

CRIPTOLOGÍA CON CRYPTOOL v 1.4.30

**Introducción a la
Criptografía y al Criptoanálisis**

Alcance, Tecnología y Futuro de CryptTool

Prof. Bernhard Esslinger y el equipo de CryptTool, Agosto 2010

www.cryptool.org
www.cryptool.com
www.cryptool.de
www.cryptool.es
www.cryptool.pl

Contenido (I)

I. CrypTool y Criptología – Visión General

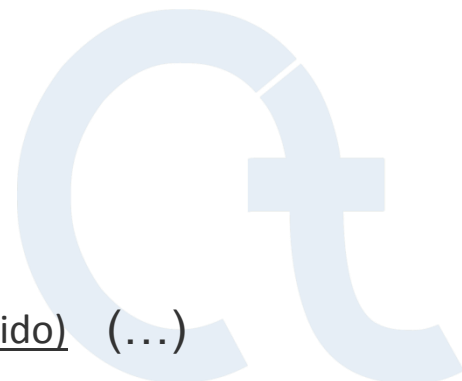
1. Definición y relevancia de la Criptología
2. El Proyecto CrypTool
3. Ejemplos de métodos clásicos de cifrado
4. Conocimientos sobre el desarrollo de la criptografía

II. Características de CrypTool

1. Visión General
2. Ejemplos de Interacción
3. Desafíos para los desarrolladores

III. Ejemplos

1. Cifrado con RSA / Test de primalidad / Cifrado Híbrido y certificados digitales
2. Visualización de firma digital
3. Ataque al cifrado RSA (modulo N demasiado pequeño)
4. Análisis del cifrado de la PSION 5
5. Claves DES débiles
6. Localizar información de la clave (“clave NSA”)
7. Ataque a la firma digital por localización de colisiones hash
8. Autenticación en un entorno cliente-servidor
9. Demonstración de un ataque de canal lateral(en un protocolo de cifrado híbrido) (...)



Contenido (II)

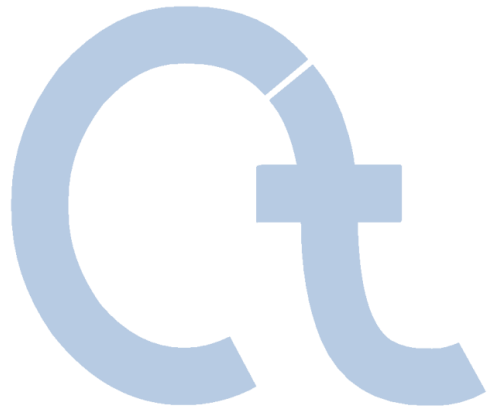
III. Ejemplos

10. Ataque RSA utilizando reducción de retículos (Lattice Reduction)
11. Análisis de aleatoriedad con visualización 3-D
12. Secreto Compartido (Teorema Chino de los Restos (CRT) / Shamir)
13. Implementación del CRT en Astronomía
14. Visualización del cifrado utilizando ANIMAL
15. Visualización del AES
16. Visualización del cifrado Enigma
17. Visualización de E-mail seguro con S/MIME
18. Generación de un código de autenticación de un mensaje (HMAC)
19. Demo Hash
20. Herramienta de aprendizaje de teoría de números y cifrado asimétrico
21. Suma de puntos en curvas elípticas
22. Medidor de calidad de contraseñas
23. Análisis por Fuerza Bruta
24. Escítala/Rail Fence
25. Cifrado Hill/Análisis Hill
26. Ayuda online de CrypTool / Vista de árbol de menús del programa

IV. Proyecto / Perspectiva / Contacto



Contenido



- I. **CrypTool y Criptología – Visión General**
 - II. Características de CrypTool
 - III. Ejemplos
 - IV. Proyecto / Perspectiva / Contacto
- Apéndice

Relevancia de la Criptografía

Ejemplos de Uso de la Criptografía

- Cajeros automáticos, transferencias entre bancos
 - TV por Satélite, TV de pago
 - Sistemas inmovilizadores en coches
 - Gestión de Derechos Digitales (DRM)
 - Tarjetas telefónicas, teléfonos móviles, controles remotos
 - Dinero electrónico, banca electrónica, correo electrónico seguro
 - La Criptografía no está limitada a las empresas, diplomacia o a los militares. La Criptografía es una caracterizada ciencia matemática.
 - Un gran cambio en la criptografía empezó con la generalización del uso de Internet
 - Para las empresas y los gobiernos es importante que los sistemas sean seguros y
- ... ¡que los usuarios (clientes, empleados) tengan un cierto entendimiento y conciencia sobre la seguridad en TI!***



Definición: Criptología y Criptografía

Criptología (del Griego *kryptós*, “escondido”, y *lógos*, “palabra”) es la ciencia de las comunicaciones seguras (generalmente secretas). Esta seguridad se obtiene con usuarios legítimos, el transmisor y el receptor, siendo capaz de transformar la información en un código utilizando una clave – por ejemplo, una parte de la información solamente conocida por ellos. Aunque el código es inescrutable y muy a menudo inolvidable para cualquiera con su clave secreta, el receptor autorizado podrá descifrar el código para recuperar la información escondida o verificar que fue enviado probablemente por alguien que posee la clave.

Criptografía al principio se preocupaba de proporcionar confidencialidad para los mensajes escritos. Sin embargo, sus leyes se aplican igualmente bien para asegurar un flujo de datos entre ordenadores o para cifrar señales televisivas. ... Hoy, las ciencias (matemáticas) modernas de criptología no sólo contienen mecanismos para cifrar sino también para la integridad, firmas electrónicas, números aleatorios, intercambio seguro de claves, recipientes seguros, voto electrónico y dinero electrónico, y también ha conseguido convertirse en una gran variedad de aplicaciones en la vida moderna.

Fuente: Britannica (www.britannica.com)

Una definición similar se puede encontrar en Wikipedia: <http://es.wikipedia.org/wiki/Criptologia>

Criptografía – Objetivos

■ Confidencialidad

- La información prácticamente no puede ser accesible o revelada a individuos, entidades o procesos desautorizados.

■ Autenticación

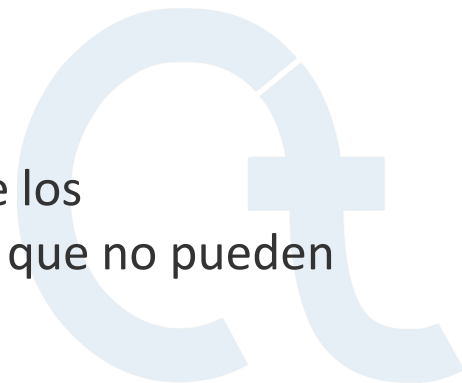
- La autenticación asegura que los usuarios se han identificado y que sus identidades se han verificado apropiadamente.

■ Integridad

- La integridad asegura que los datos no se han alterado o destruido de una forma no autorizada.

■ No-Repudio

- El principio de que, después de todo, se puede probar que los participantes de una transacción realmente la autorizan y que no pueden negar de ninguna forma su participación.



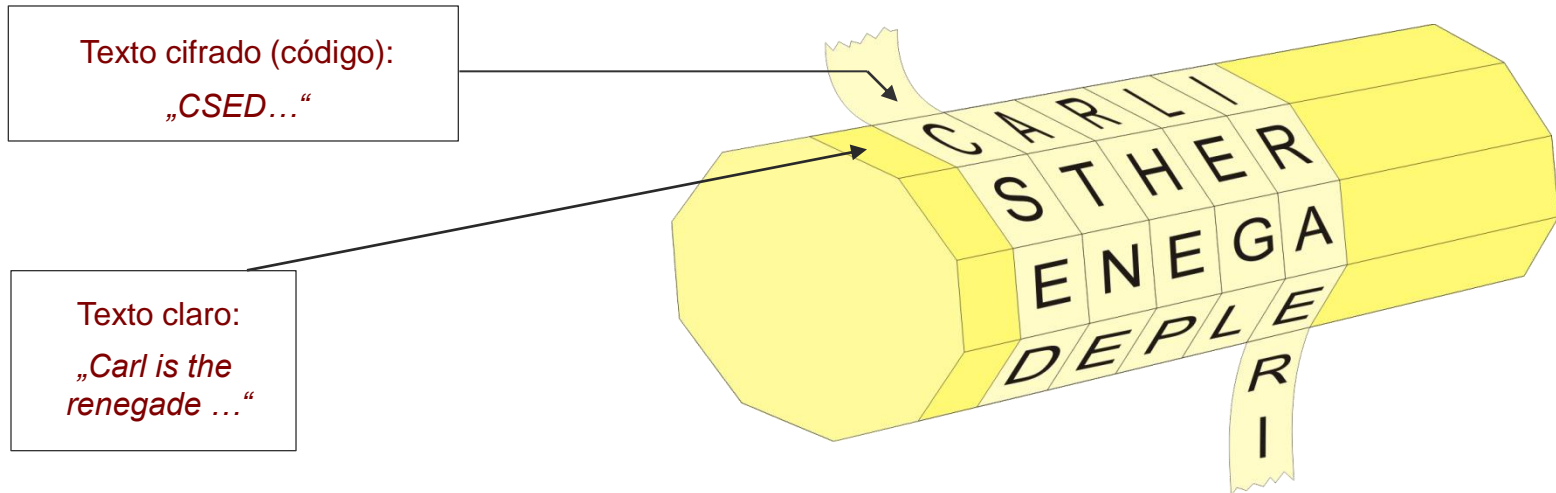
El Proyecto CrypTool

- Origen en un programa de concienciación de un banco (Capacitación Empresarial)
→ **Concienciación para empleados**
- Desarrollado en cooperación con universidades (mejorando la educación)
→ **Enfoque didáctico y orientado a estándares**
 - 1998 **Inicio del proyecto** – el esfuerzo de más de 40 años-hombre desde entonces
 - 2000 CrypTool disponible como **software libre**
 - 2002 CrypTool en el **CD-ROM-Ciudadano de la BSI** (Agencia Alemana de Seguridad de la información)
 - 2003 CrypTool se convierte en **Código-Abierto** – Soporte por Universidad de Darmstadt (Prof. Eckert)
 - 2007 CrypTool disponible en alemán, inglés, español y polaco
 - 2008 Inicio de versiones .NET y Java – Mantenidas por la Univ. de Duisburg (Prof. Weis) y SourceForge
 - 2010 CT1 disponible en su quinto idioma, serbio. Preparando versiones .NET y Java para ser lanzadas
- **Galardones**
 - 2004 TeleTrusT (TTT Förderpreis) 
 - 2004 NRW (IT Security Award NRW)  **NRW.**
 - 2004 RSA Europe (Finalista del European Information Security Award 2004) 
 - 2008 “Selected Landmark” en la iniciativa “Germany – Land of Ideas” 
- **Desarrolladores**
 - Desarrollado por gente de empresas y universidades en distintos países
 - Miembros adicionales del proyecto o códigos útiles siempre se aprecian (actualmente existen alrededor de 50 personas trabajando sobre el universo CrypTool).

Ejemplos de la primera Criptografía (1)

Métodos de cifrado antiguos.

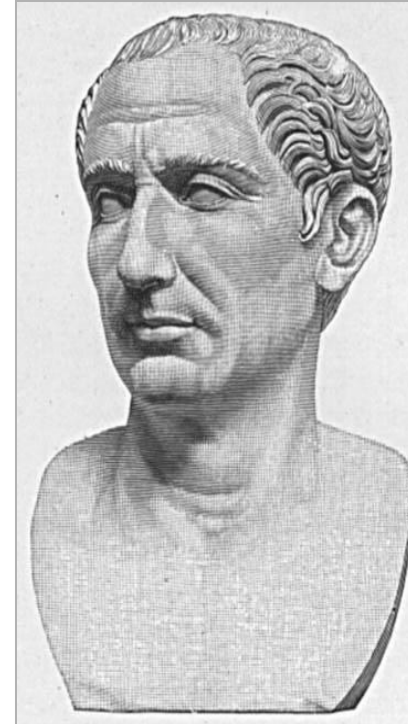
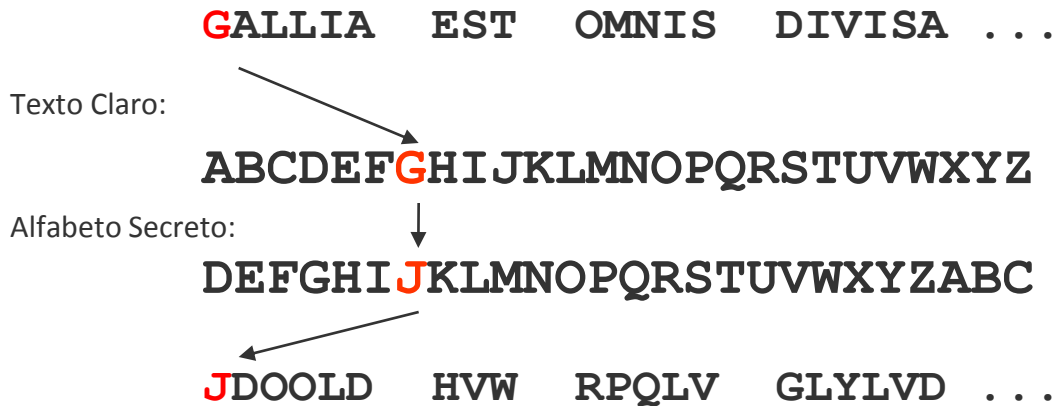
- **Tatuajes en la cabeza de un esclavo cubierto por el cabello**
- **Atbash** (sobre 600 A.C.)
 - Lenguaje secreto Hebreo, alfabeto invertido
- **Scytale de Sparta** (500 A.C.)
 - Descrito por el historiador/autor Griego Plutarco (45 - 125 A.C.)
 - Dos cilindros (varas de madera) con igual diámetro
 - Transposición (los caracteres del texto claro se reordenan)



Ejemplos de la primera Criptografía (2)

Cifrado Simétrico del César

- **Cifrado César** (Julius Caesar, 100 - 44 A.C.)
- Código de sustitución simple



- **Ataque:** Análisis de frecuencias (distribución típica de caracteres)

Presentación con CrypTool mediante los siguientes menus:

- Animación: „Procedimientos ldiv.“ \ „Visualización de algoritmos“ \ „Cesar“
- Implementación: „Cifrar/Descifrar“ \ „Simétrico (clásico)“ \ „Cesar / Rot-13“

Ejemplos de la primera Criptografía (3)

Cifrado Simétrico de Vigenère (Cifrado de sustitución polialfabética)

- **Cifrado Vigenère** (Blaise de Vigenère, 1523-1596)
 - Cifrado con una palabra clave utilizando una tabla clave
 - Ejemplo:
Palabra clave: **CHIFFRE**
Cifrando: **VIGENERE** resulta **XPOJSVVG**
 - El carácter (V) del texto claro se reemplaza por el carácter en la fila correspondiente y en la columna de la primera palabra de la palabra clave (c). El siguiente carácter del texto claro (l) se reemplaza por el carácter en la fila correspondiente y en la columna de la siguiente letra de la palabra clave (h), y así sucesivamente.
 - Si se han utilizado todos los caracteres de la palabra clave, entonces el siguiente carácter de la palabra clave es la primera letra de la palabra clave.
 - **Ataque** (por el test Kasiski): Pueden darse combinaciones de textos claros con idénticos textos cifrado. La distancia de éstos patrones se pueden utilizar para determinar la longitud de la clave.
- Un análisis de frecuencia tradicional se puede utilizar para determinar la clave.

Carácter de la clave

The diagram shows a 26x26 grid of the Vigenère square. The columns are labeled with lowercase letters 'a' through 'z', and the rows are labeled with uppercase letters 'A' through 'Z'. A key 'CHIFFRE' is written vertically above the grid, with each letter aligned with a column. The first column is labeled 'c', the second 'h', and the third 'i'. The first row is labeled 'V', the second 'I', and the third 'G'. The intersection of row 'V' and column 'c' is circled in red, and the intersection of row 'I' and column 'h' is also circled in red. A red arrow points from the text 'Carácter de la clave' to the 'c' in the key. A red arrow points from the text 'Carácter del texto claro' to the 'V' in the first row. A red arrow points from the text 'Carácter Cifrado' to the 'X' in the first row, second column.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

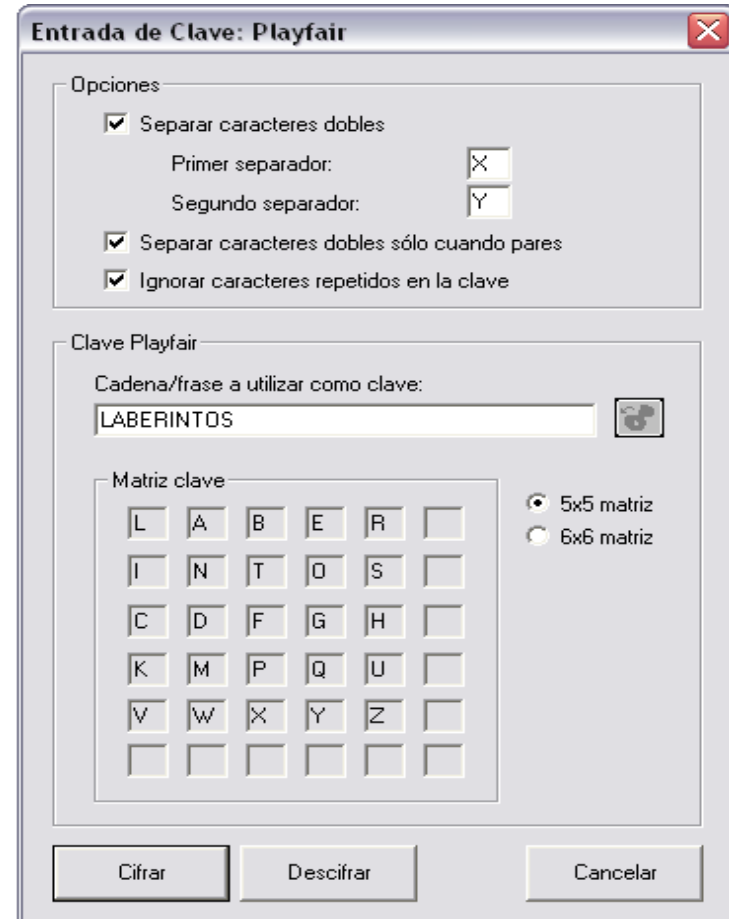
Carácter del texto claro

Carácter Cifrado

Ejemplos de la primera Criptografía (4)

Otros métodos de cifrado simétricos

- **Sustitución Homofónica**
- **Playfair** (inventado en 1854 por Sir Charles Wheatstone, 1802-1875)
 - Publicado por el Baron Lyon Playfair
 - Sustitución de un par de caracteres por otro basado en una matriz cuadrada de letras
- **Transferencia de páginas de libro**
 - Adaptación de la Libreta de un sólo uso (OTP)
- **Rejilla giratoria** (Fleissner)
- **Cifrado por permutación**
 - „Doble Dado“ (trasposición de columna doble)
(Trasposición / muy efectiva)



La Criptografía en Tiempos Modernos

Desarrollo de la Criptografía en los últimos 100 años hasta 1970

Métodos Clásicos

- Todavía se utilizan actualmente .
(ya que no todo lo puede hacer un ordenador...)
- Y sus principios de **transposición** y **sustitución** son un gran apoyo para el diseño de algoritmos modernos: la combinación de operaciones simples (un tipo de cifrado múltiple, también llamado cifrado en cascada), a nivel de bit, cifrado en bloque, ciclos.

El cifrado se vuelve

- más **sofisticado**,
- **Mecanizado o computarizado** y
- Permanece **simétrico**.

Ejemplos de la Primera Mitad del S. XX

Máquinas de cifrado mecánico (máquinas de rotores)

Cifrado Enigma (Arthur Scherbius, 1878-1929)

- Se han utilizado más de 200000 máquinas en la II Guerra Mundial.
- El cilindro giratorio elige las causas por las que cada carácter del texto se cifra con una nueva permutación.
- La oficina de cifrado polaca descifró el sistema Enigma prebélico ya en 1932.
- Código roto por un esfuerzo masivo por parte de expertos en criptografía (unas 7000 personas en Reino Unido) con máquinas de descifrado, Enigmas originales capturadas o interceptando comunicados de estado diarios (p.ej. comunicados meteorológicos).
- **Consecuencias de este exitoso criptoanálisis:**
“En general, el exitoso criptoanálisis del cifrado enigma tuvo una ventaja estratégica, que jugó un papel significativo para ganar la guerra. Algunos historiadores afirman que el descifrado del código enigma acertó la guerra varios meses o incluso un año.”

(traducido de http://de.wikipedia.org/wiki/Enigma_%28Maschine%29 - Marzo 6, 2006)



Criptografía – Conceptos Importantes (1)

- **Principio de Kerckhoffs** (establecido en 1883)
 - Separación del algoritmo (método) y la clave
p.ej. Cifrado César:
Algoritmo: “Alfabeto desplazado un cierto número de posiciones a la izquierda”
Clave: El “cierto número de posiciones” (César por ejemplo)
 - Principio de Kerckhoffs :
El secreto permanece en la clave y no en el algoritmo, es decir, “No hay seguridad por oscuridad”
- **Libreta de un sólo uso – Shannon / Vernam**
 - Demostrado teóricamente seguro, pero no es útil en la realidad (sólo el teléfono rojo)
- **Conceptos de Shannon : Confusión y Difusión**
 - Relación entre M, C y K tiene que ser tan compleja como sea posible (M=mensaje, C=código, K=clave)
 - Cada carácter del texto cifrado debe depender de tantos caracteres del texto claro como de la clave de cifrado.
 - „Efecto Avalancha“(una pequeña modificación tiene un gran impacto)
- **Función de puerta trasera** (función en una dirección)
 - Rápido en una dirección pero no en la dirección contraria (sin información secreta)
 - La dirección contraria funciona teniendo el secreto (acceso a la puerta trasera)



Ejemplos de una Fisura en el Principio de Kerckhoffs

El secreto está relacionado con la clave y no con el algoritmo

- **Penetración en el cifrado de teléfonos móviles** (Diciembre 1999)

„ Científicos Israelíes descubrieron un defecto de diseño que permitía descodificar las conversaciones privadas de cientos de millones de teléfonos móviles. Alex Biryukov y Adi Shamir describen en un artículo publicado esta semana cómo un PC con 128 MB de RAM y unos grandes discos duros puede saltarse la seguridad de una llamada telefónica o de una transmisión de datos en menos de un segundo. El algoritmo erróneo apareció en los teléfonos digitales GSM hechos por empresas como Motorola, Ericsson, y Siemens, y que son utilizados por unos 100 millones de clientes en Europa y Estados Unidos.” [...]

