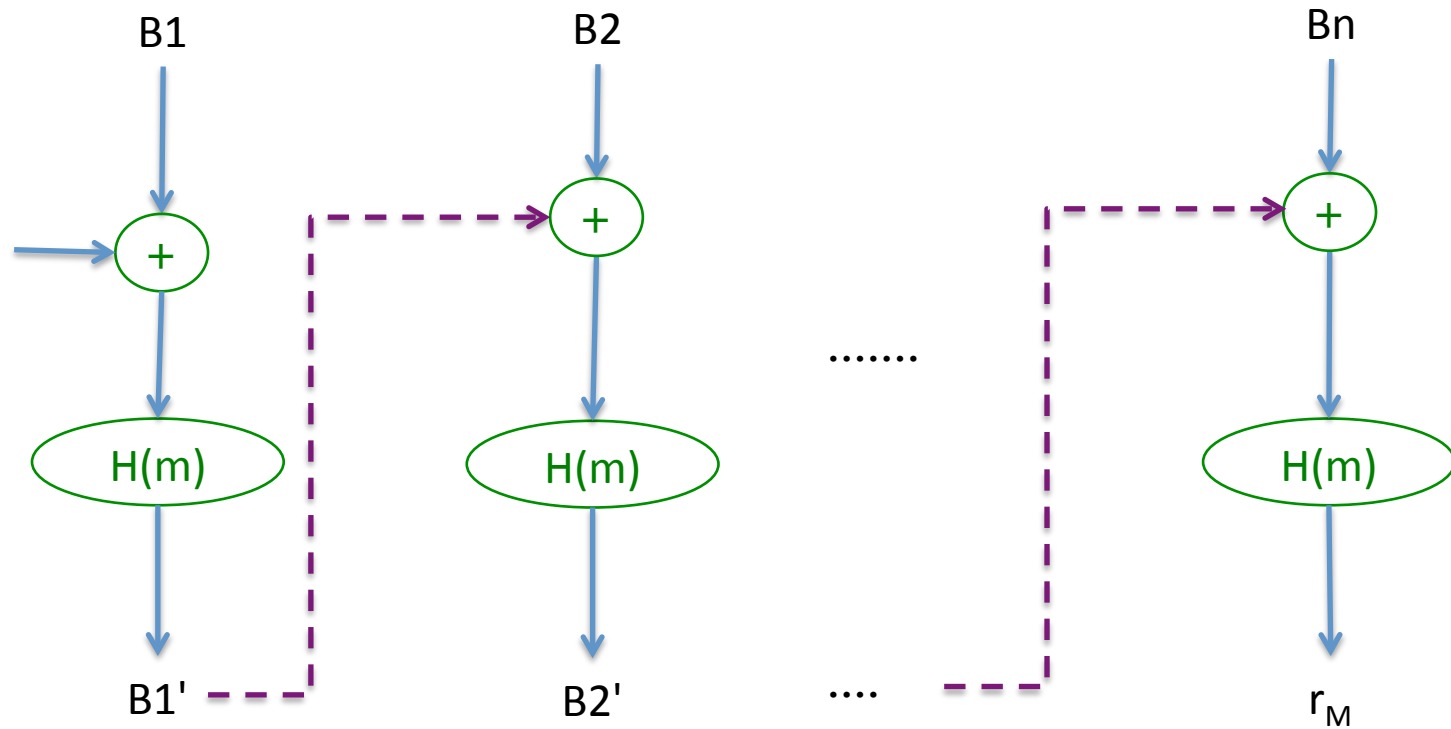


# Uso

- Integridad de datos



# Procedimiento



# Colisiones

- ¿Qué puede pasar si la función produce el mismo código de resumen para dos mensajes distintos?

# Algoritmos

- Algunos de los métodos más conocidos para elaborar resúmenes son
  - MD4 y MD5, que producen resúmenes de 128 bits,
  - SHA que produce resúmenes de 160 bits
  - RIPEMD que produce digests de 128 y 160 bits
  - También existen SHA-224, SHA-256, SHA-384 y SHA-512 que producen resúmenes más largos (224, 256,..)