*“Los algoritmos de cifrado GSM habían estado bajo prueba de ataques al **estar siendo desarrollados en secreto apartados del escrutinio público** –pero muchos expertos dicen que una alta seguridad sólo puede venir de un código publicado. Moran dijo “no fue la actitud a la hora de publicar los algoritmos” cuando los códigos A5 se desarrollaron en 1989, pero **los actuales que se están creando se publicarán para una revisión por pares.**”*

[<http://www.wired.com/politics/law/news/1999/12/32900>]

- **Otro Ejemplo:** En 1999, el navegador Netscape almacenó contraseñas para acceder al servidor de correos utilizando un método de cifrado débil.

Muestra de Adaptación de una Libreta de Uso Único



Percha de un agente Stasi con una *libreta de un sólo uso*
(extraído de: *Spiegel Spezial* 1/1990)

Menú:
"Cifrar/Descifrar" \
"Simétrico (clásico)" \
"Vernam"

Problema de Distribución de Claves

Distribución de claves para métodos de cifrado simétrico

Si **2 personas** se comunican utilizando un cifrado simétrico, **necesitan una clave secreta común.**

Si **n personas** se comunican entre ellas, entonces necesitan $S_n = n * (n-1) / 2$ claves.

Esto significa que

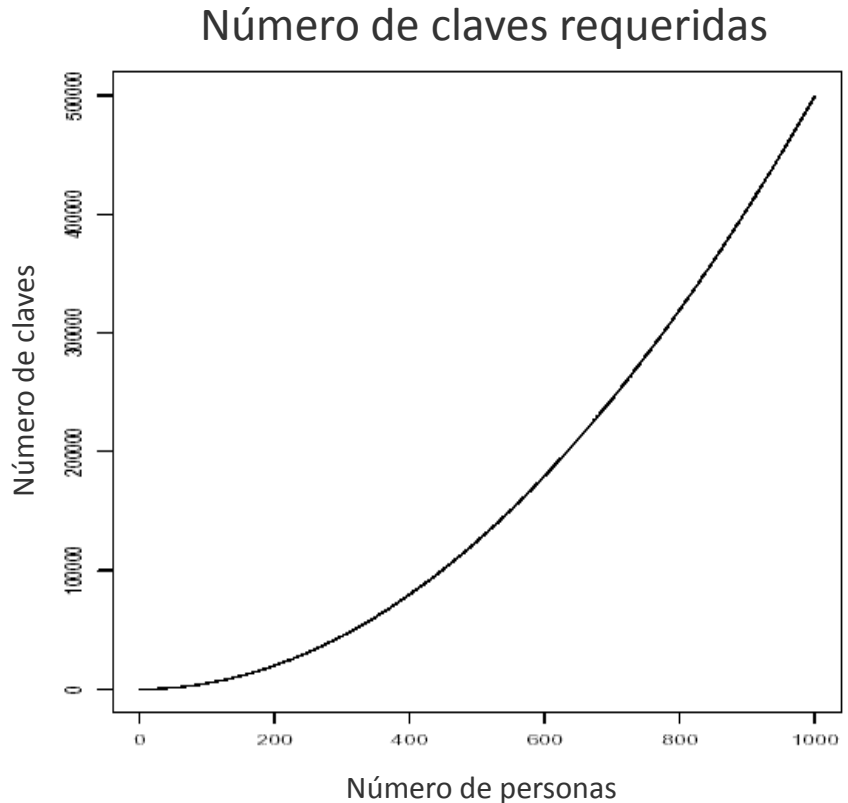
n = 100 personas requieren

$S_{100} = 4.950$ claves; y

n = 1.000 personas requieren

$S_{1000} = 499.500$ claves.

⇒ Un factor 10 de más personas, resulta un factor 100 de más claves



Criptografía – Conceptos Importantes (2)

Resolver el problema de distribución de clave mediante criptografía asimétrica

Criptografía Asimétrica

- Durante siglos se creía que: el emisor y el receptor necesitaban el mismo secreto.
- Ahora: Cada miembro necesita un par de claves (solución al problema de distribución de claves)

Cifrado Asimétrico

- „Todo el mundo puede cerrar un candado o puede dejar caer una carta en un buzón.“
- MIT, 1977: Leonard Adleman, Ron Rivest, Adi Shamir (más conocido como RSA)
- GCHQ Cheltenham, 1973: James Ellis, Clifford Cocks (aceptado públicamente en Diciembre de 1997)

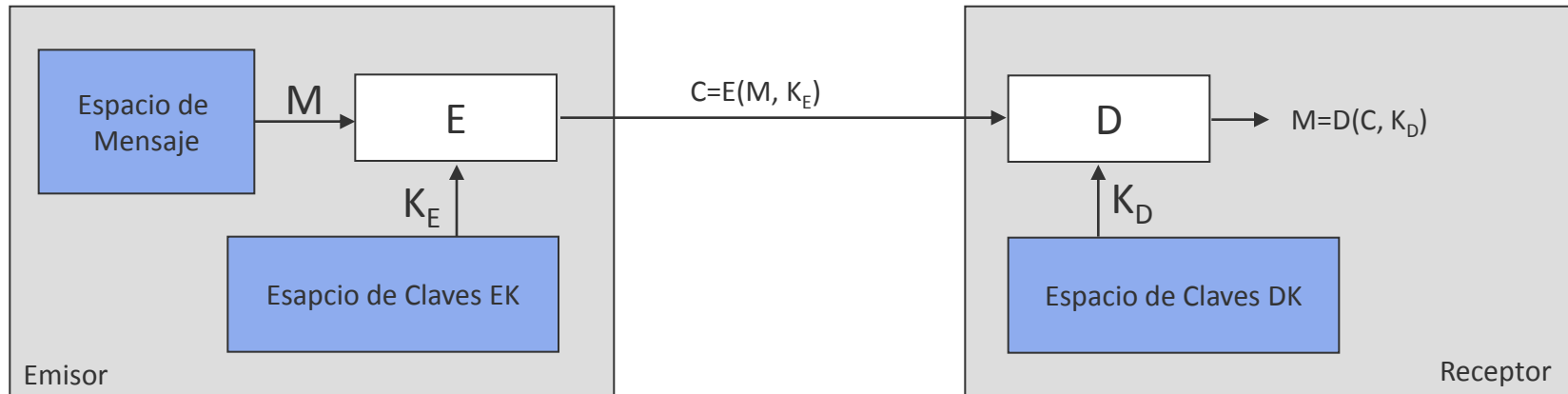
Distribución de claves

- Stanford, 1976: Whitfield Diffie, Martin Hellman, Ralph Merkle (Intercambio de clave Diffie-Hellman)
- GCHQ Cheltenham, 1975: Malcolm Williamson

¡La seguridad en redes abiertas (como Internet) sería extremadamente cara y compleja sin una criptografía asimétrica!

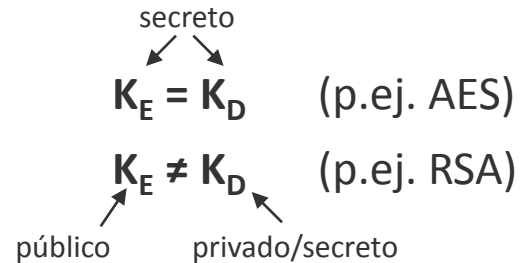
Cifrado y Descifrado

Cifrado Simétrico y asimétrico



a) Cifrado Simétrico:

b) Cifrado Asimétrico:



Criptografía – Conceptos Importantes (3)

La creciente relevancia de las matemáticas y las tecnologías de la información

- **La criptografía moderna se basa en las matemáticas**
 - A pesar de los nuevos métodos de cifrado simétrico como el AES (mejor funcionamiento y una clave más corta comparados con los métodos asimétricos basados puramente en problemas matemáticos).
- La seguridad de los métodos de cifrado dependen fuertemente del estado en el que se encuentran las **matemáticas** y las **tecnologías de la información (TI)**
 - Complejidad computacional (el principal esfuerzo de procesamiento está relacionado con la longitud de la clave, demanda de dispositivos y complejidad de los datos)
-> ver RSA: Bernstein, dispositivo TWIRL, RSA-160, RSA-200
 - Actividad muy alta en la investigación actual en:
Factorización, algoritmos no paralelizables (a causa de los ordenadores cuánticos), mejor comprensión de la debilidad de los protocolos y los generadores aleatorios, ...).
- Grave Error: “Las matemáticas reales no tienen efecto sobre la guerra.”
(G.H. Hardy, 1940)
- Los vendedores han descubierto la **seguridad** como un criterio esencial de **compra**.

Demostración con CrypTool

- **Análisis Estadístico**

- **Cifrar dos veces no siempre es mejor:**

César: $C + D = G$ ($3 + 4 = 7$)

Vigenère: - $CAT + DOG = FOZ$ [$(2,0,19)+(3,14,6)=(5,14,25)$]

No hay mejoras, sin embargo usando:

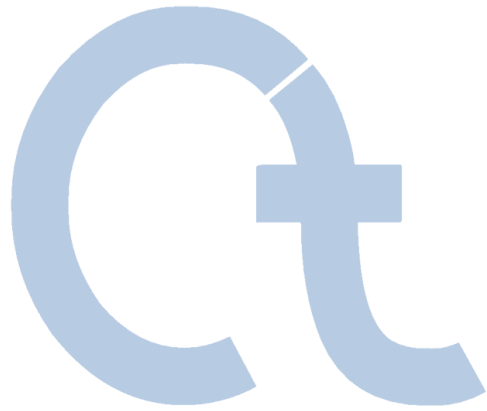
- $GATO + PERRO = VEKFUPXFXOISXRHDKRKC$)

Se produce una clave mucho más fuerte.

- **Vernam (OTP)**

- **AES** (clave de salida, análisis por fuerza bruta)

Contenido



- I. CrypTool y Criptología – Visión General
 - II. Características de CrypTool**
 - III. Ejemplos
 - IV. Proyecto / Perspectiva / Contacto
- Apéndice

1. ¿Qué es CrypTool?

- Programa libre con interfaz gráfica
- Se pueden aplicar métodos criptográficos y analizarlos
- Completa ayuda en línea (comprensible sin un conocimiento profundo sobre criptografía)
- Contiene casi todas las funciones criptográficas actuales
- Introducción fácil tanto a la criptografía clásica como a la moderna
- No es una *“herramienta de hackers”*

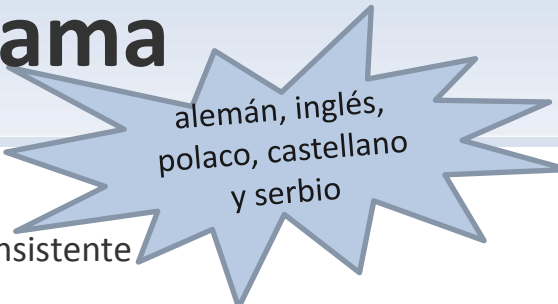
2. ¿Por qué CrypTool?

- Origen en una iniciativa de concienciación de un instituto financiero
- Desarrollado en una cercana cooperación con universidades.
- Mejora en la educación universitaria y capacitación empresarial

3. Público Objetivo

- Grupo Principal: Estudiantes de informática, negocio informático y matemáticas
- Pero también para: usuarios de ordenador, desarrolladores de aplicaciones, empleados
- Prerrequisitos: conocimiento sobre PC
- Preferiblemente: Interesados en matemáticas y/o programación

Contenido del Paquete del Programa



alemán, inglés,
polaco, castellano
y serbio

Programa CrypTool

- Todas las funciones integradas en un *único* programa con una interfaz gráfica consistente
- Funciona sobre Win32
- Librerías Criptográficas de Secude y OpenSSL
- Aritmética de enteros grandes a través de Miracl, APFLOAT y GMP/MPPIR, Reducción de base de retículos por NTL (V. Shoup)

Herramienta AES

- Programa independiente para cifrado AES (y creación de archivos autoextraíbles)

Juego Educativo

- „Number Shark“ estimula la comprensión de los factores y los números primos.

Completa Ayuda online (Ayuda HTML)

- Ayuda sensible al contexto disponible con F1 para todas las funciones del programa (incluidos los menús)
- Casos detallados de uso para muchas funciones del programa (tutorial)

Script (archivo .pdf) con información básica

- Métodos de cifrado • Factorización en Primos • Firma Digital
- Curvas Elípticas • certificado de clave pública • Teoría de Números Básica • Crypto 2020

Dos historias cortas relacionadas con la criptografía de Dr. C. Elsner

- „The Dialogue of the Sisters“ (una variante de RSA como elemento clave)
- „The Chinese Labyrinth“ (Tareas de teoría de números para Marco Polo)

Herramienta para el aprendizaje de Teoría de Números



Características (1)

Criptografía

Criptografía Clásica

- César (y ROT-13)
- Sustitución Monoalfabética (y Atbash)
- Vigenère
- Hill
- Sustitución Homofónica
- Playfair
- ADFGVX
- Suma de Bytes
- XOR
- Vernam
- Permutación / Trasposición (Rail Fence, Escítala, ...)
- Solitario

Varias opciones para entender fácilmente los métodos criptográficos

- Alfabeto seleccionable
- Opciones: manejo de espacios, etc.

Criptoanálisis

Ataque a métodos clásicos

- Sólo texto cifrado
 - César
 - Vigenère (según Friedman + Schroedel)
 - Suma
 - XOR
 - Sustitución
 - Playfair
- Texto Claro conocido
 - Hill
 - Transposición de Columna Simple
- Manual (soportado)
 - Sustitución mono-alfabética
 - Playfair, ADFGVX, Solitario

Métodos de Análisis soportados

- Entropía, frecuencia real
- Histograma, análisis de n-grama
- Autocorrelación
- Periodicidad
- Análisis de aleatoriedad
- Base64 / UU-Encode

Características (2)

Criptografía

Cifrado simétrico moderno

- IDEA, RC2, RC4, RC6, DES, 3DES, DESX
- Candidatos AES de la última ronda de selección (Serpent, Twofish, ...)
- AES (=Rijndael)
- DESL, DESXL

Cifrado Asimétrico

- RSA con certificados X.509
- Demostración RSA
 - Comprensión de ejemplos
 - Alfabeto y longitud de bloque seleccionable

Cifrado Híbrido (RSA + AES)

- Diagrama de flujo de datos interactivo

Criptoanálisis

Ataque por fuerza bruta para algoritmos simétricos

- Para todos los algoritmos
- Suposiciones:
 - La entropía de un texto claro es pequeña o la clave se conoce parcialmente o se conoce el alfabeto del texto claro

Ataque al cifrado RSA

- Factorización del módulo RSA
- Ataques de bases de Retículos

Ataque al cifrado híbrido

- Ataque a RSA o
- Ataque a AES (ataque del canal lateral)

Características (3)

Criptografía

Firma Digital

- RSA con certificados X.509
 - Firma como un diagrama de flujo de datos
- DSA con certificados X.509
- Curva Elíptica DSA, Nyberg-Rueppel

Funciones Hash

- MD2, MD4, MD5
- SHA, SHA-1, SHA-2, RIPEMD-160

Generadores Aleatorios

- Secude
- $x^2 \bmod n$
- Generador de congruencias Lineal (LCG)
- Generador de congruencias Inverso (ICG)

Criptoanálisis

Ataque a la firma RSA

- Factorización del módulo RSA
- Factible hasta los 250 bits o 75 decimales (en un PC estándar)

Ataque a las funciones hash / firma digital

- Generar colisiones hash para un texto en ASCII (paradoja del cumpleaños) (hasta 40 bit en unos 5 min)

Análisis de datos aleatorios

- Batería de pruebas FIPS-PUB-140-1
- Periodicidad, Vitany, entropía
- Frecuencia real, histograma
- Análisis de n-gramas, autocorrelación
- Test de compresión ZIP

Características (4)

Animaciones / Demostraciones

- César, Vigenère, Nihilist, DES (todo con ANIMAL)
- Enigma (Flash)
- Rijdael/AES (Flash)
- Cifrado y descifrado Híbrido (AES-RSA y AES-ECC)
- Generación y verificación de firmas digitales
- Intercambio de claves Diffie-Hellman
- Secreto compartido (con CRT o Shamir)
- Método Desafío-Respuesta (autenticación)
- Ataque del canal lateral
- E-mail seguro con protocolo S/MIME (con Java y Flash)
- Presentación gráfica en 3D de chorros de datos (aleatorios)
- Sensibilidad de funciones hash con respecto a cambios en el texto claro
- Teoría de Números y criptosistema RSA (con Authorware)



Características (5)

Funciones Adicionales

- Diferentes funciones para RSA y números primos
- Cifrado Homofónico y por permutación (Transposición Doble Columna)
- PKCS #12 importado y exportado para PSEs (Entorno Personal de Seguridad)
- Generar archivos has de archivos grandes sin cargarlos
- Ataques por fuerza bruta flexibles sobre cualquier algoritmo simétrico moderno.
- Demostración de ECC (como aplicación Java)
- Medidor de Calidad de Contraseñas (PQM)
- Múltiples opciones de texto para los cifrados clásicos (ver [Ejemplo 24](#))
- Y mucho más ...

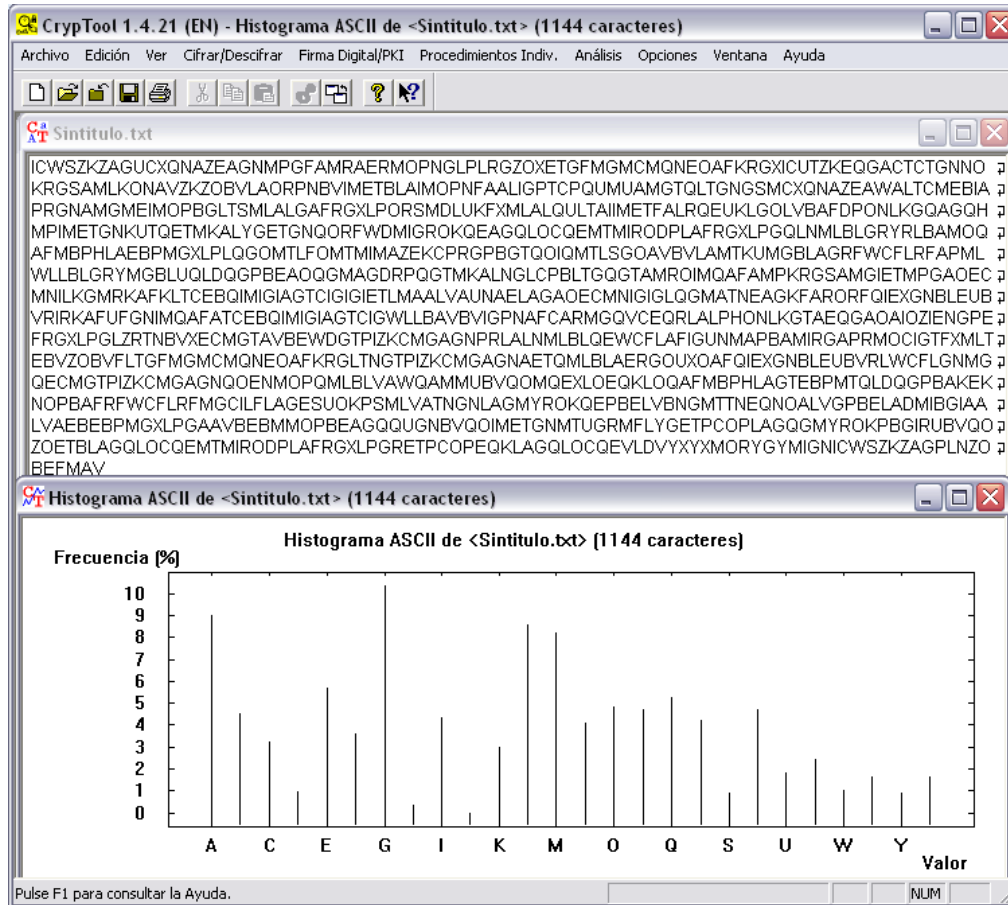


Análisis de la Estructura de un Idioma

Opciones de análisis disponibles en CrypTool

Número de caracteres, n-grama, entropía

- ver menú “Análisis” \ “Herramientas para el Análisis” \ ...



Entropía <Sintitulo.txt>

Este documento contiene 25 caracteres diferentes comparados con los 26 caracteres del alfabeto seleccionado.

La entropía del documento es 4.31 (la entropía máxima posible es 4.70).

Aceptar

Lista de N-Gramas de Sintitulo.txt

Selección:

- Histograma
- Digrama
- Trigrama
- 4 -grama

Mostrar los: 26

N-gramas más comunes (valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuen...	Frecuencia en...	Frecuencia
1	G	10.3147	118
2	A	9.0035	103
3	L	8.5664	98
4	M	8.2168	94
5	E	5.6818	65
6	Q	5.2448	60
7	O	4.8077	55
8	P	4.7203	54
9	T	4.7203	54
10	B	4.5455	52
11	I	4.3706	50
12	R	4.1958	48
13	N	4.1084	47
14	F	3.5839	41
15	C	3.2343	37
16	K	2.9720	34
17	V	2.4476	28
18	U	1.8357	21
19	X	1.6608	19
20	Z	1.6608	19
21	W	1.0490	12
22	D	0.9615	11
23	S	0.8741	10
24	Y	0.8741	10
25	H	0.3497	4

Demonstración de Interactividad (1)

Demostración en
CrypTool

Análisis Vigenère

El resultado del análisis de Vigenère puede rehacerse manualmente (cambiando la longitud de la clave):

1. Cifrar el ejemplo inicial con: **TESTETE**

- “Cifrar/Descifrar” \ “Simétrico (clásico)” \ “Vigenère”
- Introducir TESTETE ⇨ “Cifrar”

Análisis del resultado del cifrado:

- “Análisis” \ “Cifrado Simétrico (clásico)” \ “Sólo texto cifrado” \ “Vigenère”
- Longitud de clave deducida: 7, Clave deducida: TESTETE ✓

2. Cifrar el ejemplo inicial con: **TEST**

- “Cifrar/Descifrar” \ “Simétrico (clásico)” \ “Vigenère”
- Introducir TEST ⇨ “Cifrar”

Análisis del resultado del cifrado:

- “Análisis” \ “Cifrado Simétrico (clásico)” \ “Sólo texto cifrado” \ “Vigenère”
- Longitud de clave deducida: 8 – Falso ✗
- Longitud de clave seleccionada automáticamente a 4 (puede ajustarse manualmente)
- Clave deducida: TEST ✓

Demonstración de Interactividad (2)

Demostración en
CrypTool

Factorización automatizada

Factorización de un número compuesto con algoritmos de factorización

- Algunos métodos se ejecutan en paralelo (multihilo)
- Los métodos tienen ventajas e inconvenientes específicos (p.ej. Algunos métodos sólo pueden determinar factores pequeños)

Ejemplo de Factorización 1:

316775895367314538931177095642205088158145887517

Número decimal de 48-dígitos

=

3 * 1129 * 6353 * 1159777 * 22383173213963 * 567102977853788110597

Ejemplo de Factorización 2:

$2^{250} - 1$

Número decimal de 75-dígitos

=

3 * 11 * 31 * 251 * 601 * 1801 * 4051 * 229668251 * 269089806001 *
4710883168879506001 * 5519485418336288303251

Menú: "Procedimientos Indiv." \ "Criptosistema RSA" \ "Factorización de un Número"

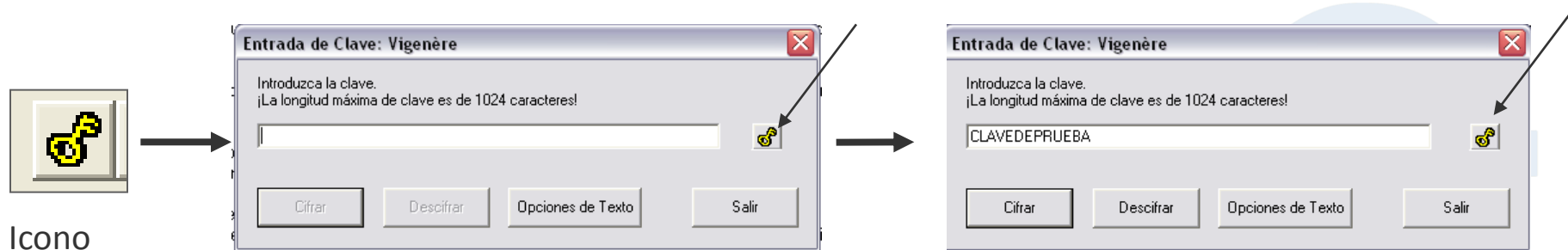
Conceptos para una Interfaz de fácil manejo

1. Ayuda sensible al contexto (F1)

- F1 sobre una entrada de menú seleccionada nos muestra información sobre el algoritmo/método.
- F1 en una ventana de diálogo explica la utilidad de la ventana.
- Estas asistencias y los contenidos de los menús principales están vinculados de forma cruzada en la ayuda en línea.

2. Pegar claves en una ventana de entrada de claves

- Se puede utilizar CTRL-V para pegar contenidos desde el porta papeles.
- Las claves utilizadas se pueden obtener de una ventana de texto cifrado por medio de un icono de la barra de herramientas. Su correspondiente icono en la ventana de entrada de clave se puede utilizar para pegar la clave en el campo de entrada. Se utiliza un **depósito de claves interno** de CrypTool que está disponible para cada método (útil para claves largas y/o “específicas”- p.ej. en el cifrado homofónico).



Desafíos para los Desarrolladores (Ejemplos)

1. Muchas funciones trabajan en paralelo

- La factorización trabaja con algoritmos multihilo

2. Alto Rendimiento

- Localizar colisiones hash (paradoja del cumpleaños) o ejecutar análisis por fuerza bruta

3. Considera límites de memoria

- Algoritmo de Floyd (mapeados para localizar colisiones hash) o con una factorización con criba cuadrática

4. Medida del tiempo y estimaciones

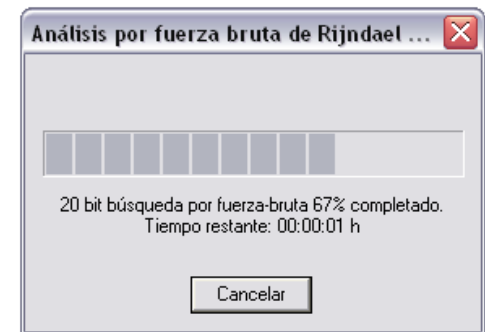
- Muestra el tiempo restante durante la fuerza bruta

5. Reusabilidad / Integración

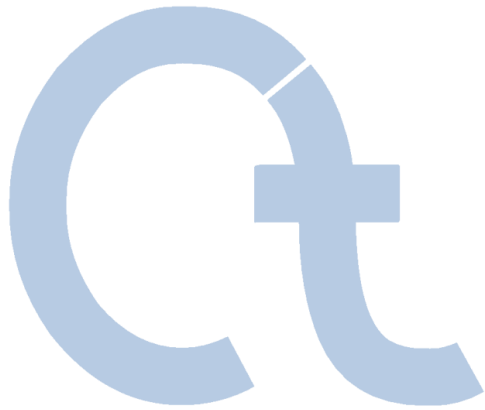
- Aplicaciones para la generación de números primos
- Criptosistema RSA (cambia la vista después de un ataque exitoso de un usuario de clave pública al propietario de clave privada)

6. Automatizar parcialmente la consistencia de funciones, GUI y ayuda en línea

(incluyendo varios idiomas y los SOs de Windows: XP, Vista y 7)



Contenido



- I. CrypTool y Criptología – Visión General
 - II. Características de CrypTool
 - III. Ejemplos**
 - IV. Proyecto / Perspectiva / Contacto
- Apéndice

Ejemplos de CrypTool

Visión general de los ejemplos

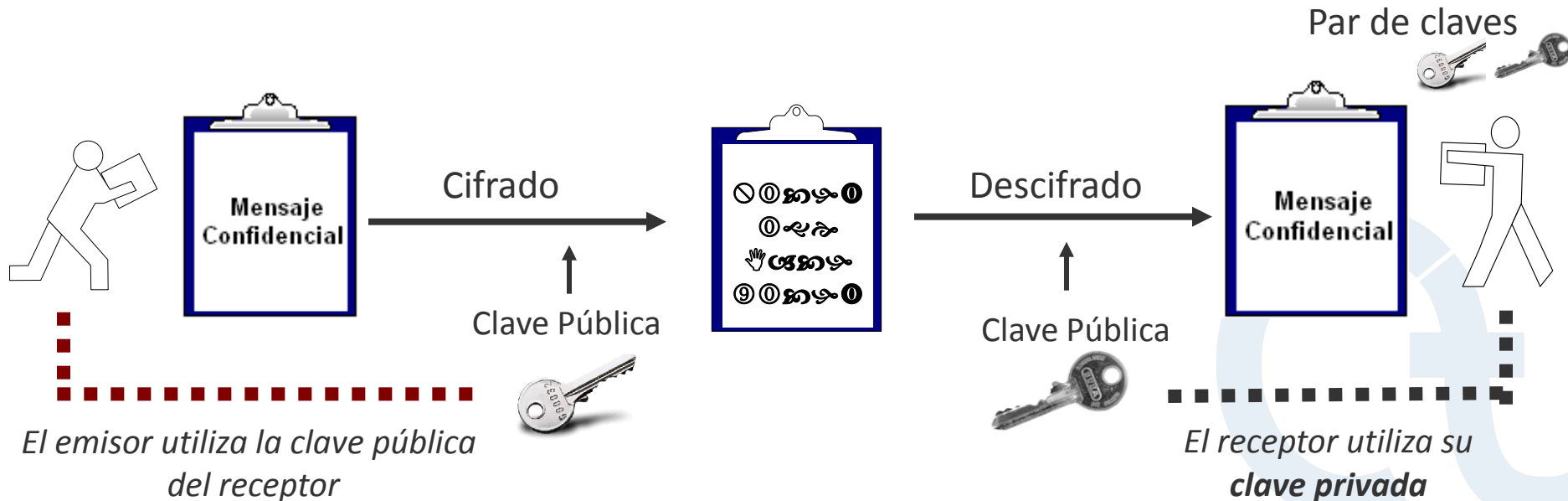
1. [Cifrado con RSA / Test de primalidad / Cifrado híbrido y certificados digitales / SSL](#)
2. [Visualización de firma digital](#)
3. [Ataque al cifrado RSA \(módulo N demasiado pequeño\)](#)
4. [Análisis del cifrado en la PSION 5](#)
5. [Claves DES débiles](#)
6. [Localizando información de la clave \(“clave NSA”\)](#)
7. [Ataque a la firma digital por búsqueda de colisiones hash](#)
8. [Autenticación en un entorno cliente-servidor](#)
9. [Demostración de un ataque de canal lateral \(en un protocolo de cifrado híbrido\)](#)
10. [Ataque RSA utilizando reducción de retículos \(lattice reduction\)](#)
11. [Análisis de aleatoriedad con visualización 3-D](#)
12. [Secreto Compartido \(Teorema Chino de los Restos \(CRT\) / Shamir\)](#)
13. [Implementación del CRT en Astronomía](#)
14. [Visualización del cifrado utilizando ANIMAL](#)
15. [Visualización del AES](#)
16. [Visualización del cifrado Enigma](#)
17. [Visualización de E-mail seguro con S/MIME](#)
18. [Generación de un código de autenticación de un mensaje \(HMAC\)](#)
19. [Demo Hash](#)
20. [Herramienta de aprendizaje de teoría de números y cifrado asimétrico](#)
21. [Suma de puntos en curvas elípticas](#)
22. [Medidor de calidad de contraseñas](#)
23. [Análisis por Fuerza Bruta](#)
24. [Escítala / Rail Fence](#)
25. [Cifrado Hill / Análisis Hill](#)
26. [Ayuda online de CrypTool / Vista de árbol de menús del programa](#)



Ejemplos de CrypTool

Cifrado con RSA (en realidad, la mayoría de cifrados híbridos)

- Bases para, por ejemplo, el protocolo SSL (acceso a sitios web protegidos)
- Cifrado asimétrico utilizando RSA
 - Cada usuario tiene un par de claves– una pública y otra privada
 - El emisor cifra con la clave pública del receptor
 - El receptor descifra con su clave privada
- Normalmente se implementa combinándolo con métodos simétricos (transferencia de la clave simétrica por codificación/descodificación RSA)



Ejemplos (1)

Cifrado utilizando RSA – trasfondo Matemático / algoritmo

- Clave Pública: (n, e)
- Clave Privada: (d)

donde:

p, q grandes, números primos elegidos aleatoriamente con $n = p \cdot q$;

d se calcula bajo las constantes $\text{mcd}[\varphi(n), e] = 1$; $e \cdot d \equiv 1 \pmod{\varphi(n)}$.

Operación de cifrado y descifrado: $(m^e)^d \equiv m \pmod{n}$

- n es el módulo, cuya longitud en bit se refiere a la longitud de la clave RSA.
- mcd = máximo común divisor.
- $\varphi(n)$ es la función ϕ de Euler.

Procedimiento :

- Transformación del mensaje en representación binaria
- Mensaje Cifrado $m = m_1, \dots, m_k$ en el sentido de los bloques, con para todo m_j :
 $0 \leq m_j < n$; tamaño de bloque máximo r , por eso: $2^r \leq n$ ($2^{r-1} < n$)

Vea también: Animación flash interactiva sobre los fundamentos del cifrado RSA:

<http://cryptool.com/download/RSA/RSA-Flash-en/player.html>

Ejemplos (1)

Test de Primalidad – Se necesita para los enormes primos de RSA.

- Pruebas probabilísticas rápidas
- Pruebas Deterministas

Los métodos de prueba de números primos se realizan mucho más rápido si un número grande es primo, entonces los métodos de factorización conocidos pueden separar un número de tamaño similar en sus factores primos.

Para los test AKS se integraron a CrypTool las bibliotecas GMP (GNU Multiple Precision Arithmetic Library) y MPIR (Multiple Precision Integers and Rationals).

Test de Primalidad

Existen varios métodos para comprobar si un número es primo o no. Normalmente se aplican métodos probabilísticos: son muy rápidos pero realmente sólo pueden determinar con una cierta precisión (el error cometido es mínimo) si el número es primo. No obstante, existen otros métodos deterministas que proporcionan un resultado 100% fiable (desde el punto de vista matemático).

Algoritmos para el test de primalidad

- Test de Miller-Rabin
- Test de Fermat
- Test de Solovay-Strasse
- Test de AKS (procedimiento determinista)

Test de Primalidad

Cargar número desde archivo

Número a:

Resultado:  5789604461865809771178549250434395392663499233282028201972879200

Analizar número Cancelar

Menú: "Procedimientos. Individ" \ "RSA Criptosistema" \ "Test de Primalidad"

Ejemplos (1)

El mayor número primo descubierto hasta ahora – Números primos de Mersenne

Los números primos más grandes descubiertos, son los denominados: Números primos de Mersenne.

El número actualmente recordista tiene 12.978.189 dígitos decimales y fue descubierto en 2008 por el grupo del proyecto GIMPS.

En el siguiente diálogo de CrypTool, podrá calcular y mostrar rápidamente cada una de sus cifras en un archivo.

Para eso, la biblioteca APFLOAT fue integrada al programa.

En el menú contextual de cada uno de los campos de entrada o salida puede des/activar el separador de miles.

Calcular números de Mersenne

Base b: 2

Exponente e: 43.112.609

Resultado $b^e - 1$: 3164702693302559231434537239493375160541061884752

Tamaño del resultado: 12978189 (número de cifras)

Iniciar cálculo

Escribir resultado

Cancelar cálculo

Cerrar

Nota: $2^{43.112.609} - 1 = 316.470.269 \dots 697.152.511$

Los números extremadamente grandes no deberían ser seleccionados y copiados directamente del campo “Resultado”; para no perjudicar la performance de la GUI. Por favor, utilice el botón “Escribir resultado” para poder mostrar el resultado en su totalidad en la misma ventana de CrypTool.

Menú: “Procedimientos Indiv.” \ “Teoría de Números – Interactiva” \ “Calcular números de Mersenne”

Ejemplos (1)

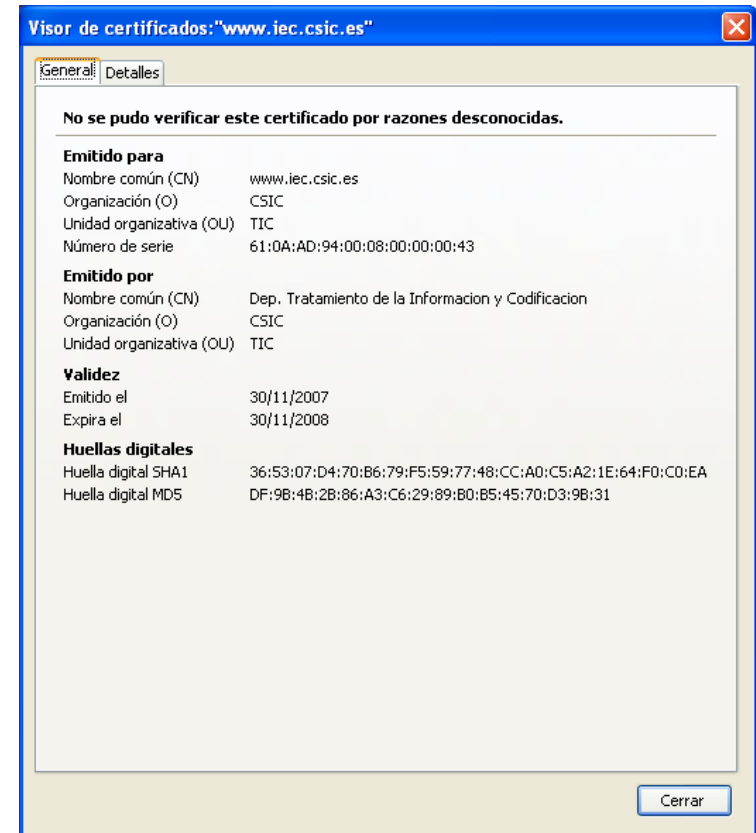
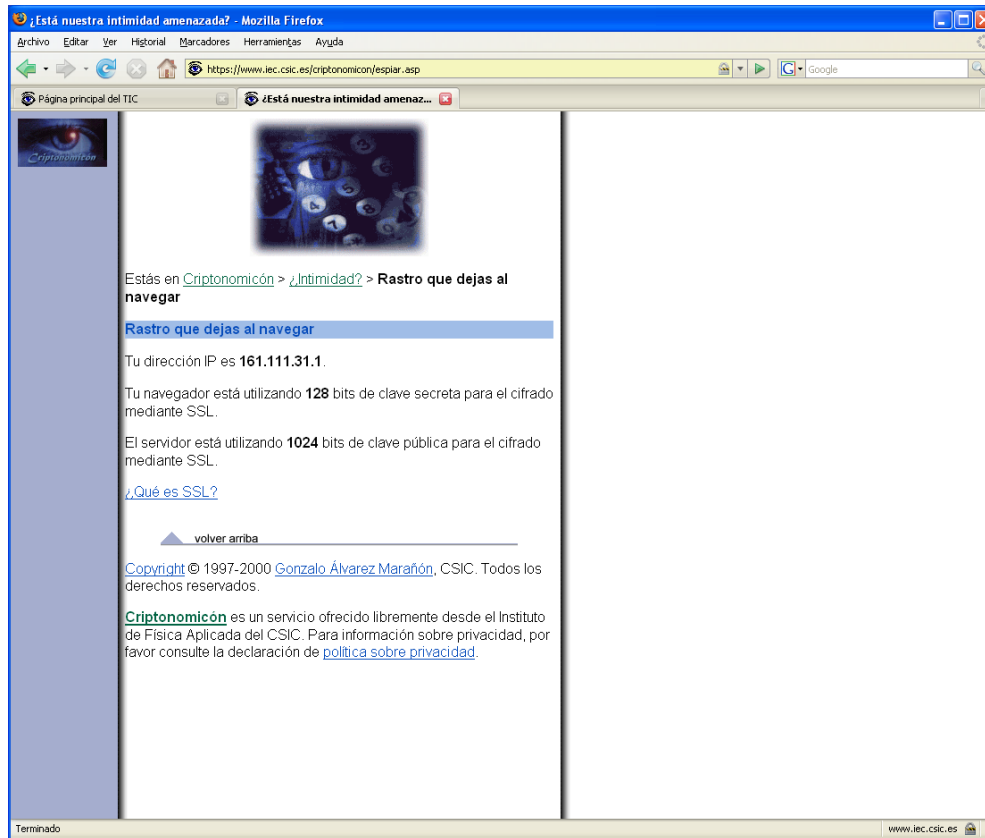
Cifrado Híbrido y certificados digitales

- Cifrado Híbrido – **Combinación de cifrado simétrico y asimétrico**
 1. Generación de una clave simétrica aleatoria (clave de sesión)
 2. Se transfiere la clave de sesión – protegida por una clave asimétrica
 3. Se transfiere el mensaje – protegida por la clave de sesión
- Problema: **Ataques del *hombre en el medio* – ¿La clave pública del receptor pertenece realmente al receptor?**
- Solución: Certificados Digitales – **Una central (p. ej. Telesec, VeriSign, Deutsche Bank PKI), en la que confían los usuarios, asegura la autenticidad del certificado y la clave pública contenida (parecido al pasaporte expedido por el estado).**
- El cifrado híbrido basado en certificados digitales es la base para todas las **comunicaciones electrónicas seguras:**
 - Compra por Internet y Banca Online
 - Correo electrónico seguro



Ejemplos (1)

Conexión online segura utilizando SSL y certificados



Esto significa que la conexión es autenticada y (al menos en un sentido) la transferencia de datos está fuertemente cifrada.



Ejemplos (1)

Atributos o campos de un certificado

Visor de certificados: "www.iec.csic.es"

General Detalles

Jerarquía de certificados

- Dep. Tratamiento de la Información y Codificación
 - www.iec.csic.es

Campos del certificado

- No después
- Asunto
- Información de la clave pública del sujeto
 - Algoritmo de la clave pública del sujeto
 - Clave pública del sujeto
- Extensiones
 - Utilización de la clave de certificado
 - Identificador de objeto (1 2 840 113549 1 9 15)
 - Uso extendido de la clave

Valor del campo

Tamaño: 140 Bytes / 1120 Bits

```
30 81 89 02 81 81 00 c3 72 cc 75 48 8c 21 e6 7f
ea 2a fe f6 6e aa 16 37 e1 94 cc 0f c2 09 d5 b4
91 d9 b8 11 66 23 6b 52 8b 8c 86 71 86 df 74 05
9c e7 31 cd 93 07 3f f6 b2 95 6d 2c 7e 02 c3 b7
95 ea 54 10 4e 53 18 97 e4 44 2b 5b 09 2c a8 15
d7 da 3d db db be fd 0c f6 df 26 90 9b 90 bb 21
76 63 05 62 25 47 e6 46 24 62 86 88 7c 06 5b c9
69 8a 98 9f cc 6d 86 b2 a1 74 3e d8 33 92 32 55
```

Cerrar

Atributos generales / campos

- Emisor (p.ej. VeriSign)
- Solicitante
- Período de validez
- Número de Serie
- Tipo de Certificado/ Versión (X.509v3)
- Algoritmo de firma
- Clave Pública (y método)

Clave Pública



Ejemplos (1)

Establecer una conexión segura SSL (Autenticación del Servidor)

Client



1. Inicio SSL

Server



Enviar certificado del servidor



2.

3. Validar certificado del servidor (utilizado raíces de certificados instalados localmente)

4. Recuperar la clave pública del servidor (desde el certificado del servidor)

5. Generar una clave simétrica aleatoria (clave de sesión)

6. Enviar clave de sesión
(cifrada con la clave pública del servidor)

Recuperar clave de sesión
(descifrada por la clave privada del servidor) 7.



SSL Secured (128 Bit)

Comunicación cifrada basada en el intercambio de la clave de sesión

Ejemplos (1)

Establecer una conexión segura SSL (Autenticación del Servidor)

General

- El ejemplo muestra el establecimiento de una conexión SSL típica para transferir datos delicados a través de internet (p.ej. compra online).
- Al establecer la conexión SSL solamente se autentifica el servidor utilizando el certificado digital (la autenticación del usuario se da normalmente a través del nombre de usuario y su contraseña después de que se haya establecido la conexión SSL).
- SSL también ofrece la opción de la autenticación del cliente basada en certificados digitales.

Comentarios al establecimiento de la conexión SSL (ver diapositiva anterior)

- Paso 1: Inicialización SSL – durante esta fase, se negocian las características tanto de la clave de sesión (p.ej. Tamaño en bits) como del algoritmo de cifrado simétrico (p.ej. 3DES, AES).
- Paso 2: En el caso de una jerarquía de certificado multinivel, también se pasan los certificados intermedios al cliente.
- Paso 3: En esta fase los certificados raíz instalados en la memoria de certificados del navegador se utilizan para validar el certificado del servidor.
- Paso 5: La clave de sesión se basan en las características negociadas (ver 1).