# Desempeño

## Algoritmos de generación de resúmenes 2.1 GHz Pentium 4

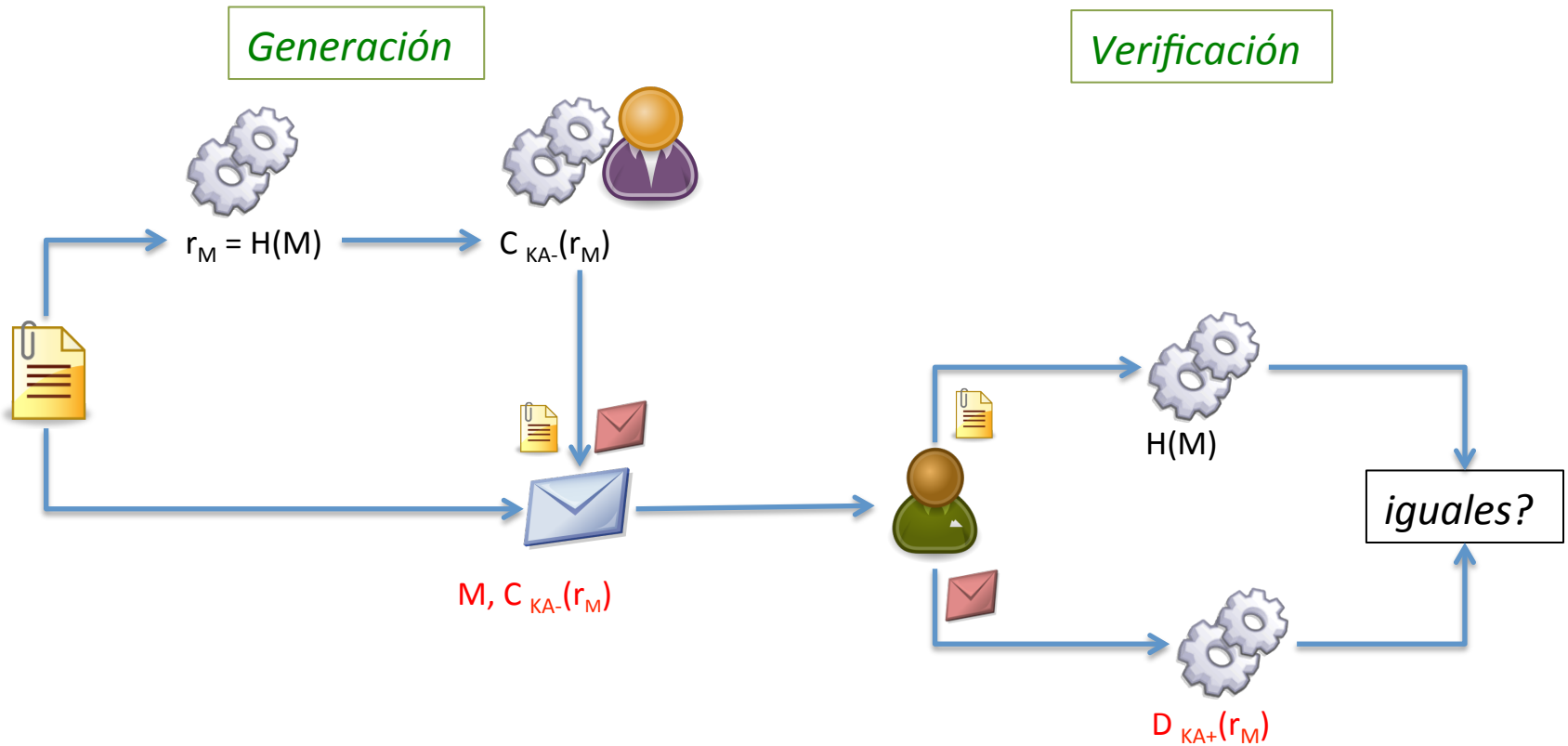
Algoritmo	Tamaño de Llave	Velocidad (Mbytes/s)
DES	56	21.34
3DES	112	9.848
MD5	128	216.67
SHA	160	67.97

Coulouris2001

# Firma Digital

- Se quiere evitar falsificaciones
  - El destinatario puede verificar la identidad del remitente del mensaje
  - El remitente no puede repudiar el contenido del mensaje
  - El destinatario no puede haber creado el mensaje
- Respuesta:
  - Firmas digitales
    - basadas en algoritmos de cifrado con llaves públicas

# Firma Digital



# Garantías

- El remitente firmó el mensaje:
  - Confidencialidad e integridad
  - Autenticación de la fuente
  - No-repudio
    - Si hay una marco legal vigente, el receptor puede tomar el mensaje y probar que fue enviado por el remitente

# Firma Digital

- Se recomienda usar llaves de tamaño 160 para el resumen y de 1024 para la llave asimétrica
- Para el futuro se recomienda usar llaves de 224 para el resumen y de 2432 para la llave asimétrica

# Firma Digital

- Usualmente se firma el resumen, no el mensaje
  - Eficiencia
- A diferencia de la firma manuscrita, la firma digital está asociada con el documento
  - Si el documento cambia, la firma cambia