Ejemplos (2)

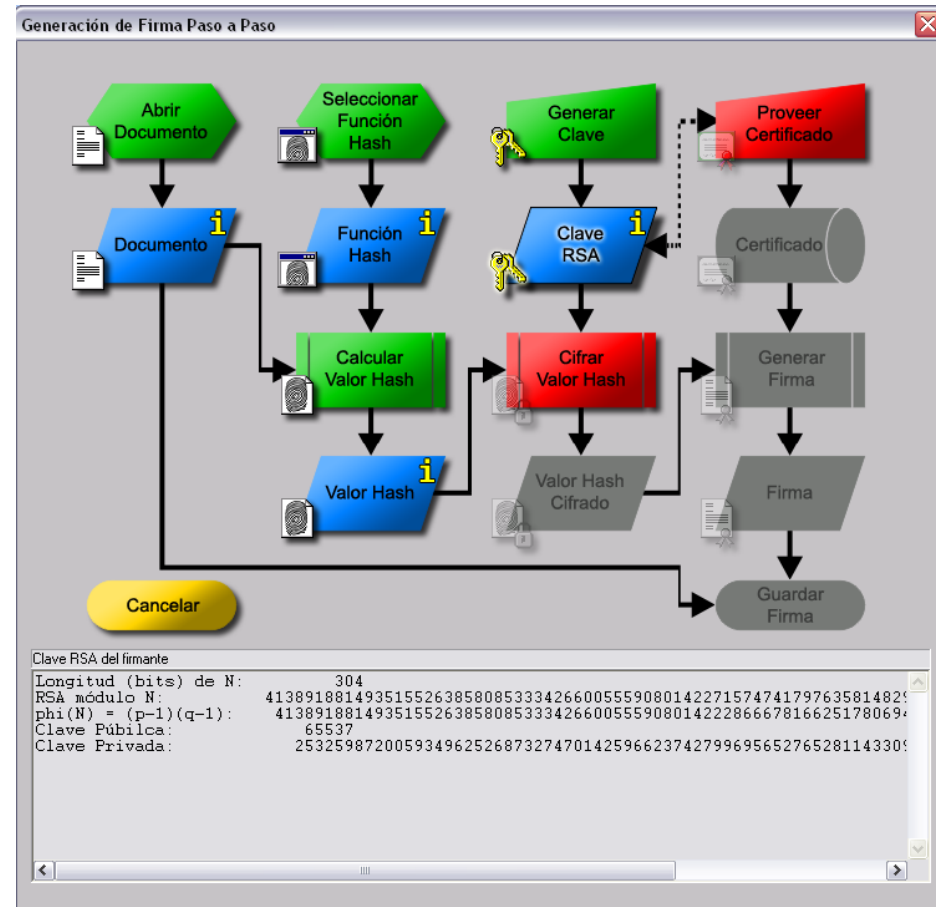
Visualización de una firma digital

Firma Digital

- Importancia creciente:
 - Equivalencia con la firma manual (ley de la firma digital)
 - Cada vez más utilizada en la industria,
 - Gobierno y usuarios
- Poca gente sabe cómo funciona exactamente

Visualización en CrypTool

- Diagrama de flujo de datos interactivo
- Parecida a la visualización del cifrado híbrido



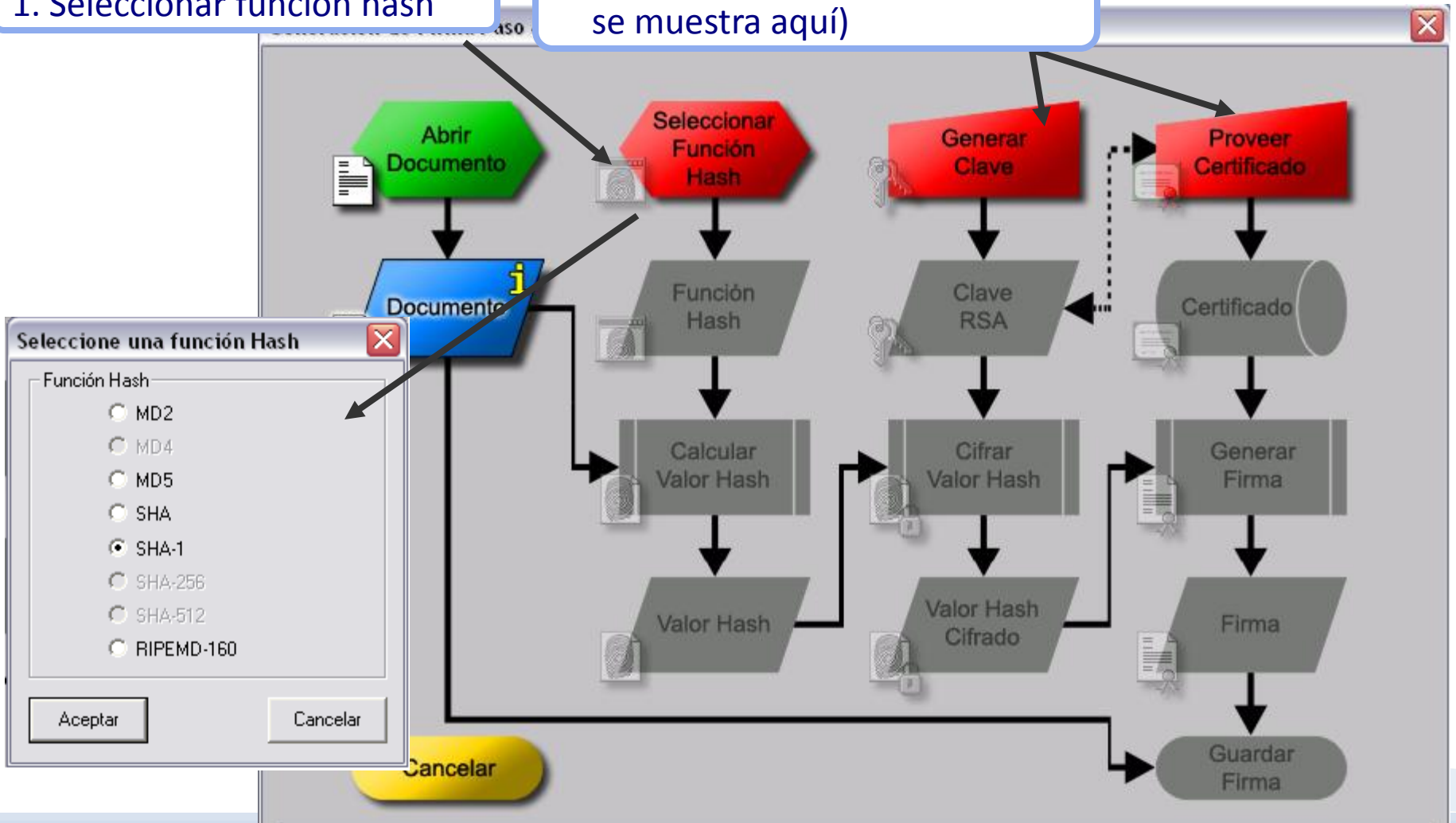
Menú: „Firma Digital/PKI“ \
„Demostración de firma(Generación de Firma)“

Ejemplos (2)

Visualización de una firma digital : a) Preparación

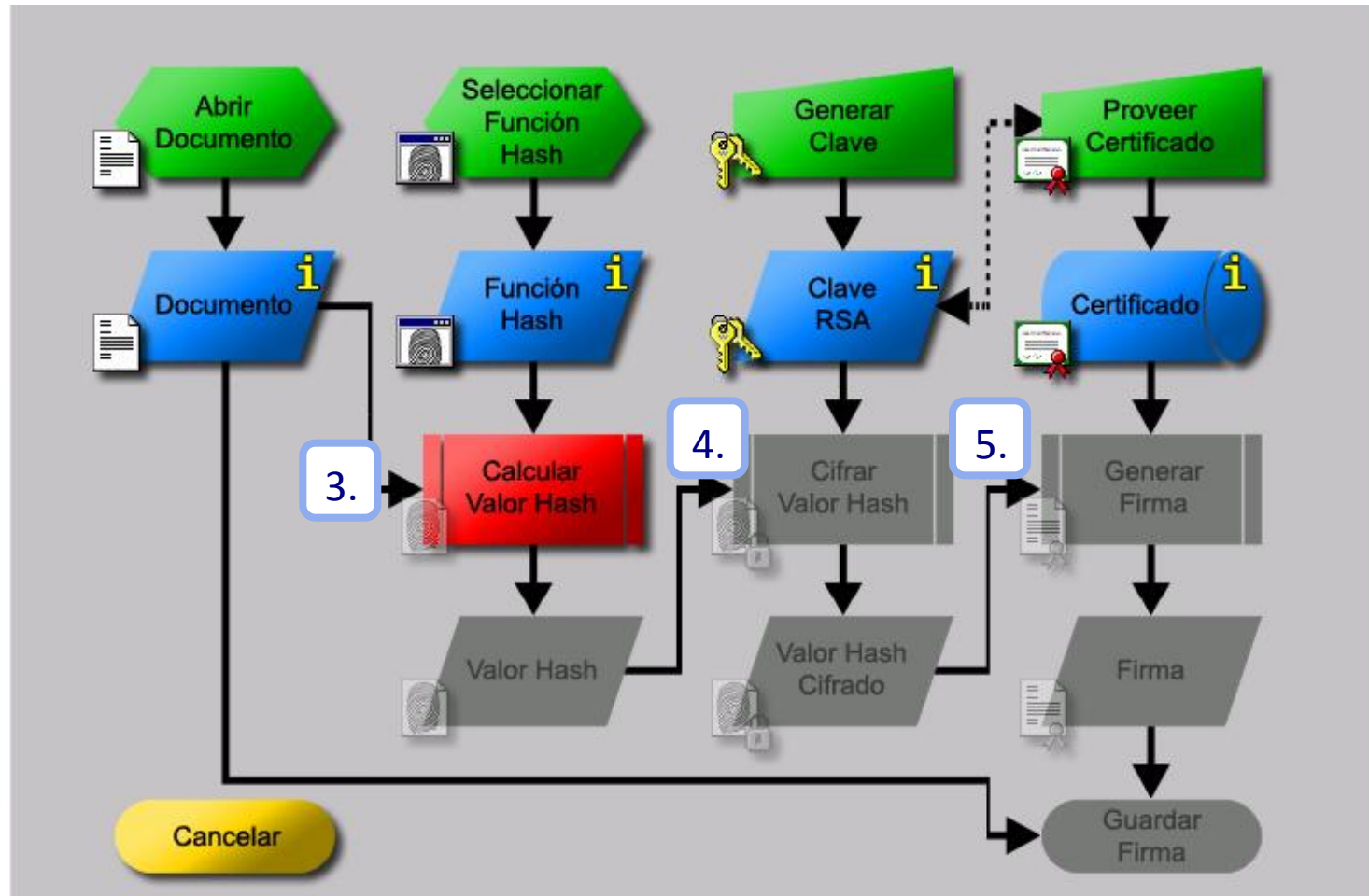
1. Seleccionar función hash

2. Facilitar clave y certificado (no se muestra aquí)



Ejemplos (2)

Visualización de una firma digital : b) Criptografía



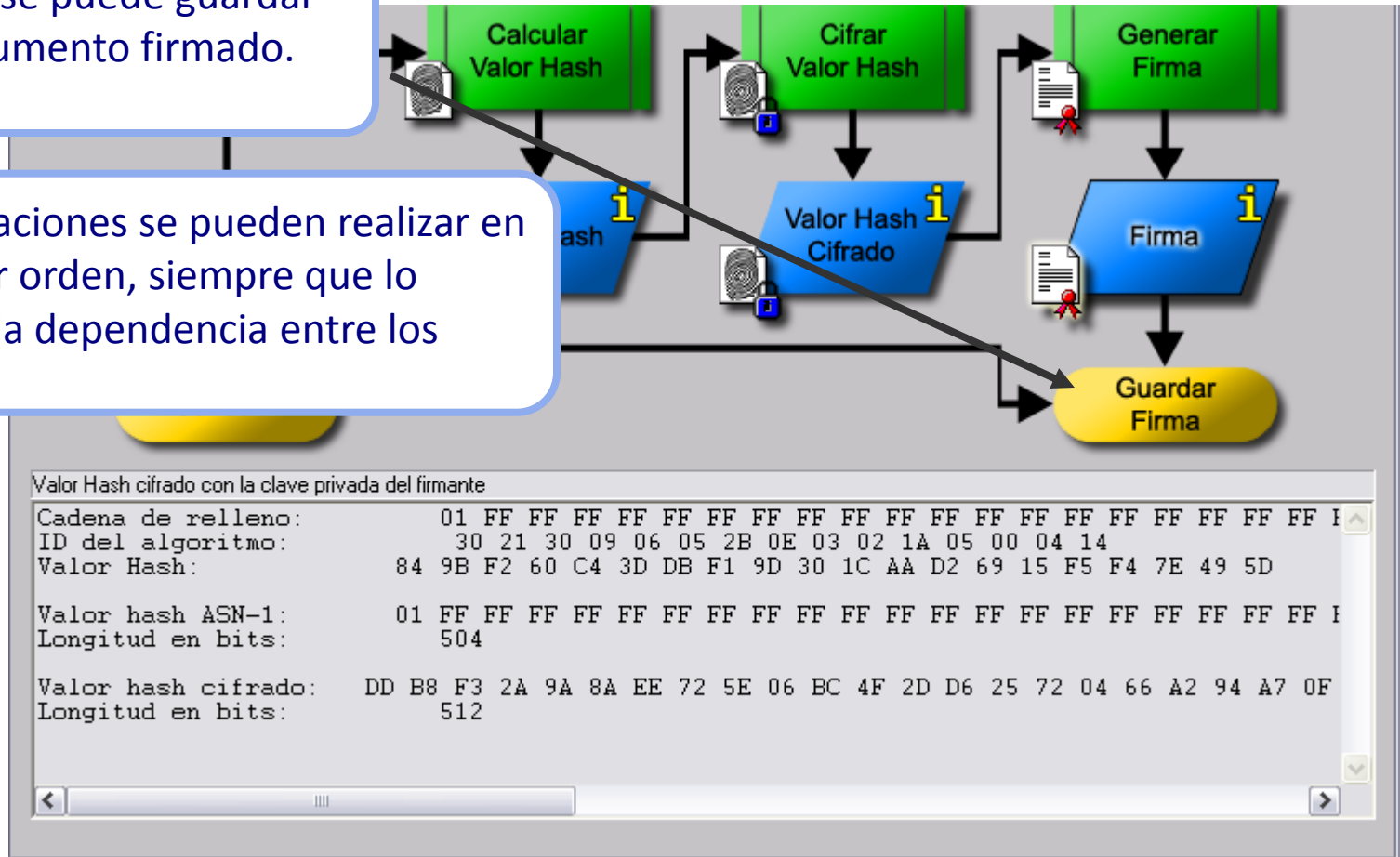
3. Calcular valor hash
4. Cifrar el valor hash con la clave privada (firmar)
5. Generar firma

Ejemplos (2)

Visualización de una firma digital : c) Resultado

6. Ahora se puede guardar el documento firmado.

Las operaciones se pueden realizar en cualquier orden, siempre que lo permita la dependencia entre los datos.



Ejemplos (3)

Ataque al cifrado RSA con un RSA de módulo pequeño

Ejemplo de *Song Y. Yan*, *Number Theory for Computing*, Springer, 2000

- Clave pública
 - Módulo RSA $N = 63978486879527143858831415041$ (95 bit, 29 dígitos decimales)
 - exponente publico $e = 17579$

- Texto cifrado(longitud de bloque = 8):

$$C_1 = 45411667895024938209259253423,$$

$$C_2 = 16597091621432020076311552201,$$

$$C_3 = 46468979279750354732637631044,$$

$$C_4 = 32870167545903741339819671379$$

¡El texto cifrado no se necesita para el criptoanálisis actual (localizar la clave privada)!

- ¡el texto debe ser descifrado!

Solución utilizando **CrypTool** (de forma más detallada en la sección de la ayuda online)

- Introducir parámetros públicos en “RSA Criptosistema ” (menú: “Procedimientos Indiv. ”)
- Botón “Factorizar módulo RSA” produciendo los dos factores primos $pq = N$
- Basado en la información del exponente privado se determina $d=e^{-1} \bmod (p-1)(q-1)$
- Descifrar el texto cifrado con d : $M_i = C_i^d \bmod N$

El ataque con CrypTool funciona para el módulo RSA hasta 250 bits.

¡Entonces podría firmar digitalmente por otra persona!

Ejemplos (3)

RSA de módulo pequeño: Introducir parámetros públicos del RSA

Menú: "Procedimientos. Indiv." \ "RSA Criptosistema" \ "RSA Demostración ..."

Demostración de RSA

RSA usando las Claves Pública y Privada o usando sólo la Clave Pública

Elija dos número primos p y q . El número $N = pq$ es el módulo público RSA y $\phi(N) = (p-1)(q-1)$ es la función phi de Euler. La clave pública e es prima relativa a $\phi(N)$ y la clave privada $d = e^{-1} \pmod{\phi(N)}$.

Para cifrar datos o comprobar un certificado es suficiente con introducir los parámetros públicos de RSA: el módulo N y la clave pública e

Ataque de Factorización

Para cifrar datos o comprobar un certificado es suficiente con introducir los parámetros públicos de RSA: el módulo N y la clave pública e .

Factorizar módulo RSA...

Parámetros RSA

RSA módulo N 49163 (público)

$\phi(N) = (p-1)(q-1)$ (secreto)

Clave Pública e $2^{16}+1$

Clave Privada d

Actualizar Parámetros

Cifrado RSA utilizando e / descifrado utilizando d

1. Introducir parámetros: "N" y "e"

2. Factorizar

Ejemplos (3)

RSA de módulo pequeño: Factorizar módulo RSA

Factorización de un Número

Algoritmos de Factorización

- Fuerza Bruta
- Algoritmo Brent
- Método Pollard
- Método Williams
- Algoritmo Lenstra
- Método Criba Cuadrática

Entrada

Introduzca el número a factorizar:

35237

Factorización (paso a paso)

Pulsando en el botón 'Continuar' irá viendo qué algoritmos se utilizan para factorizar, en primer lugar el valor de la entrada y después los números en rojo del campo resultado.

Continuar

Factorización

La factorización se representa en el formato $\langle z_1^{a_1} * z_2^{a_2} * \dots * z_n^{a_n} \rangle$.
Los números compuestos aparecen en color rojo.

Último método utilizado: Brute Force

Tiempo total necesario: 0,078 segundos.

Resultado de la Factorización:
167 * 211

Detalles

Cerrar

3. La factorización proporciona p y q

CrypTool

El módulo N de RSA ha sido factorizado satisfactoriamente en los primos p y q. Puede realizar la operación RSA con la clave secreta d: Para ello, haga click en el botón 'Descifrar'.

Aceptar

Ejemplos (3)

RSA de módulo pequeño: determinar la clave privada d

Demostración de RSA

Elija dos número primos p y q . El número $N = pq$ es el módulo público RSA y $\phi(N) = (p-1)(q-1)$ es la función phi de Euler. La clave pública e es prima relativa a $\phi(N)$ y la clave privada $d = e^{-1} \pmod{\phi(N)}$.

Para cifrar datos o comprobar un certificado es suficiente con introducir los parámetros públicos de RSA: el módulo N y la clave pública e

Entrada de número primo

Número primo p : 7997393 Generar números primos...

Número primo q : 2258651

Parámetros RSA

RSA módulo N : 18063319696843 (público)

$\phi(N) = (p-1)(q-1)$: 18063309440800 (secreto)

Clave Pública e : $2^{16}+1$

Clave Privada d : 5351989604673 Actualizar Parámetros

Cifrado RSA utilizando e / descifrado utilizando d

Entrada texto números Opciones del alfabeto y sistema numérico...

Cambia la visión del propietario de la clave secreta.

4. p y q se han introducido automáticamente y se ha calculado la clave privada

5. Ajustar Opciones



Ejemplos (3)

RSA de módulo pequeño: Ajustar Opciones

Opciones para la Demostración RSA

Opciones del Alfabeto

Todos los caracteres ASCII(256) Número de caracteres: 256

Alfabeto específico:

Variante RSA

Normal Diálogo de las Hermanas

Método para codificar un bloque en números

b-ádico Sistema Numérico

Longitud de bloque

El número de caracteres que es cifrado en cada operación del RSA.
El tamaño máximo está sujeto a la longitud del RSA modulo N en bits, el número de caracteres del alfabeto y el método de codificación empleado.

Longitud de bloque en caracteres: (Longitud máxima del bloque: 4 caracteres)

Sistema Numérico

Los números para las operaciones de cifrado y descifrado RSA serán representados en el siguiente sistema:

Decimal Binario Octal Hexadecimal

Aceptar Cancelar

6. Seleccionar alfabeto

7. Seleccionar método de codificación

8. Seleccionar longitud de bloque



Ejemplos (3)

RSA de módulo pequeño: Descifrar texto cifrado

Parámetros RSA

RSA módulo N	<input type="text" value="345947477033"/>	(público)
$\phi(N) = (p-1)(q-1)$	<input type="text" value="345946300500"/>	(secreto)
Clave Pública e	<input type="text" value="2^16+1"/>	
Clave Privada d	<input type="text" value="333504543473"/>	

Cifrado RSA utilizando e / descifrado utilizando d

Entrada texto números

Texto cifrado codificado en número de base 16

Descifrar mensaje $m[i] = c[i]^d \pmod{N}$

El texto de salida del proceso de descifrado (en segmentos de tamaño 4; el símbolo '#' es el usado como separa

Texto claro

9. Introducir texto cifrado

10. Descifrar

Ejemplos (4)

Análisis del cifrado utilizado en la PSION 5

Aplicación práctica del criptoanálisis:

*Ataque a la opción de cifrado de la aplicación de
Procesador de texto de la PDA PSION 5*

Punto de partida: un archivo cifrado con PSION

Requisitos

- Texto en alemán o en inglés cifrado
- Dependiendo del método y la longitud de la clave, texto desde 100 Bytes hasta varios kB

Procedimiento

- preanálisis
 - entropía
 - Entropía real
 - Test de compresión
- autocorrelación
- Intentar análisis automático con métodos clásicos

*Probablemente un
algoritmo de cifrado
clásico*



Ejemplos (4)

PDA PSION 5 – determinar entropía, test de compresión

The screenshot displays the CrypTool 1.4.21 interface. The main window shows a hex dump of the file 'psion-enc.hex'. A 'CrypTool' dialog box is open, displaying 'Tasa de compresión: 21 %' and an 'Aceptar' button. Below it, an 'Entropía <psion-enc.hex>' dialog box shows 'Este documento contiene los 256 valores posibles.' and 'La entropía del documento es 7.56 (la entropía máxima posible es 8.00)'. A graph titled 'Frecuencia real de <psion-enc.hex>' shows 'Caracteres diferentes por bloque de 64 bytes' on the y-axis (ranging from 40 to 60) and a logarithmic x-axis (1, 5000, 10000). The graph shows a noisy signal fluctuating between 45 and 60. A large blue watermark 't' is visible in the background.

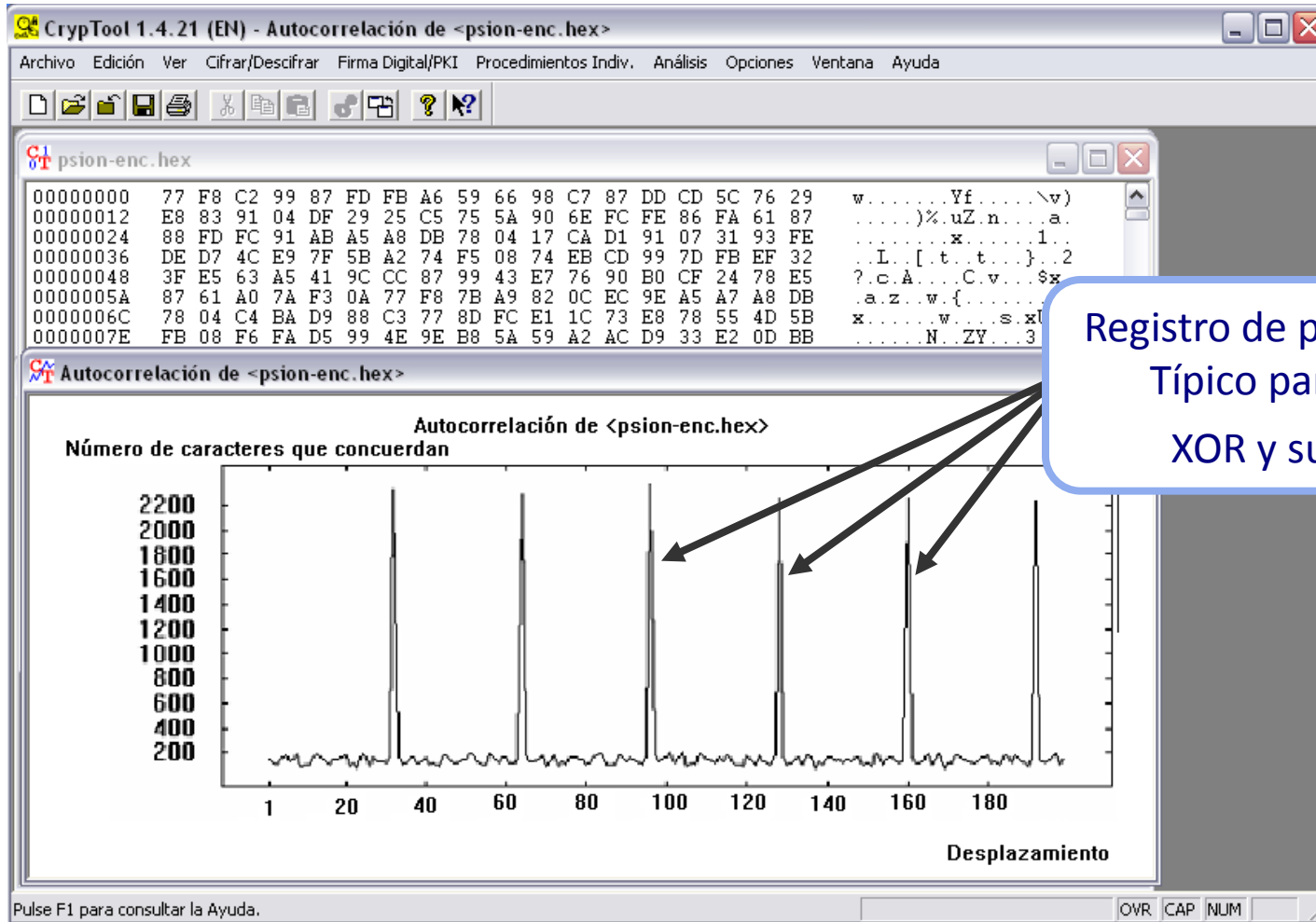
Comprendibilidad: indicador claro para la criptografía débil (se redujo el tamaño un 21%)

La entropía no proporciona información sobre el método de cifrado específico.

CrypTool 1.4.30

Ejemplos (4)

PDA PSION 5 – Determinar auto-correlación



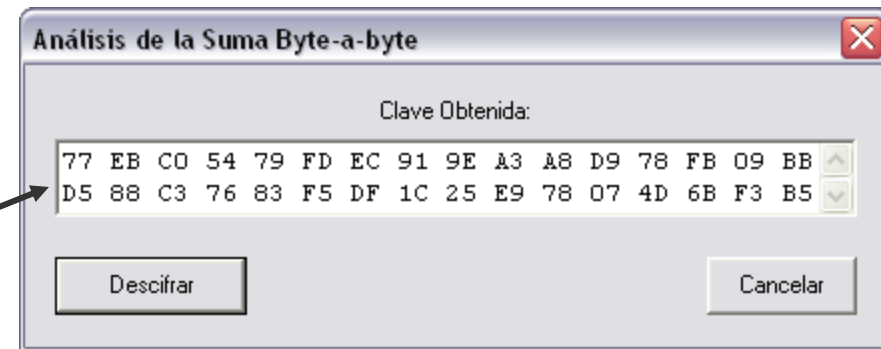
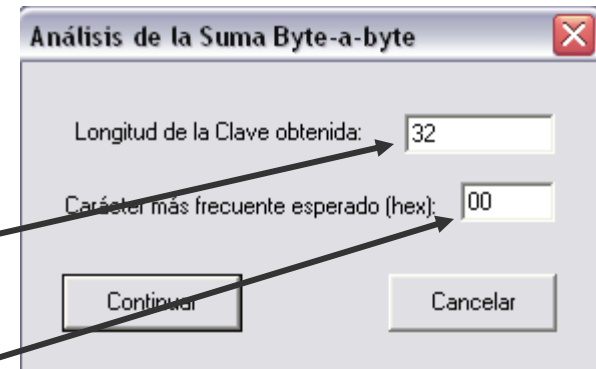
* El archivo cifrado está disponible en CrypTool (ver: CrypTool\examples\psion-en-enc.hex)

Ejemplos (4)

PDA PSION 5 – análisis automático

Análisis automático utilizando

- **Vigenère: sin éxito**
- **XOR: sin éxito**
- **Suma binaria**
 - CrypTool calcula la longitud de la clave utilizando la auto-correlación: 32 bytes
 - El usuario puede elegir el carácter que se espera que aparezca con mayor frecuencia:
“e” = 0x65 (código ASCII)
 - El análisis calcula la clave más probable (basada en las suposiciones sobre la distribución)
 - Resultado: bueno, pero no perfecto

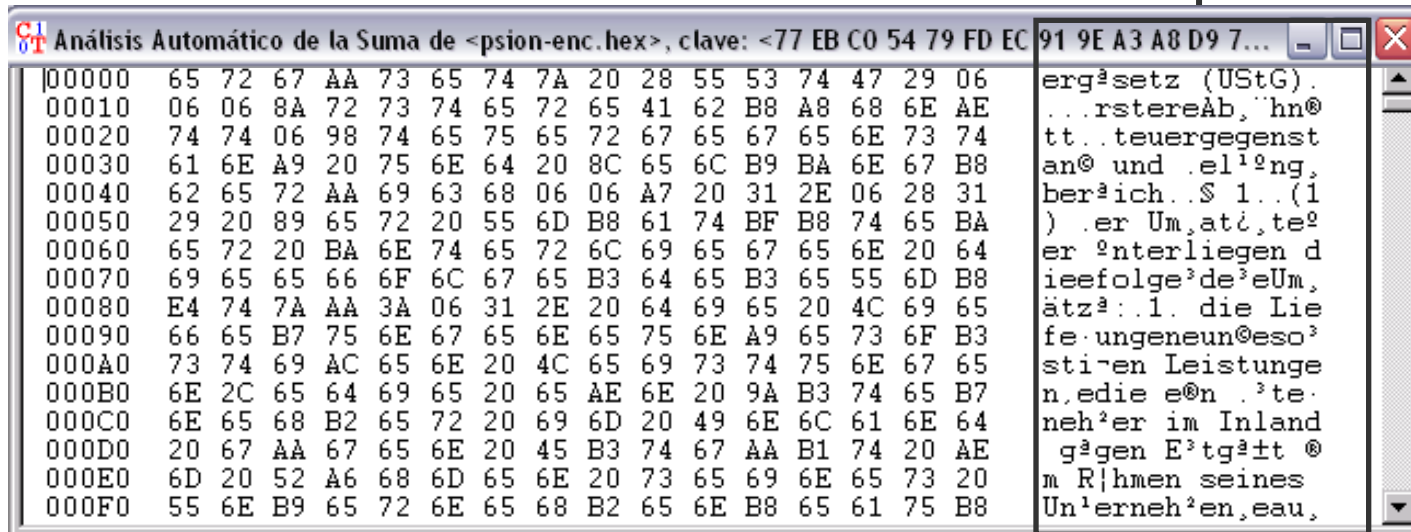


Ejemplos (4)

PDA PSION 5 – resultados del análisis automático

Resultados del análisis automático asumiendo “suma binaria”:

- El resultado es bueno, pero no perfecto: 24 de los 32 bytes de la clave son correctos.
- Se determina correctamente la longitud de la clave:32 .



```

Análisis Automático de la Suma de <psion-enc.hex>, clave: <77 EB C0 54 79 FD EC 91 9E A3 A8 D9 7...
|00000 65 72 67 AA 73 65 74 7A 20 28 55 53 74 47 29 06
|00010 06 06 8A 72 73 74 65 72 65 41 62 B8 A8 68 6E AE
|00020 74 74 06 98 74 65 75 65 72 67 65 67 65 6E 73 74
|00030 61 6E A9 20 75 6E 64 20 8C 65 6C B9 BA 6E 67 B8
|00040 62 65 72 AA 69 63 68 06 06 A7 20 31 2E 06 28 31
|00050 29 20 89 65 72 20 55 6D B8 61 74 BF B8 74 65 BA
|00060 65 72 20 BA 6E 74 65 72 6C 69 65 67 65 6E 20 64
|00070 69 65 65 66 6F 6C 67 65 B3 64 65 B3 65 55 6D B8
|00080 E4 74 7A AA 3A 06 31 2E 20 64 69 65 20 4C 69 65
|00090 66 65 B7 75 6E 67 65 6E 65 75 6E A9 65 73 6F B3
|000A0 73 74 69 AC 65 6E 20 4C 65 69 73 74 75 6E 67 65
|000B0 6E 2C 65 64 69 65 20 65 AE 6E 20 9A B3 74 65 B7
|000C0 6E 65 68 B2 65 72 20 69 6D 20 49 6E 6C 61 6E 64
|000D0 20 67 AA 67 65 6E 20 45 B3 74 67 AA B1 74 20 AE
|000E0 6D 20 52 A6 68 6D 65 6E 20 73 65 69 6E 65 73 20
|000F0 55 6E B9 65 72 6E 65 68 B2 65 6E B8 65 61 75 B8

```

erg²setz (UStG).
...rstereAb,`hn@
tt..teuergegenst
an@ und .el¹ng,
ber²ich..\$ 1..(1
) .er Um,at,te²
er ²nterliegen d
ieefolge³de³eUm,
ätz²..1. die Lie
fe .ungeneun@eso³
stiren Leistunge
n,edie e@n .³te
neh²er im Inland
g²gen E³tg²tt @
m R|hmen seines
Un¹erneh²en,eau,

- la contraseña introducida no tenía 32 bytes de longitud.
⇒ PSION Word deduce la clave actual de la contraseña.
- El post-procesado manual produce el texto cifrado (no se muestra)

Ejemplos (4)

PDA PSION 5 – determinar los bytes de clave restantes

Copiar la clave en el porta papeles durante el análisis automático

En análisis automático en hex dump,

- Determinar las posiciones de bytes incorrectos, p.ej. 0xAA en la posición 3
- Adivinar y escribir los bytes correctos: “e” = 0x65

En un archivo inicial hex dump cifrado

- Determinar los bytes iniciales de las posiciones de bytes calculadas: 0x99
- Calcular los bytes correctos de la clave con CALC.EXE: $0x99 - 0x65 = 0x34$

Clave desde el portapapeles

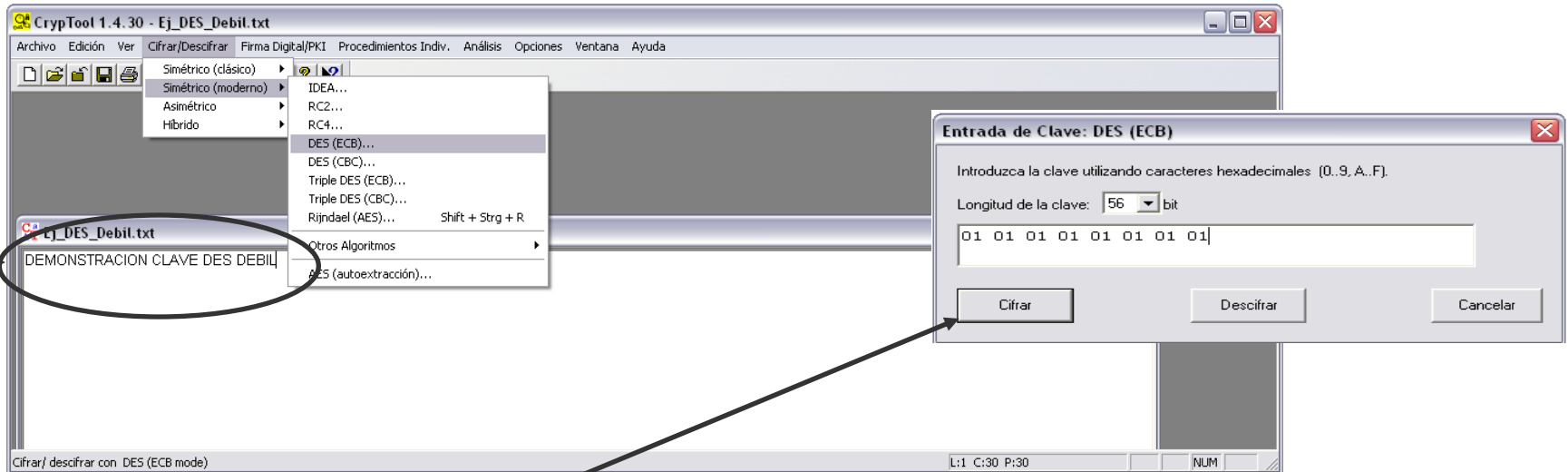
- Corrección 12865B**34**1498872C393E43741396A45670235E111E907AB7C0841...
- Descifrar el documento inicial cifrado utilizando la suma binaria
- bytes en la posición 3, 3+32, 3+2*32, ... Ahora son correctos

```
Análisis Automático de la Suma de <psion-enc.hex>, clave: <77 EB C0 54 79 FD EC 91 9... A3 A8 D9 7...
00000 65 72 67 65 73 65 74 7A 20 28 55 53 74 47 29 06  ergesetz (UStG).
00010 06 06 8A 72 73 74 65 72 65 41 62 B8 A8 68 6E AE  ...rstereAb,`hn@
00020 74 74 06 53 74 65 75 65 72 67 65 67 65 6E 73 74  tt.Steuergegenst
```

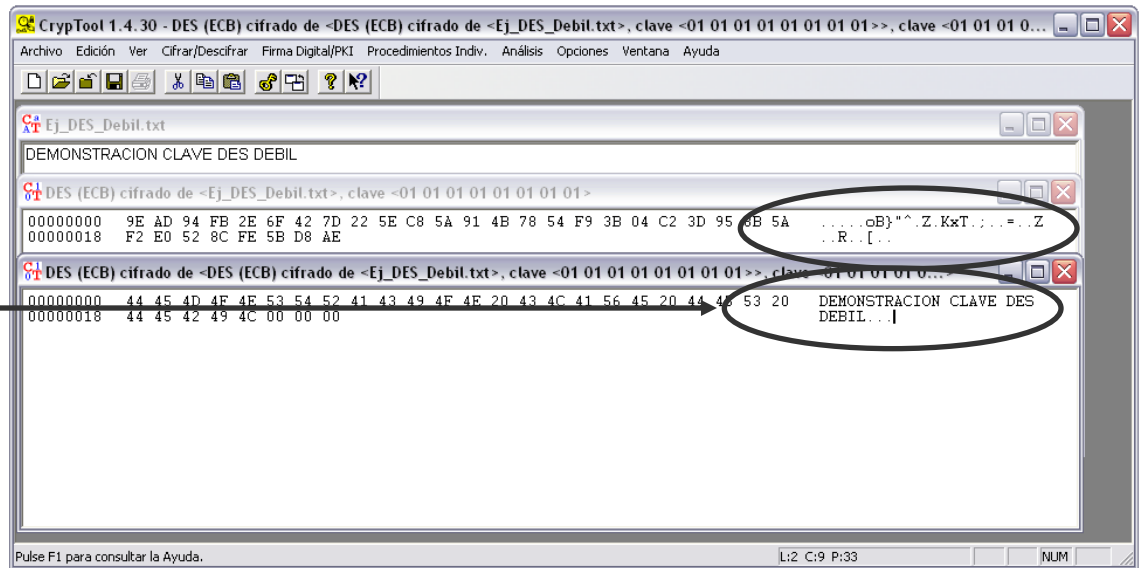


Ejemplos (5)

clave DES débil



Cifrando 2 veces con esta clave volvemos a obtener el texto claro



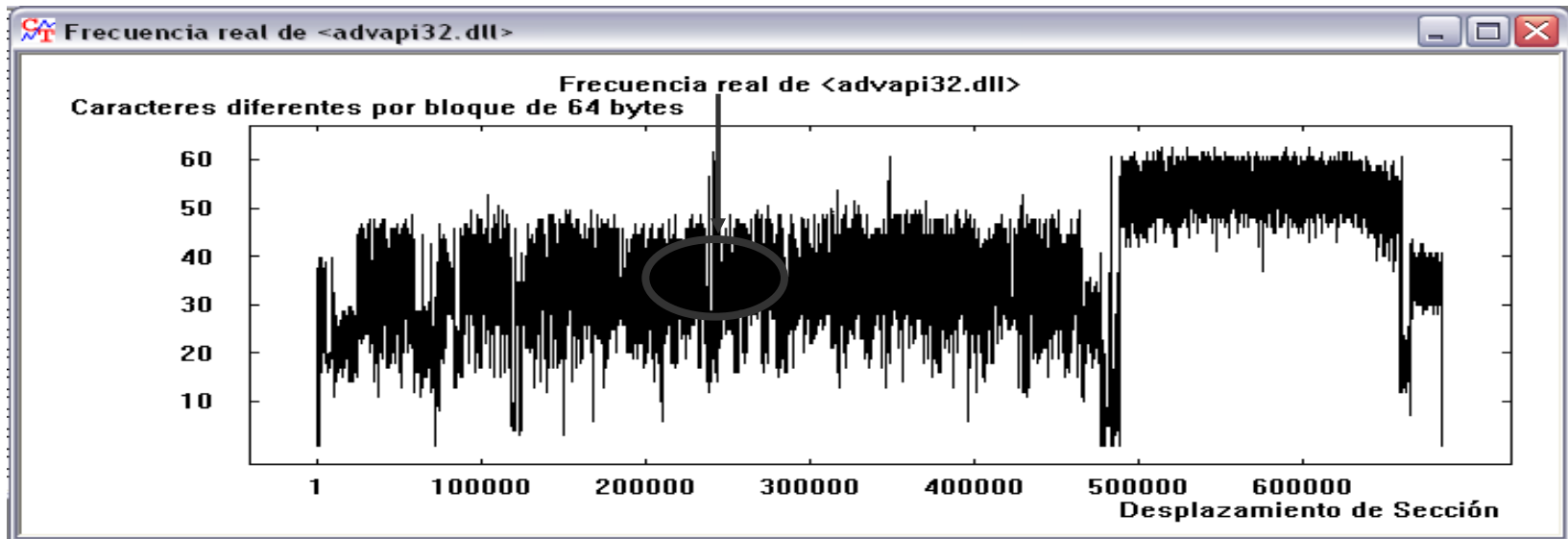
Ejemplos (6)

Localizar información de la clave

La función “Frecuencia real” es adecuada para localizar la información sobre la clave y áreas cifradas en archivos.

Trasfondo:

- Los datos de la clave son “más aleatorios” que el texto o el código programado
- Se puede reconocer como los picos en la “frecuencia real”
- Ejemplo: la “clave NSA” de advapi32.dll (Windows NT)



Ejemplos (6)

Comparación de frecuencia real con otros archivos

The screenshot displays the CryptTool 1.4.30 application interface. The main window shows the file 'startingexample-es.txt' with its content. Below the text, there are two frequency analysis plots. The top plot, titled 'Frecuencia real de <startingexample-es.txt>', shows the frequency of different characters per 64-byte block for the encrypted file. The bottom plot, titled 'Frecuencia real de <Startingexample-en.txt>', shows the same for the original file. The bottom window shows the Rijndael (AES) analysis results for the encrypted file, including a hex dump and the corresponding plaintext.

startingexample-es.txt

CrypTool (Ejemplo inicial para la familia de versiones 1.x de CrypTool)

CrypTool es una extensa herramienta educativa y libre sobre criptografía y criptoanálisis, con Ayuda Online y muchas visualizaciones.

Este fichero de texto tiene la intención de orientarle con sus primeros pasos en CrypTool.

- 1) Lo primero que se recomienda es que lea la ayuda incluida, que le proporcionará una idea general de todas las funciones disponibles con esta aplicación. A la página inicial de la ayuda se puede acceder a través del menú "Ayuda > Página de Inicio" o buscando "Starting page" en el índice de la ayuda, al que puede acceder pulsando la tecla F1.
- 2) Un posible segundo paso sería cifrar un fichero con un algoritmo de cifrado simétrico clásico (como por el ejemplo el algoritmo César). Esto lo haría a través del menú "Cifrar/Descifrar > Simétrico (clásico)". Puede encontrar guías y manuales de ayuda en las secciones de la ayuda.