# Firma Digital

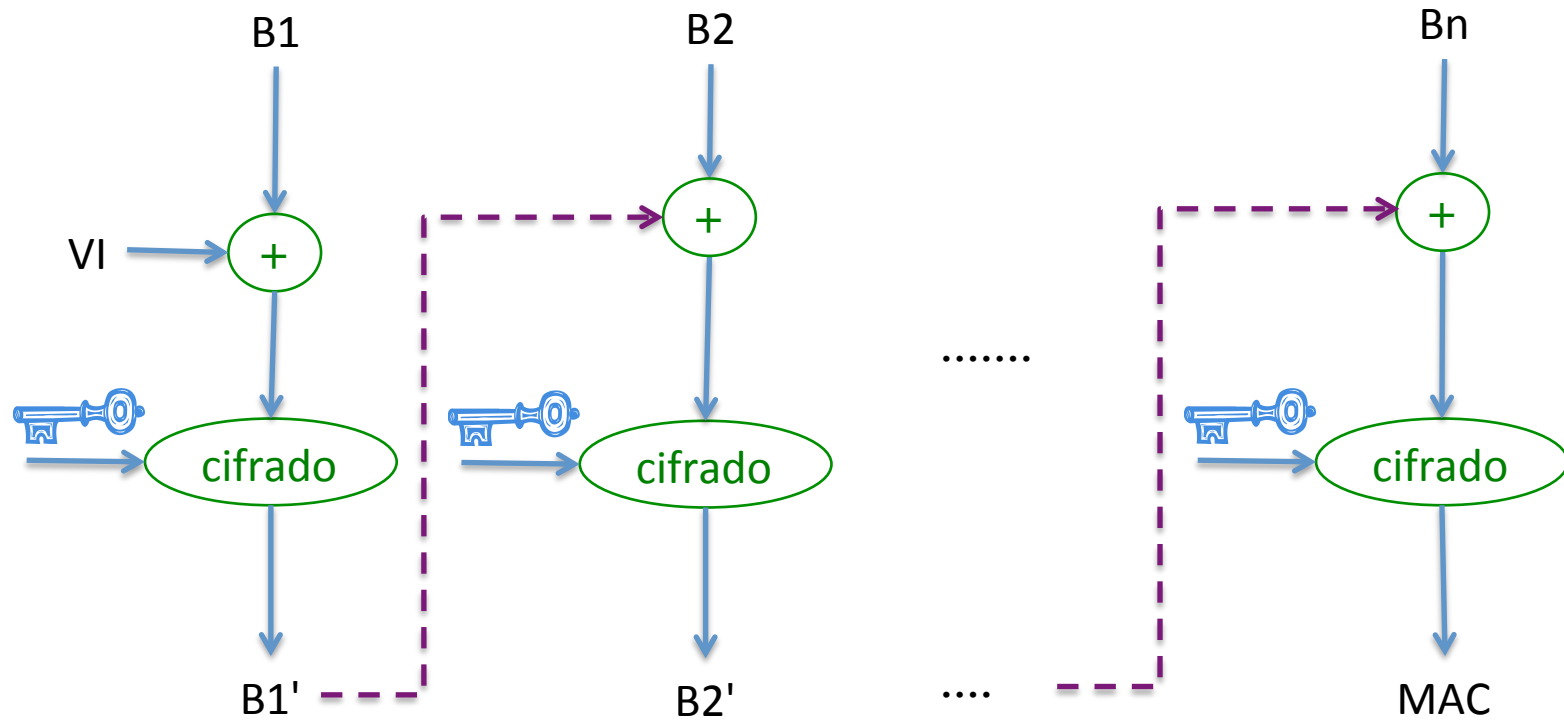
- No se recomienda usar MD5 pues genera colisiones y no es muy resistente a ataques
- SHA-1 no es muy seguro porque genera colisiones.
  - No se recomienda para generar firmas digitales
  - Es efectivo para generar códigos HMAC