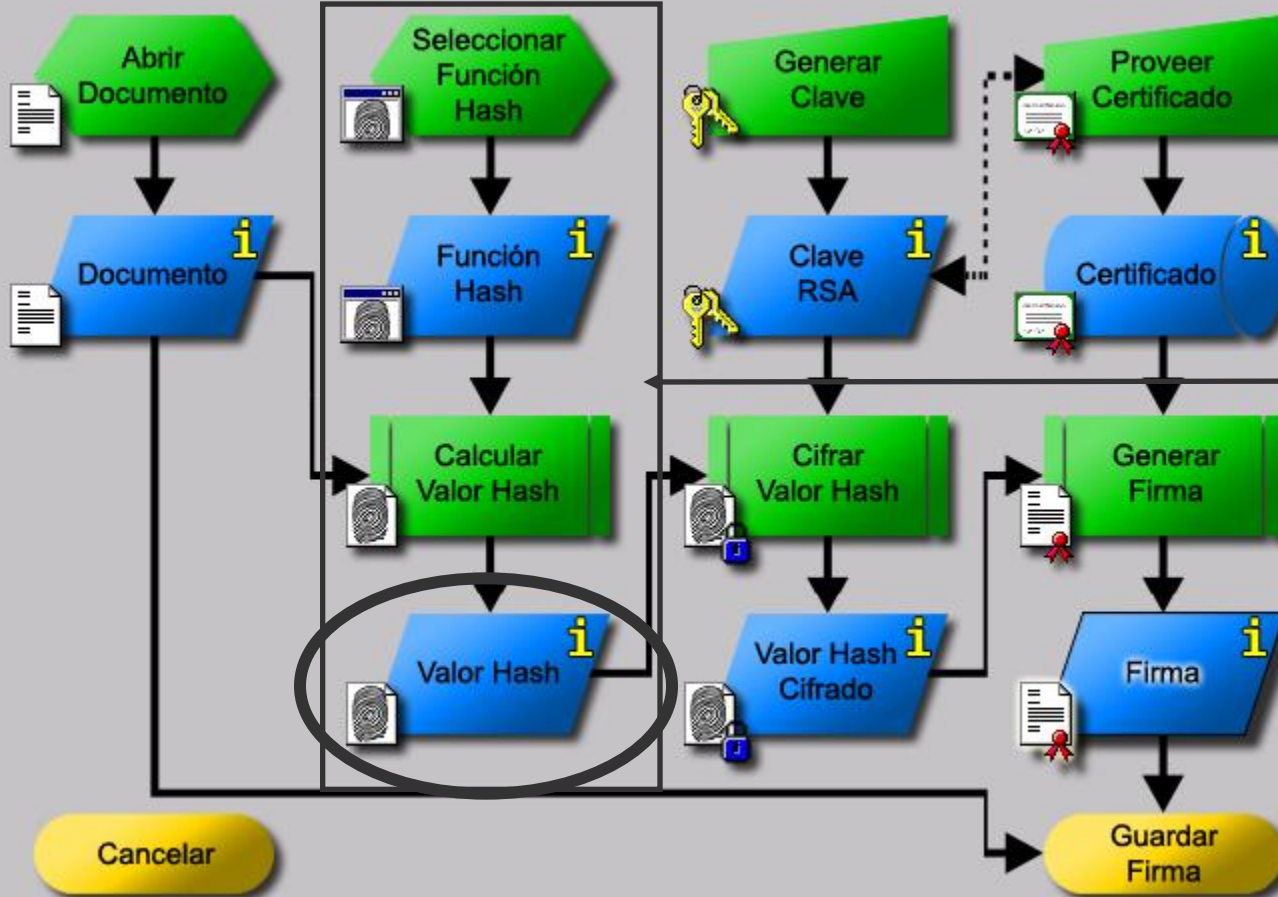
Rijndael (AES) Análisis de <Startingexample-en.txt>, clave: <269971...

00000000	E3 7F F7 C8 46 3A 33 CD C4 58 3C 32	...F:3..X<2
0000000C	A2 CF 02 97 F5 F9 AB 17 E0 D9 29 6En
00000018	AE 3B 32 D9 AD B3 5B 71 65 96 52 A2	..2...[qe.R.
00000024	FA 91 83 53 4B B3 79 15 AE 12 F9 C6	...SK.y....
00000030	23 39 37 91 09 FE 33 AE E3 E3 FE 1A	#97...3....
0000003C	72 D9 1C 0D CF 8B 44 65 F0 42 65 6E	r.....De.Ben
00000048	AE 83 97 D5 B7 0E E3 ED CD 79 8D BAy..
00000054	FE BA FE B6 1A B6 4C 29 20 A2 6B A5(L) .k.
00000060	02 84 1C 4B 0F D3 97 C4 A4 B6 5A F9	...K.....Z.
0000006C	A5 AC FB 9A 90 E5 82 EF 96 D9 A4 FA
00000078	2B C4 FA AB 40 0F 19 9F 1B 88 43 B0	+...@...C.
00000084	B5 7A 7E 78 A0 41 F8 6B C4 89 66 5E	z~x.A.k..f^
00000090	0F 5E 3C 01 4B D9 D4 E4 51 8B 8C CE	<<.K...Q...
0000009C	9A 61 36 94 82 F2 5C 4A 30 C0 CF 44	.a6...J0...D
000000A8	29 F7 49 9D 31 02 5A 8E DB 21 DE 57).I.1.Z...!W
000000B4	2E F3 85 7A 21 81 B1 6C 81 64 4F D0	...z!...l.d0.
000000C0	AB 21 FB 7D 95 70 60 0F D1 37 82 8E	!..}..p...7...
000000CC	3B 35 6D 29 8E 0B 1F 09 0A ED B8 3E	:5m).....>
000000D8	AC 98 97 81 3D B9 26 01 99 F5 89 F4	...=...&.....
000000E4	76 28 9A 3B E2 AB 03 93 DA 53 67 DD	v(...).Sg.
000000F0	69 23 AE 47 09 28 8D 6D 75 02 A3 10	i#.G...(.mu...

Pulse F1 para consultar la Ayuda. L:7 C:224 P:530 NUM

Ejemplos (7)

Ataque a la firma digital



Ataque:

¡Encontrar dos mensajes con el mismo valor hash!

Menú: "Análisis" \ "Hash" \ "Ataque al valor Hash de una firma digital"

Ejemplos (7)

Ataque a la firma digital– idea (I)

Ataque a la firma digital de un texto en ASCII basado en la búsqueda de colisiones.

Idea:

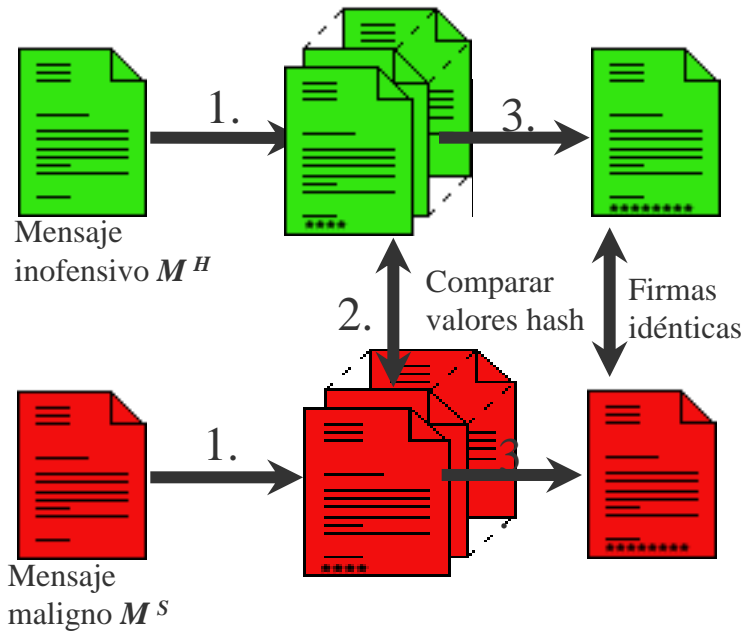
- Los textos ASCII se pueden modificar cambiando/insertando caracteres **no imprimibles**, sin cambiar el contenido visible
- Modificar dos textos en paralelo hasta encontrar una colisión hash
- Aprovechar la paradoja del cumpleaños (ataque del cumpleaños)
- Ataque genérico aplicable también a las funciones hash
- Se puede ejecutar en paralelo en varias máquinas (no está implementado)
- Se ha implementado en CrypTool como parte de la tesis de un licenciado “*Métodos y herramientas para ataques a firmas digitales*” (alemán), 2003.

Conceptos:

- Mapeados
- Algoritmo de Floyd modificado (consumo de memoria constante)

Ejemplos (7)

Ataque a la firma digital– idea (II)



- 1. Modificación:** empezando desde un mensaje M se crean N mensajes distintos M_1, \dots, M_N con el mismo “contenido” como M .
- 2. Búsqueda:** encontrar mensajes modificados M_i^H y M_j^S con el mismo valor hash.
- 3. Ataque:** las firmas de ambos documentos M_i^H y M_j^S son iguales.

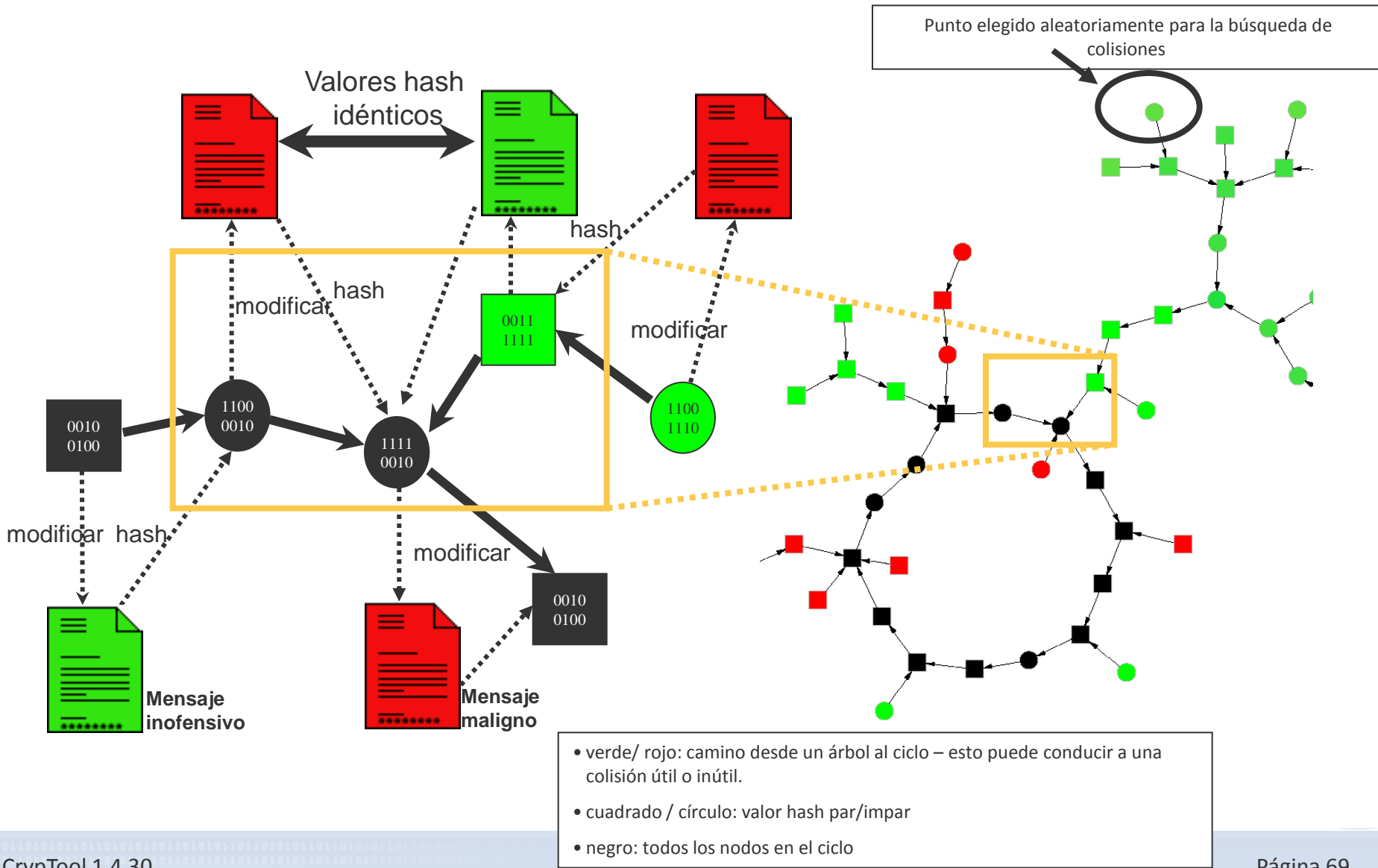
Conocemos por la paradoja del cumpleaños que para valores hash de longitud n en bits:

- buscar colisiones entre M^H y M_1^S, \dots, M_N^S : $N \approx 2^n$
- Buscar colisiones entre M_1^H, \dots, M_N^H y M_1^S, \dots, M_N^S : $N \approx 2^{n/2}$ ↑

Número estimado de mensajes generados para encontrar una colisión hash.


Localizar Colisiones Hash (1)

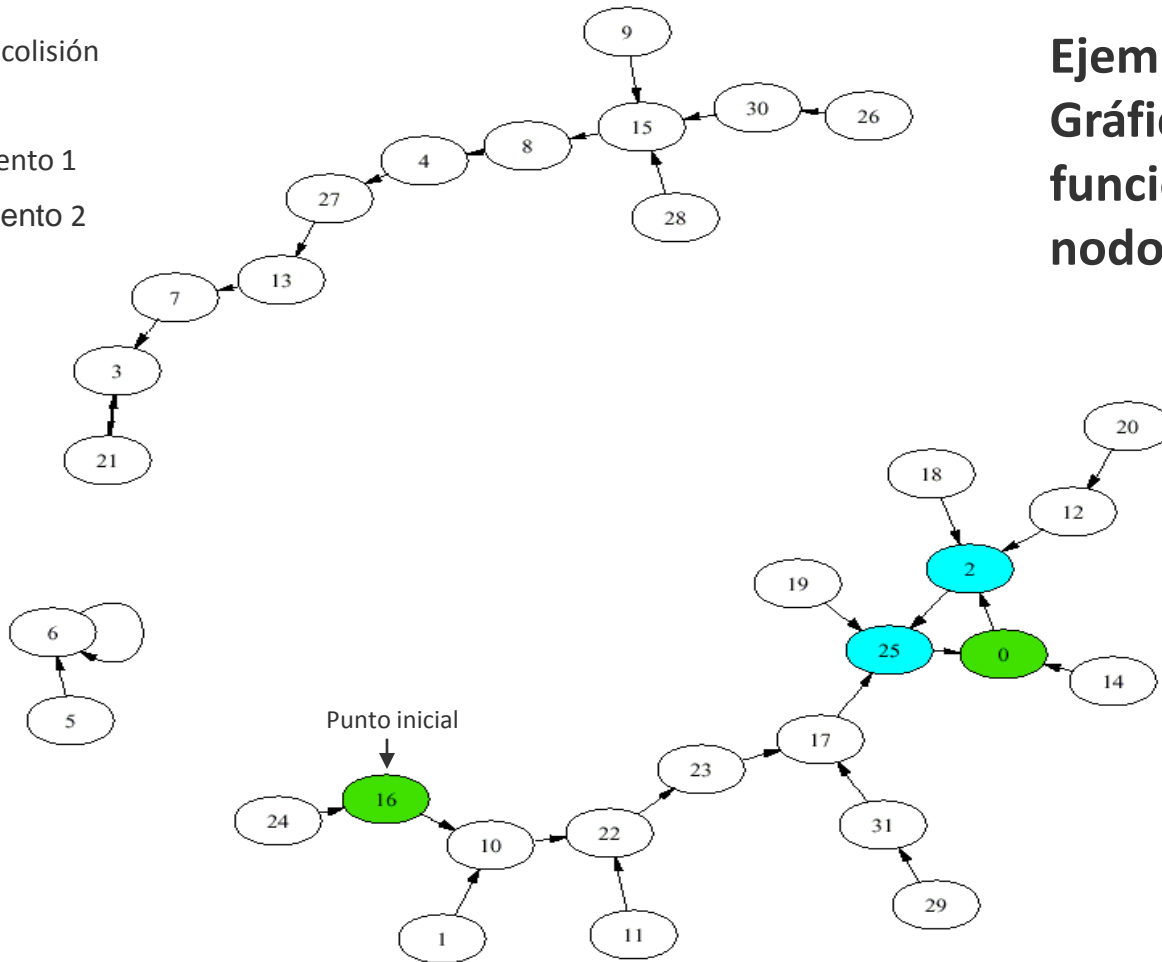
Mapeado por modificaciones del texto



Localizar Colisiones Hash (2)

Algoritmo de Floyd: encontrar el ciclo

-  inicio / colisión
-  ciclo
-  incremento 1
-  incremento 2



Ejemplo:
Gráfico de una
función con 32
nodos

Paso 1: Localizar el punto que concuerde con el ciclo:





- Dos series con idéntico punto de inicio[16]: una serie con incremento 1, la otra con incremento 2.

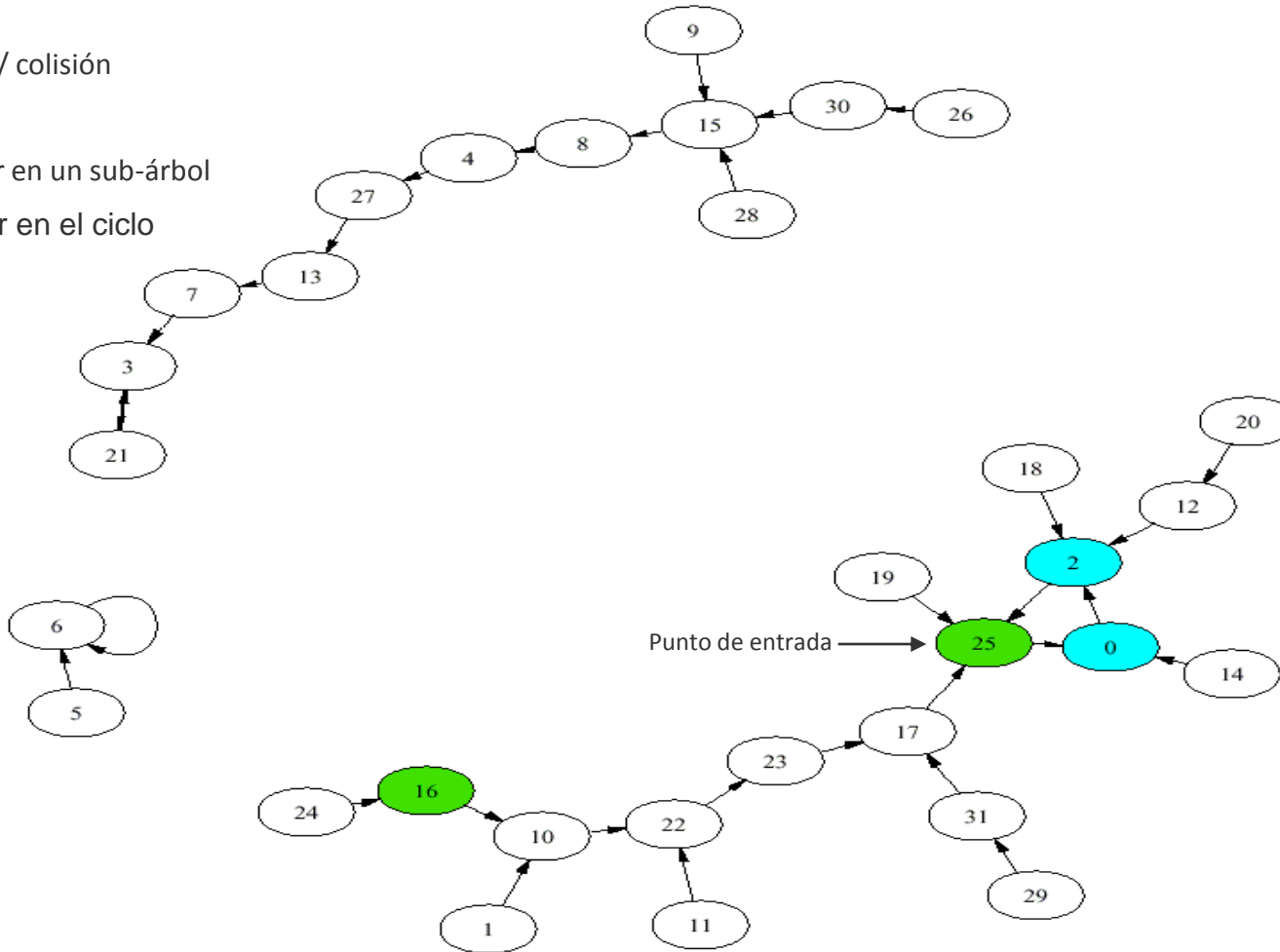
Resultado (basado en teoría de grafos):

- Ambas series siempre terminan en un ciclo.
- Ambas series coinciden en un nodo en el ciclo (en este caso 0).

Localizar Colisiones Hash (3)

Seguir el ciclo (Extensión de Floyd): encontrar el punto de entrada

-  inicio / colisión
-  ciclo
-  Mover en un sub-árbol
-  Mover en el ciclo



Paso 2: Localizar el punto de entrada de las series 1 en el ciclo [25]:

- La Serie 1 empieza otra vez desde el punto de entrada; la serie 3 con un incremento de 1 empieza en el punto de encuentro con el ciclo (en este caso en 0).

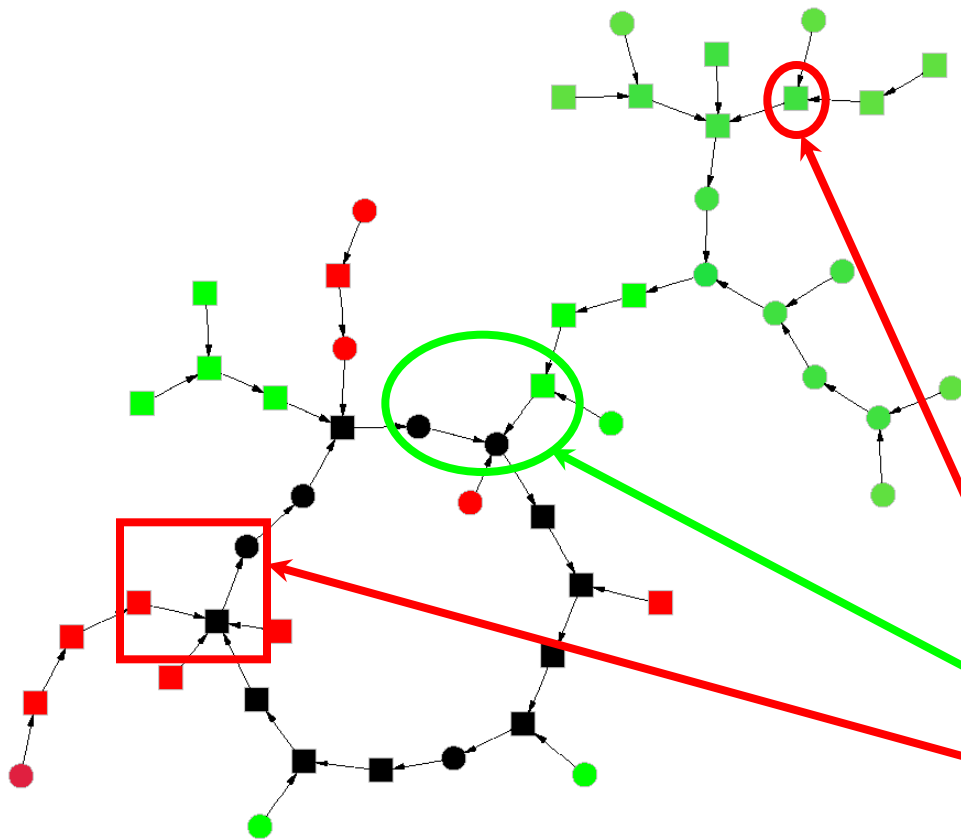
Resultado: Las series (1 y 3) coinciden en el punto de entrada del ciclo de la serie 1 (en este caso 25)

- Los predecesores (en este caso 17 y 2) resultan en una colisión hash.

Ataque de la Paradoja del Cumpleaños a la Firma Digital

Examinar el algoritmo Floyd

- Presentación visual e interactiva del algoritmo Floyd (“Desplazándose a través del mapeo” en un ciclo).
- Adaptación del algoritmo de Floyd para un ataque de firma digital.



Punto Inicial

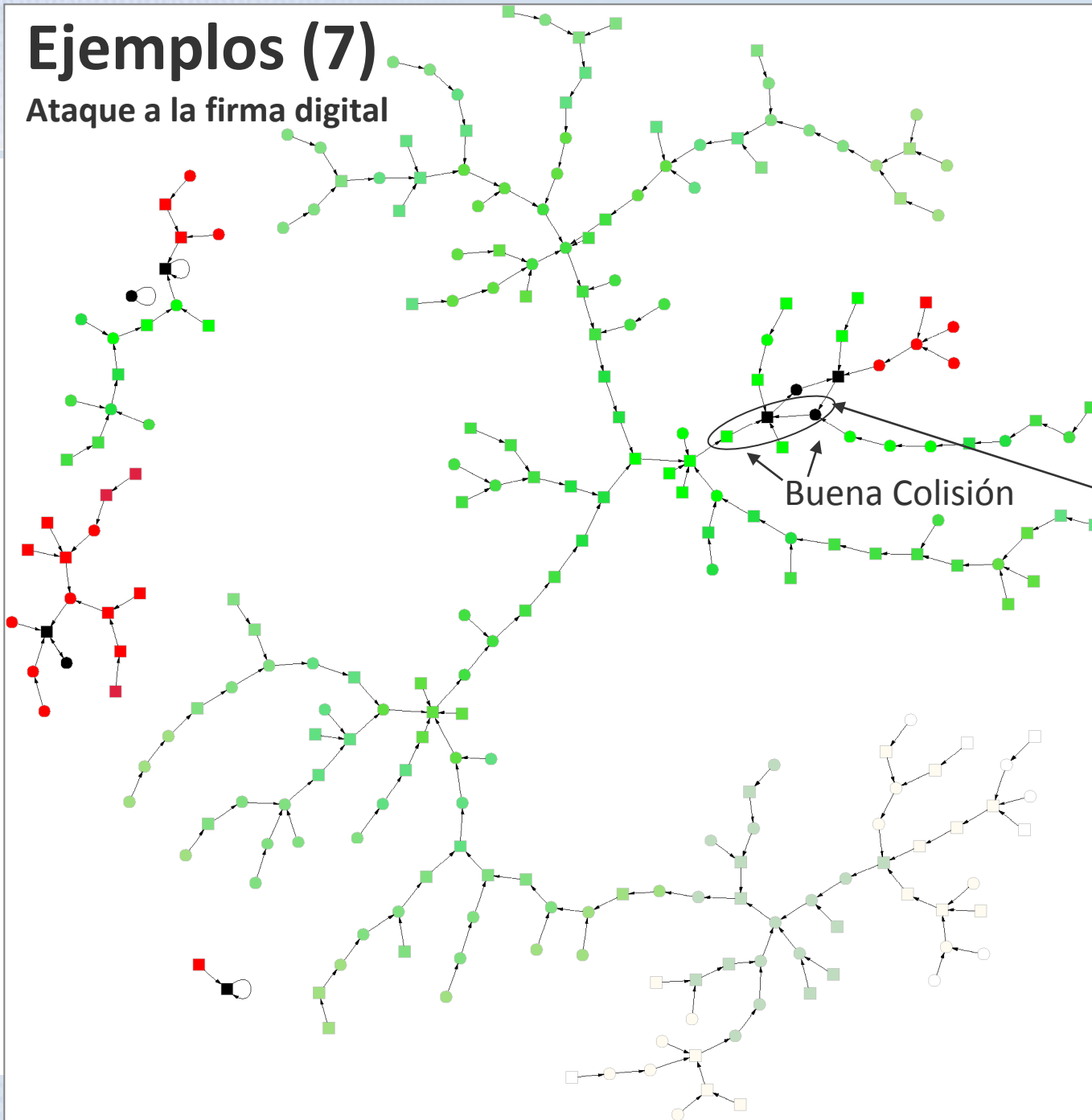
Buena colisión

Mala colisión

*El algoritmo de Floyd se implementa en CrypTool, pero la visualización del algoritmo aún no está implementada.

Ejemplos (7)

Ataque a la firma digital



Un ejemplo de un “buen” Mapeado (casi todos los nodos son verdes). En este grafo casi todos los nodos pertenecen al árbol grande, el cual se encuentra con el ciclo cuando se igualan los valores hash y donde el predecesor al punto de entrada en el ciclo es impar. Esto significa que el atacante encuentra útil la colisión para casi cualquier punto de inicio.

Ejemplos (7)

Ataque a la firma digital: Ataque

The image displays the CryptTool interface for a digital signature attack. The main window is titled "Ataque al Valor Hash de una Firma Digital". It contains several sections:

- 1.** "Elija el mensaje 'inofensivo'": A text box with the path "C:\Archivos de programa\CrypTool\examples\original.txt" and an "Examinar ..." button.
- 2.** "Elija el mensaje 'peligroso'": A text box with the path "C:\Archivos de programa\CrypTool\examples\fake.txt" and an "Examinar ..." button.
- 3.** "Opciones ...": A button to open the options dialog.
- 4.** "Iniciar Búsqueda": A button to start the attack.

The "Opciones para el Ataque al valor Hash de la Firma Digital" dialog box is open, showing:

- Función Hash:** Radio buttons for MD2, MD4, MD5 (selected), SHA, SHA-1, and RIPEMD-160.
- Número de bits:** A text box containing "40" and "(Co-dominio: 1 - 128)".
- Opciones para la modificación de los mensajes:** Checkboxes for "Insertar espacios" and "Añadir caracteres" (selected). Radio buttons for "Al inicio", "Espacio", "Carácter", and "Carácter" (selected).

Two progress dialog boxes are shown:

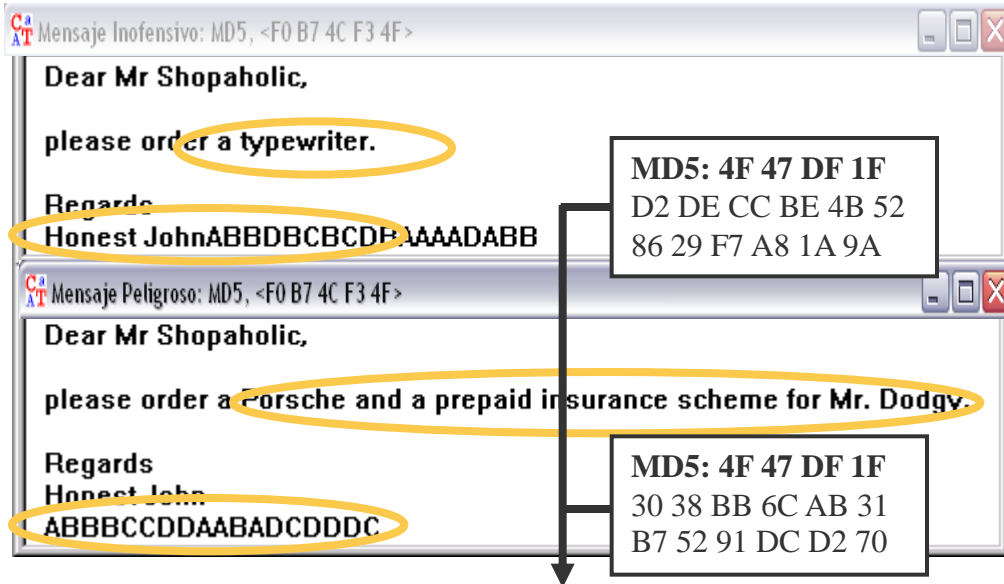
- Buscando un par de mensajes... (Ejecución 1):** "Ciclo de búsqueda (40 bit)", "Progreso: 29% tiempo restante: 00:00:03".
- Buscando un par de mensajes... (Ejecución 2):** "Ciclo de búsqueda (40 bit)", "Progreso: 37% tiempo restante: 00:00:05".

Numbered callouts 1, 2, 3, and 4 are placed around the main window. An arrow points from the "Opciones ..." button (3) to the options dialog box.

Menú: "Análisis" \ "Hash" \ "Ataque en el valor Hash de una Firma Digital"

Ejemplos (7)

Ataque a la firma digital: Resultados



Los primeros 32 bits de los valores hash son idénticos.

Adicionalmente al manejo manual:

Característica automática desconectada en CrypTool: Ejecuta y registra los resultados para todos los conjuntos de configuraciones de parámetros. Disponible a través de la ejecución de CrypTool por línea de comandos.

Resultados Experimentales

- Colisión parcial de 72 Bit (igualdad para los valores has de los primeros 72 bits) se encontró en un par de días en un único PC.
- ¡Las firmas que utilizan valores hash de hasta 128 bits se pueden atacar hoy en día con búsqueda en paralelo!
- Utilizar valores has de como poco 160bits de longitud.

Ejemplos (8)

Autenticación en un entorno cliente-servidor

Contraseñas de un sólo uso: Para intentar evitar el ataque del escenario anterior, el cliente y el servidor 1 han acordado cambiar la contraseña después de que tenga lugar una autenticación. De este modo, han creado una lista de contraseñas de un sólo uso que ambos conocen y pueden utilizar; de esta forma, después de que se utilice una contraseña, ésta es marcada como utilizada y no puede volver a ser usada. Para la próxima autenticación, se utilizará otra contraseña de la lista.

De nuevo, su labor es la de autenticarse ante el servidor 1 que está a la espera de que lo haga el cliente.

- Demostración interactiva para distintos métodos de autenticación.
- Oportunidades definidas del atacante.
- Puede tomar el papel del atacante.
- **Moraleja:** Sólo es segura la autenticación mutua.

Menú: “Procedimientos Indiv.” \ “Protocolos” \ “Autenticación en Red”

Ejemplos (9)


Demonstración de un ataque de canal lateral (en un protocolo de cifrado híbrido)

Ataque de Canal Lateral contra un protocolo de cifrado híbrido (RSA)


Ataque paso a paso

- Introducción al Escenario
- Ejecutar Preparación
- Transmitir Mensaje
- Descifrar Mensaje
- Interceptar Mensaje
- Comenzar Ciclo de Ataque
- Generar Informe


Alice [Cliente]



Bob [Server]



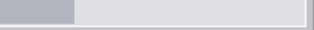
Trudy [Atacante]



Control del ataque:

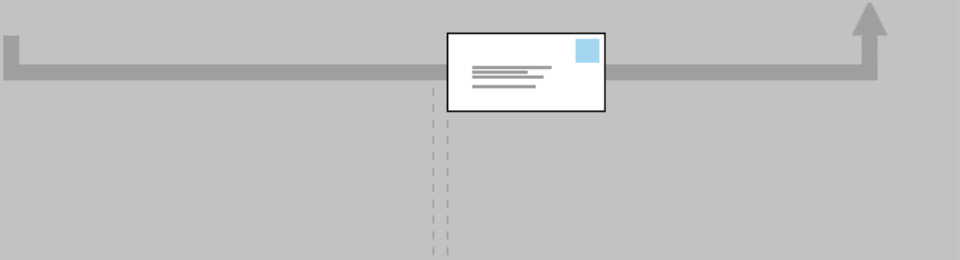
- Paso Siguiente
- Todos los pasos a la vez

Progreso del ataque:



Mostrar diálogo de información

Salir



Menú: "Análisis" \ "Cifrado Asimétrico" \ "Ataque de canal lateral"

Ejemplos (9)

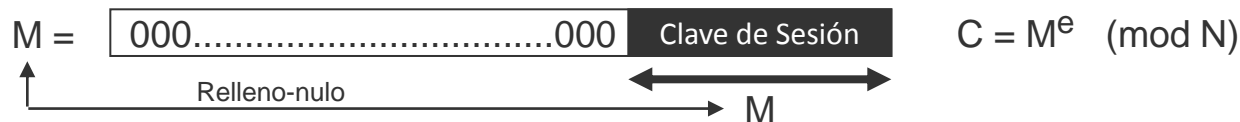
Idea para este ataque de canal lateral

Ulrich Kühn “Side-channel attacks on textbook RSA and ElGamal encryption” (2003)

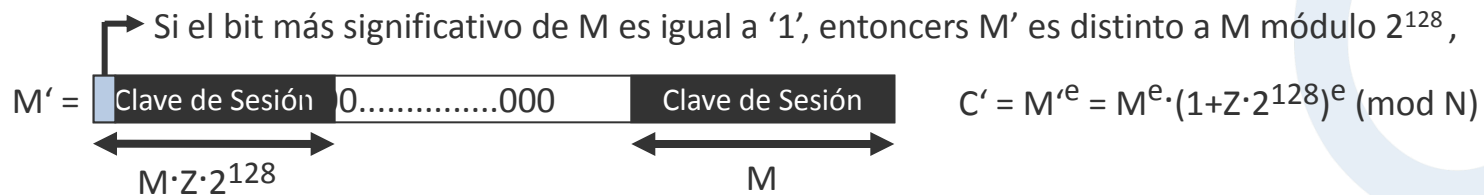
Prerrequisitos:

- Cifrado RSA: $C = M^e \pmod{N}$ y descifrado: $M = C^d \pmod{N}$.
- Las Claves de sesión de 128-Bits (en M) están “cifradas por diccionario” (relleno nulo).
- El servidor conoce la clave secreta d y
 - La utiliza después de descifrar sólo los 128 bits menos significativos (sin validación de los bits 0 de relleno) (esto significa que el servidor no reconoce si hay algo distinto a cero).
 - Avisos y mensajes de error, si del intento de cifrado resulta una clave de sesión errónea (el texto descifrado no se puede interpretar en el servidor). En el resto de casos no habrá mensajes.

Idea para el ataque: Aproximación para Z en la ecuación $N = M * Z$ para cada $M = \lfloor N/Z \rfloor$



Se calculan de forma sucesiva todas las posiciones de bits para Z: En cada paso se toma un bit más. El atacante modifica C a C' (ver más abajo). Si ocurre un desbordamiento de bits mientras se calcula M' en el servidor (receptor), el servidor envía un mensaje de error. Basándose en esta información, el atacante obtiene un bit para Z.



Ejemplos (10)

Matemáticas: Ataques a RSA utilizando reducción de retículos (Lattice Reduction)

Ataque a claves demasiado cortas (según Bloemer / May)

Descripción
Este ataque permite factorizar un módulo N de RSA siempre que la clave secreta d elegida sea suficientemente pequeña en comparación con N . El número $\delta = \log(d)/\log(N)$ es llamado "tamaño de d ". Este ataque es posible para deltas < 0.290 .

- Para aplicar ejemplos de la bibliografía, puede introducir la clave pública (N, e) . Después introduzca el valor estimado de delta, o bien, puede introducir directamente el d que es utilizado para calcular delta.
- Para generar un ejemplo aleatorio introduzca los parámetros delta y la longitud (en bits) de N . Pulsando sobre 'Generar Clave Aleatoria' se generarán las claves.

Después pulse sobre

Paso 1: Introduzca la clave y sus parámetros

Longitud de N : delta:

N :

e :

d :

Paso 2: Introduzca parámetros para la reducción de la celosía

m : Determina el tamaño de la celosía a reducir y el tamaño máximo de delta. Debe ser al menos 4.

t : Se calcula óptimamente en función de m .

Dimensión de la celosía: Tamaño a reducir de la celosía. Tiene un impacto importante en el tiempo

Maximal delta: Maximal size of delta for big N ($N > 1000$ Bit).

Paso 3: Iniciar Ataque

Construyendo:

Reduciendo: Reducciones:

Calculando resultado: Resultantes:

Tiempo Total:

Factorización

p : q :

- Muestra cómo se tienen que elegir los parámetros del método RSA, por eso el algoritmo resiste al ataque de reducción de retículos descrito en la bibliografía.

- **3 variantes**

1. El exponente secreto d es demasiado pequeño en comparación con N .
2. Se conoce parcialmente a uno de los factores de N .
3. Se conoce una parte del texto claro.

- Estas suposiciones son realistas.

Menú: "Análisis" \ "Cifrado Asimétrico" \ "Colección de ataques basados en RSA" \ ...

Ejemplos (11)

Análisis de Aleatoriedad con visualización 3-D

Visualización 3D para el análisis de aleatoriedad

Ejemplo 1

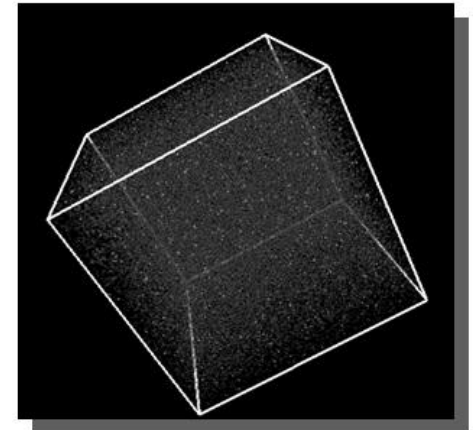
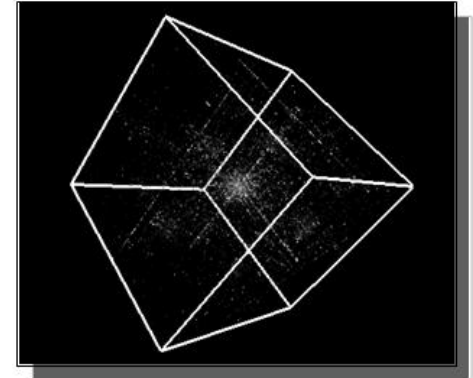
- Abrir un archivo arbitrario (p.ej. Un informe en Word o una presentación de PowerPoint)
- Se recomienda seleccionar un archivo de al menos 100 Kb
- Análisis 3D
- Resultado: **se reconocen fácilmente las estructuras**

Ejemplo 2

- Generación de números aleatorios: “Procedimientos Individ.” \ “Herramientas” \ “Generar Números Aleatorios”
- Se recomienda generar al menos 100.000 bytes aleatorios
- Análisis 3D
- Resultado: **distribución uniforme (no se reconocen las estructuras)**

Menú: “Análisis” \ “Análisis de Aleatoriedad” \ “Visualización 3D”

Puede girar el cubo con el mouse para obtener una mejor perspectiva.

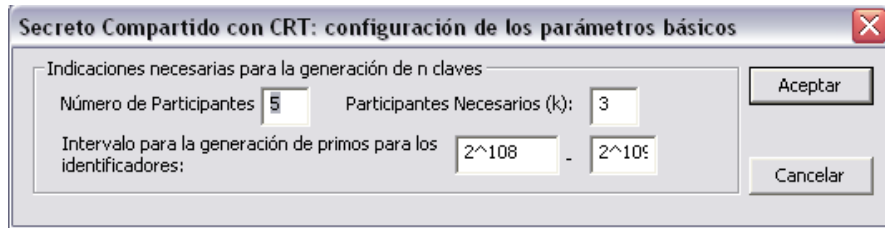


Ejemplos (12)

Secreto Compartido con CRT – Implementación del Teorema Chino de los Restos (CRT)

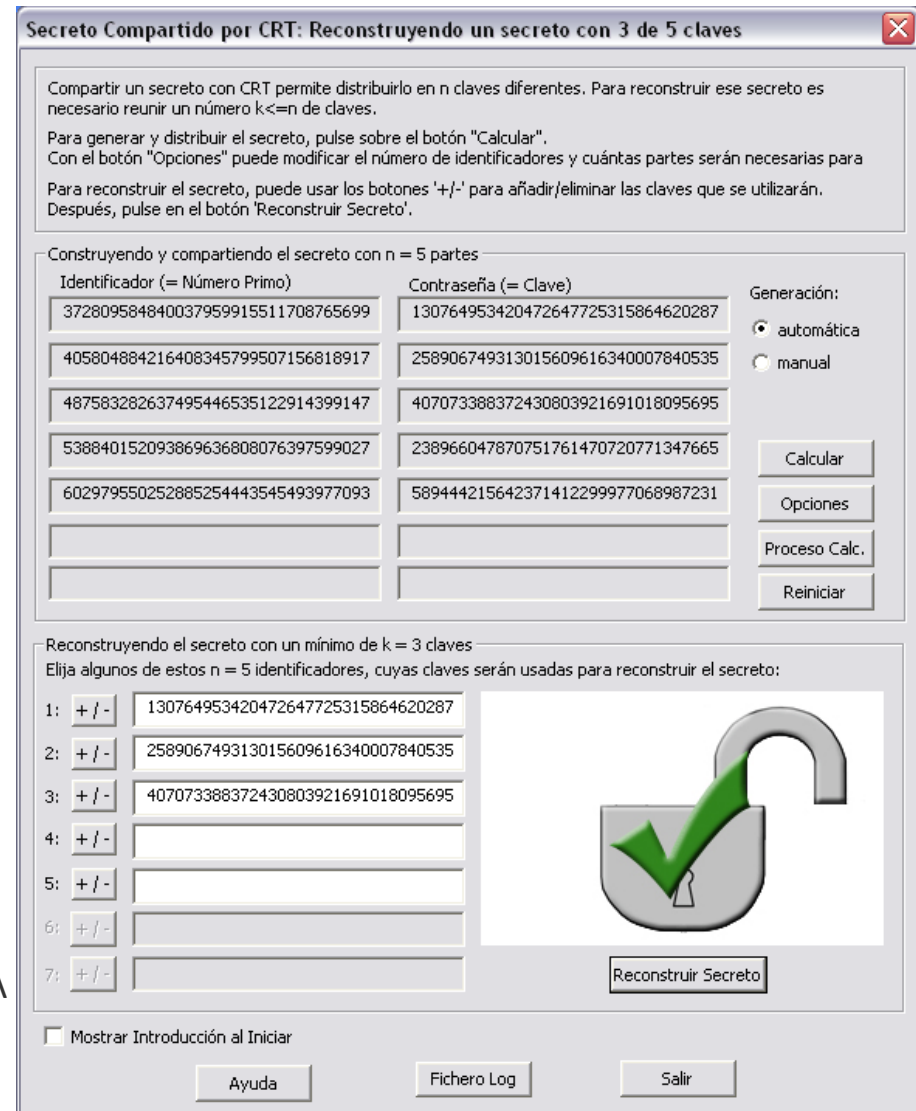
Ejemplo de Secreto compartido (1):

- **Problema:**
 - 5 personas tienen una clave
 - Para ganar acceso al menos 3 de esas 5 personas tienen que estar presentes
- **“Opciones”** permite configurar los detalles del método.