# Códigos HMAC

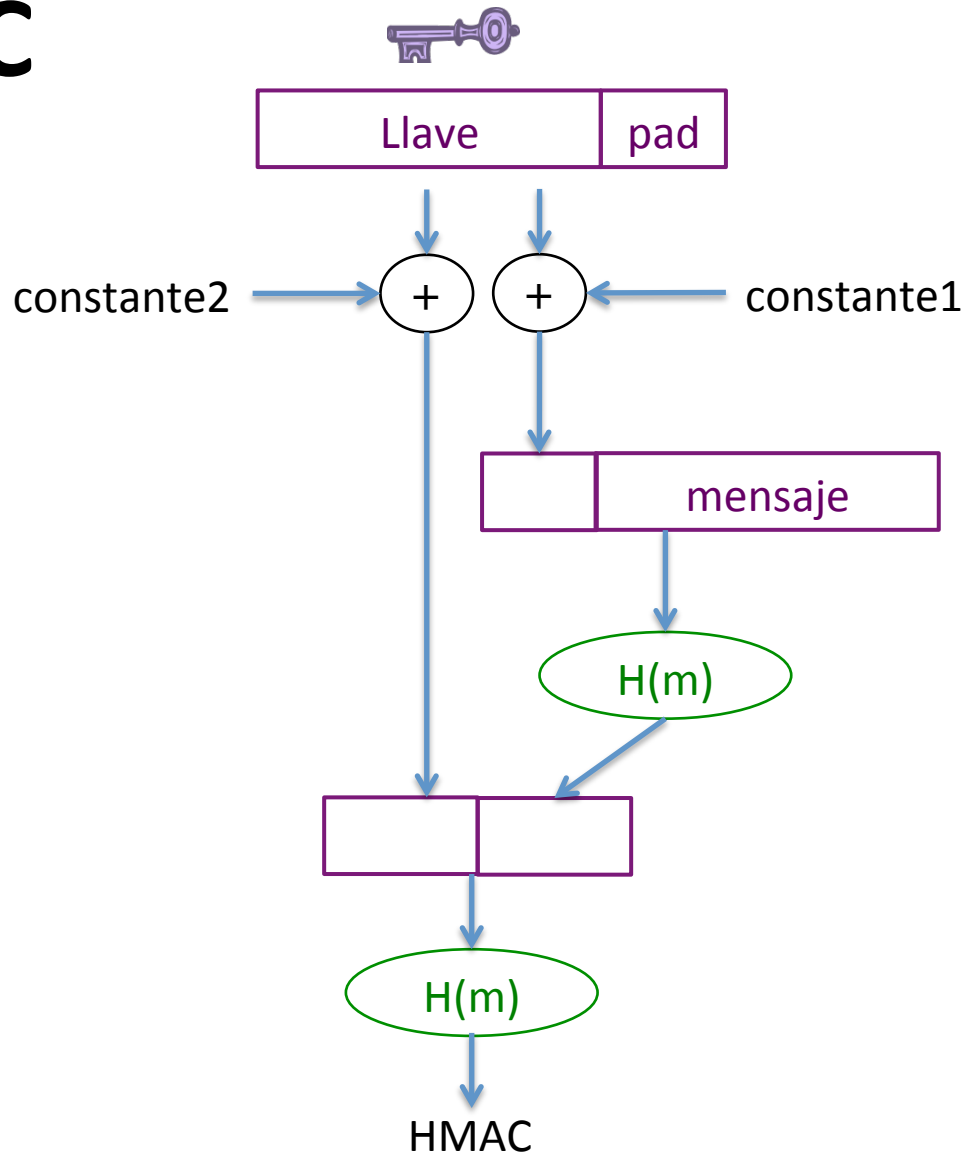
- Es posible usar un resumen digital para autenticación
  - Message Authentication Code
  - Hashed Message Authentication Code
- Procedimiento
  - Cifrar el resumen digital
  - Usar una llave para producir el resumen



# MAC



# HMAC



# MAC y HMAC

- El tiempo para producir un HMAC es ligeramente superior al necesario para obtener un resumen
- Descubrir la llave a partir del mensaje y el MAC es un proceso dispendioso
  - Se debe conocer el dominio de la función
  - Habría que evaluar todas las posibles llaves en ese dominio

# Referencias

- [NIST2002] *Risk Management Guide for Information Technology Systems*. NIST, 2002.
- [NIST2012] *Recommendation for Key Management*. NIST, 2012.
- [ForoUniandes2012] *Segundo Foro de Computación Móvil*. Uniandes, 2012.
- [Stallings2003] *Cryptography and Network Security*. William Stallings. Prentice Hall, 2003.
- [Swaminatha2003] *Wireless Security and Privacy*. Tara Swaminatha y Charles Elden. Addison-Wesley, 2003.
- [Coulouris2005] *Sistemas Distribuidos: conceptos y diseño*. George Coulouris, Jean Dollimore y Tim Kindberg. Addison-Wesley, 2005.
- [Martinez2007] A Survey of Electronic Signature Development in Mobile Devices. Martínez, Sánchez, Ruiz, Gómez. Journal of Theoretical and Applied Electronic Commerce Research. 2007.