- **“Pasos de Calc.”** muestra todos los pasos para generar la clave.

Menú: “Procedimientos Indiv.” \
“Aplicaciones del Teorema Chino de los Restos” \
“Secreto Compartido por CRT”



Ejemplos (12)

Secreto Compartido de Shamir

Ejemplo Secreto Compartido (2)

■ Problema

- Un valor secreto se puede separar para n personas.
- t de las n personas se necesitan para recuperar el valor secreto K .
- (t, n) esquema de borde

■ Realizar lo siguiente:

1. Introducir el secreto K , número de personas n y el umbral t
2. Generar polinomio
3. Utilizar Parámetros
4. Utilizando “**Reconstrucción**” se puede recuperar el secreto

Menú: “Procedimientos Indiv.” \ “Demostración Secreto Compartido (Shamir)”

Secreto Compartido : Inicializando el esquema umbral

Por definición de un esquema Shamir (t, n) , un secreto puede ser distribuido en n personas. Después de esto, se necesitarán al menos t de esas personas $(t \leq n)$ para reconstruir el secreto original combinando sus secretos. Para configurar el esquema, se debe generar un polinomio $f(x)$ de grado máximo $t-1$ (con $t-1$ coeficientes elegidos aleatoriamente) y un primo aleatorio p . Cada participante recibe un valor público x elegido aleatoriamente y su secreto se corresponde con el valor $y=f(x)$. Para obtener más información puede consultar la ayuda pulsando la tecla F1.

Elija un secreto y determine los parámetros para configurar un esquema

Secreto S con $S \geq 0$

Número de participantes n con $n > 0$

Umbral (mínimo) t con $t > 0$

Parámetros concernientes el polinomio $f(x)$ de grado $t-1$

Todos los cálculos tienen lugar en el espacio discreto $GF(p)$

Polinomio $f(x)$

Primo p

Valor de los participantes, calculado a partir de los parámetros:

Participants	Valor público x	Parte [valor secreto $f(x)$]
<input checked="" type="checkbox"/> participante 1	2996	1069
<input type="checkbox"/> participante 2	89	3665
<input checked="" type="checkbox"/> participante 3	4828	5009
<input type="checkbox"/> participante 4	5437	3696
<input checked="" type="checkbox"/> participante 5	2757	3378
<input type="checkbox"/> participante 6	2751	3808
<input type="checkbox"/> participante 7	3903	4625
<input type="checkbox"/> participante 8	154	5666

Seleccione de entre los participantes aquellos que reconstruirán el secreto.

Mostrar información al inicio.

Ejemplos (13)

Implementación del CRT para resolver sistemas de ecuaciones modulares lineales

Escenario en astronomía

- ¿Cuánto tiempo tiene que pasar hasta que un número dado de planetas (con distintos períodos de rotación) se alineen?
- El resultado es un sistema lineal de ecuaciones modulares, que se puede resolver con el Teorema Chino de los Restos (CRT).
- En esta demostración se pueden introducir hasta 9 ecuaciones y calcular una solución utilizando el CRT.

Ejemplo de uso: Visualización del Teorema Chino de los Restos aplicado en la Astronomía - Movimiento Planetario

Utilizando el Teorema Chino de los Restos (TCR) se pueden resolver sistemas de congruencias. En este ejemplo puedes introducir hasta 9 ecuaciones de la forma: $x = a[i] \bmod m[i]$ ($i=1, \dots, 9$); que serán utilizadas para calcular el tiempo que tardan los planetas en alinearse

Sistema de Congruencias

x ≡	15	mod	88
x ≡		mod	
x ≡	100	mod	365
x ≡		mod	
x ≡	0	mod	4327
x ≡		mod	
x ≡		mod	
x ≡	0	mod	60149
x ≡		mod	

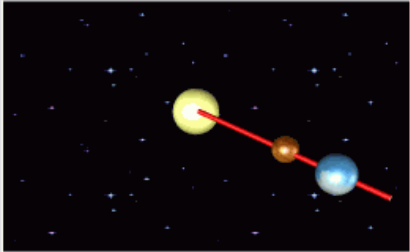
Solución

126.228.390.655

Resolver Salir

Borrar Todos los Parámetros Restaurar los valores por defecto

Ejemplo de uso en Astronomía (visualización)



El periodo de los planetas Mercurio y Tierra alrededor del Sol es de 88 y 365 días. Hasta alcanzar el rayo s (en rojo) quedan:

15 y 100 días.

¿Podría ocurrir que Mercurio y la Tierra volvieran a coincidir sobre el rayo s?

Elige un Planeta

<input checked="" type="checkbox"/> Mercurio	<input type="checkbox"/> Marte	<input type="checkbox"/> Urano
<input type="checkbox"/> Venus	<input checked="" type="checkbox"/> Júpiter	<input checked="" type="checkbox"/> Neptuno
<input checked="" type="checkbox"/> La Tierra	<input type="checkbox"/> Saturno	<input type="checkbox"/> Plutón

Intervalo de tiempo (en días) hasta que se repita el incidente

Menú: "Procedimientos Indiv." \ "Aplicación del Teorema chino de los restos" \ "Astronomía y Movimiento planetario"

Ejemplos (14)

Visualización de métodos de cifrado simétrico utilizando ANIMAL (1)

Visualizaciones animadas de varios algoritmos simétricos

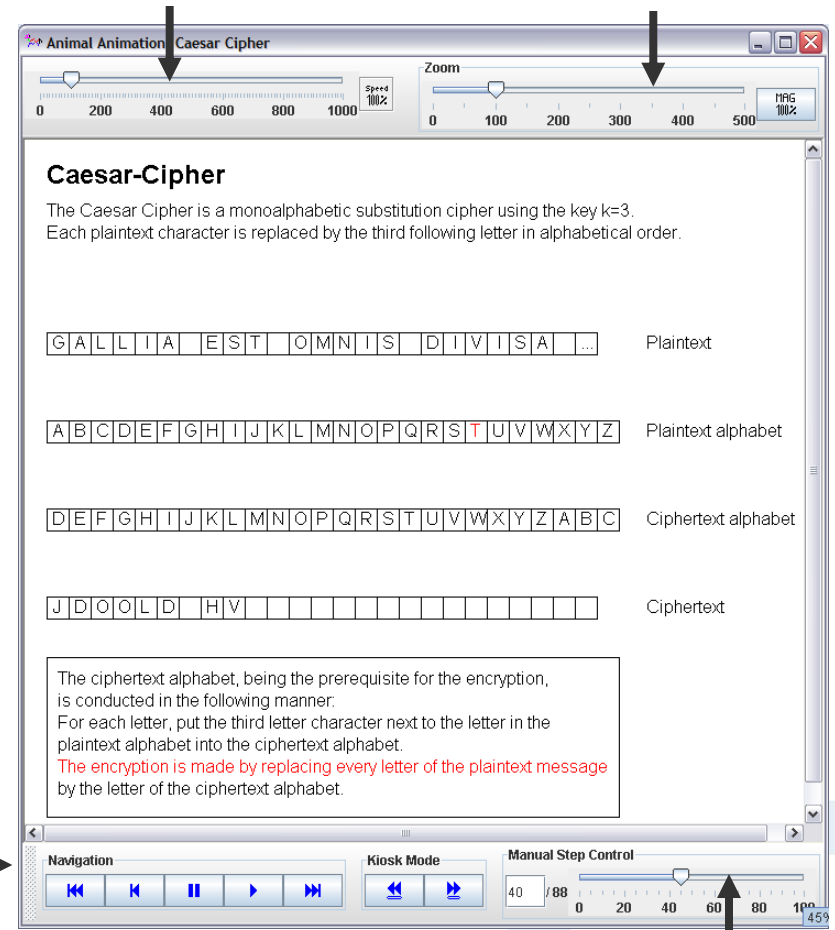
- César
- Vigenère
- Nihilist
- DES

CrypTool

- Menú: “Procedimientos Individ.” \ “Visualización de algoritmos” \ ...
- Control de la animación interactivo utilizando los controles integrados en la ventana.

Controles de la animación (siguiente, atrás, pausa, etc.)

Velocidad de la animación Escala de visionado



Selección directa de un paso de la animación

Ejemplos (14)

Visualización de métodos de cifrado simétrico utilizando ANIMAL (2)

Visualización del cifrado DES

Animal Animation: DES Data Encryption Standard (ECB Mode)

Zoom: 0 100 200 300 400 500

Input Block X (64-bit):

1	0	1	0	0	1	0	0
1	0	1	1	1	0	0	1
0	0	0	1	1	0	0	1
1	0	1	0	0	0	1	0
0	1	0	1	1	0	1	0
1	0	0	1	0	0	1	0
1	1	0	0	0	0	1	0
1	1	1	0	0	0	0	1

Key K (64-bit):

0	1	1	1	1	1	1	1
0	0	1	1	0	0	0	0
1	1	1	1	0	0	0	1
1	1	0	0	0	0	1	1
0	1	1	1	1	0	0	0
0	1	0	0	0	0	0	1
0	1	0	0	0	0	1	1
0	0	1	1	0	0	0	1

PC2:

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Overview:

```

    Input Block X -- IP --> Permuted Input --> 16 DES rounds --> Pre-Output -- IP^-1 --> Output Block Y
    Key K -- PC1 --> PC2(K) --> 16 subkeys
    
```

Round Function Parameters:

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
# of bits to rotate	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	1

Navigation: Kiosk Mode Manual Step Control 165 / 424

Animal Animation: DES Data Encryption Standard (ECB Mode)

Zoom: 0 100 200 300 400 500

Function f :

110110 001010 110110 010100 000100 100110 101001 010011

B[1] B[2] B[3] B[4] B[5] B[6] B[7] B[8]

$10 = 1 \times 2^1 + 0 \times 2^0 = 2$ $1011 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 11$

S-Box 1:

row	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	3

S-Box 8:

row	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Overview:

```

    Input Block X -- IP --> Permuted Input --> 16 DES rounds --> Pre-Output -- IP^-1 --> Output Block Y
    Key K -- PC1 --> PC2(K) --> 16 subkeys
    
```

Navigation: Kiosk Mode Manual Step Control 294 / 424

Después de la permutación del bloque de entrada utilizando el vector de inicialización IV, la clave K se permuta con PC1 y PC2.

La función de núcleo f del DES, que se enlaza la mitad derecha del bloque R_{i-1} con la clave parcial K_i .

Ejemplos (15)

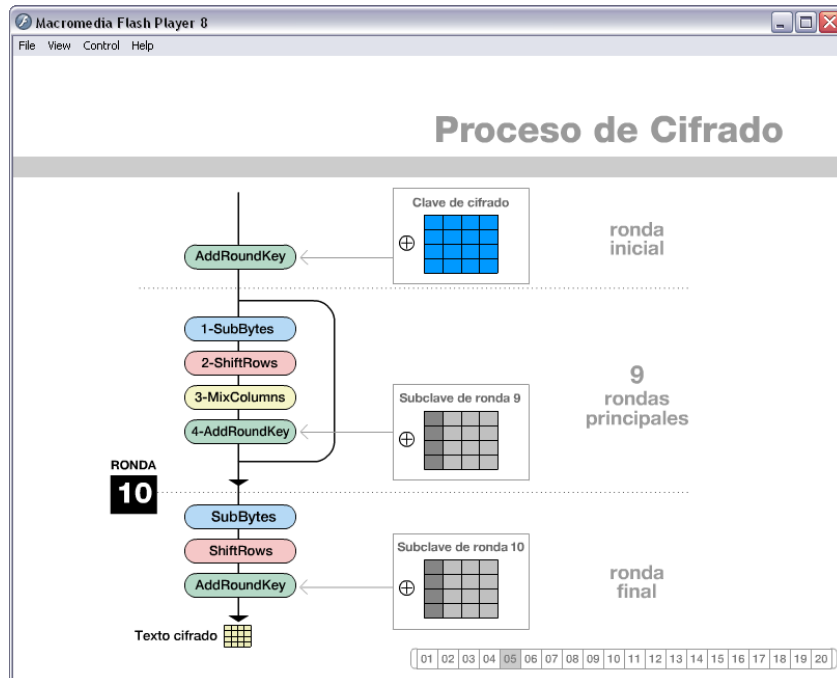
Visualización de AES (cifrado Rijndael)

Animación Rijndael (el cifrado Rijndael fue el ganador de la dependencia del AES)

- La visualización muestra la animación del proceso del cifrado basado en ciclos (utilizando datos fijos)

Inspector Rijndael

- El proceso de cifrado para probar (utilizando tus propios datos)



RijndaelInspector

modo cifrado / modo descifrado

entrada (texto claro)

7e	e9	45	4f
cf	70	5f	aa
58	97	d4	21
c0	90	7e	d9

Clave

3d	6e	e6	d1
14	54	8d	88
23	84	2d	e0
94	93	64	f8

salida

8b	e1	07	1a
65	5d	ce	8b
1b	7f	39	e3
62	7f	f4	b3

comienzo de la ronda / después de SubBytes / después de ShiftRows / después de MixColumns / Subclave de ronda

	comienzo de la ronda	después de SubBytes	después de ShiftRows	después de MixColumns	Subclave de ronda																																																																																
entrada	<table border="1"><tr><td>7e</td><td>e9</td><td>45</td><td>4f</td></tr><tr><td>cf</td><td>70</td><td>5f</td><td>aa</td></tr><tr><td>58</td><td>97</td><td>d4</td><td>21</td></tr><tr><td>c0</td><td>90</td><td>7e</td><td>d9</td></tr></table>	7e	e9	45	4f	cf	70	5f	aa	58	97	d4	21	c0	90	7e	d9	<table border="1"><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table border="1"><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table border="1"><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table border="1"><tr><td>3d</td><td>6e</td><td>e6</td><td>d1</td></tr><tr><td>14</td><td>54</td><td>8d</td><td>88</td></tr><tr><td>23</td><td>84</td><td>2d</td><td>e0</td></tr><tr><td>94</td><td>93</td><td>64</td><td>f8</td></tr></table>	3d	6e	e6	d1	14	54	8d	88	23	84	2d	e0	94	93	64	f8
7e	e9	45	4f																																																																																		
cf	70	5f	aa																																																																																		
58	97	d4	21																																																																																		
c0	90	7e	d9																																																																																		
3d	6e	e6	d1																																																																																		
14	54	8d	88																																																																																		
23	84	2d	e0																																																																																		
94	93	64	f8																																																																																		
ronda 1	<table border="1"><tr><td>43</td><td>87</td><td>a3</td><td>9e</td></tr><tr><td>db</td><td>24</td><td>d2</td><td>22</td></tr><tr><td>7b</td><td>13</td><td>e9</td><td>c1</td></tr><tr><td>54</td><td>03</td><td>1a</td><td>21</td></tr></table>	43	87	a3	9e	db	24	d2	22	7b	13	e9	c1	54	03	1a	21	<table border="1"><tr><td>1a</td><td>17</td><td>0a</td><td>0b</td></tr><tr><td>b9</td><td>36</td><td>b5</td><td>93</td></tr><tr><td>21</td><td>7d</td><td>99</td><td>78</td></tr><tr><td>20</td><td>7b</td><td>a2</td><td>fd</td></tr></table>	1a	17	0a	0b	b9	36	b5	93	21	7d	99	78	20	7b	a2	fd	<table border="1"><tr><td>1a</td><td>17</td><td>0a</td><td>0b</td></tr><tr><td>36</td><td>b5</td><td>93</td><td>b9</td></tr><tr><td>99</td><td>78</td><td>21</td><td>7d</td></tr><tr><td>fd</td><td>20</td><td>7b</td><td>a2</td></tr></table>	1a	17	0a	0b	36	b5	93	b9	99	78	21	7d	fd	20	7b	a2	<table border="1"><tr><td>0a</td><td>b2</td><td>e0</td><td>19</td></tr><tr><td>3b</td><td>ce</td><td>2f</td><td>47</td></tr><tr><td>19</td><td>32</td><td>56</td><td>b5</td></tr><tr><td>60</td><td>b4</td><td>5a</td><td>86</td></tr></table>	0a	b2	e0	19	3b	ce	2f	47	19	32	56	b5	60	b4	5a	86	<table border="1"><tr><td>f8</td><td>96</td><td>70</td><td>a1</td></tr><tr><td>f5</td><td>a1</td><td>2c</td><td>a4</td></tr><tr><td>62</td><td>e6</td><td>cb</td><td>2b</td></tr><tr><td>aa</td><td>39</td><td>5d</td><td>a5</td></tr></table>	f8	96	70	a1	f5	a1	2c	a4	62	e6	cb	2b	aa	39	5d	a5
43	87	a3	9e																																																																																		
db	24	d2	22																																																																																		
7b	13	e9	c1																																																																																		
54	03	1a	21																																																																																		
1a	17	0a	0b																																																																																		
b9	36	b5	93																																																																																		
21	7d	99	78																																																																																		
20	7b	a2	fd																																																																																		
1a	17	0a	0b																																																																																		
36	b5	93	b9																																																																																		
99	78	21	7d																																																																																		
fd	20	7b	a2																																																																																		
0a	b2	e0	19																																																																																		
3b	ce	2f	47																																																																																		
19	32	56	b5																																																																																		
60	b4	5a	86																																																																																		
f8	96	70	a1																																																																																		
f5	a1	2c	a4																																																																																		
62	e6	cb	2b																																																																																		
aa	39	5d	a5																																																																																		
ronda 2	<table border="1"><tr><td>f2</td><td>24</td><td>90</td><td>b8</td></tr><tr><td>ce</td><td>6f</td><td>03</td><td>e3</td></tr><tr><td>7b</td><td>d4</td><td>9d</td><td>9e</td></tr><tr><td>ce</td><td>8d</td><td>07</td><td>23</td></tr></table>	f2	24	90	b8	ce	6f	03	e3	7b	d4	9d	9e	ce	8d	07	23	<table border="1"><tr><td>89</td><td>36</td><td>60</td><td>6c</td></tr><tr><td>8b</td><td>a8</td><td>7b</td><td>11</td></tr><tr><td>21</td><td>48</td><td>5e</td><td>0b</td></tr><tr><td>74</td><td>5d</td><td>c5</td><td>26</td></tr></table>	89	36	60	6c	8b	a8	7b	11	21	48	5e	0b	74	5d	c5	26	<table border="1"><tr><td>89</td><td>36</td><td>60</td><td>6c</td></tr><tr><td>a8</td><td>7b</td><td>11</td><td>8b</td></tr><tr><td>5e</td><td>0b</td><td>21</td><td>48</td></tr><tr><td>26</td><td>74</td><td>5d</td><td>c5</td></tr></table>	89	36	60	6c	a8	7b	11	8b	5e	0b	21	48	26	74	5d	c5	<table border="1"><tr><td>92</td><td>9e</td><td>8f</td><td>d3</td></tr><tr><td>06</td><td>a9</td><td>7c</td><td>7c</td></tr><tr><td>f7</td><td>c7</td><td>d4</td><td>23</td></tr><tr><td>3a</td><td>c2</td><td>2a</td><td>e6</td></tr></table>	92	9e	8f	d3	06	a9	7c	7c	f7	c7	d4	23	3a	c2	2a	e6	<table border="1"><tr><td>b3</td><td>25</td><td>55</td><td>f4</td></tr><tr><td>04</td><td>a5</td><td>89</td><td>2d</td></tr><tr><td>64</td><td>82</td><td>49</td><td>62</td></tr><tr><td>98</td><td>a1</td><td>fc</td><td>59</td></tr></table>	b3	25	55	f4	04	a5	89	2d	64	82	49	62	98	a1	fc	59
f2	24	90	b8																																																																																		
ce	6f	03	e3																																																																																		
7b	d4	9d	9e																																																																																		
ce	8d	07	23																																																																																		
89	36	60	6c																																																																																		
8b	a8	7b	11																																																																																		
21	48	5e	0b																																																																																		
74	5d	c5	26																																																																																		
89	36	60	6c																																																																																		
a8	7b	11	8b																																																																																		
5e	0b	21	48																																																																																		
26	74	5d	c5																																																																																		
92	9e	8f	d3																																																																																		
06	a9	7c	7c																																																																																		
f7	c7	d4	23																																																																																		
3a	c2	2a	e6																																																																																		
b3	25	55	f4																																																																																		
04	a5	89	2d																																																																																		
64	82	49	62																																																																																		
98	a1	fc	59																																																																																		
ronda 3	<table border="1"><tr><td>21</td><td>bb</td><td>de</td><td>27</td></tr><tr><td>02</td><td>0c</td><td>f5</td><td>51</td></tr><tr><td>93</td><td>45</td><td>9d</td><td>41</td></tr><tr><td>a2</td><td>63</td><td>d6</td><td>bf</td></tr></table>	21	bb	de	27	02	0c	f5	51	93	45	9d	41	a2	63	d6	bf	<table border="1"><tr><td>fd</td><td>ee</td><td>57</td><td>cc</td></tr><tr><td>77</td><td>fe</td><td>e6</td><td>d1</td></tr><tr><td>dc</td><td>6e</td><td>5e</td><td>83</td></tr><tr><td>3a</td><td>fb</td><td>f6</td><td>08</td></tr></table>	fd	ee	57	cc	77	fe	e6	d1	dc	6e	5e	83	3a	fb	f6	08	<table border="1"><tr><td>fd</td><td>ee</td><td>57</td><td>cc</td></tr><tr><td>fe</td><td>e6</td><td>d1</td><td>77</td></tr><tr><td>5e</td><td>83</td><td>dc</td><td>6e</td></tr><tr><td>08</td><td>3a</td><td>fb</td><td>f6</td></tr></table>	fd	ee	57	cc	fe	e6	d1	77	5e	83	dc	6e	08	3a	fb	f6	<table border="1"><tr><td>ae</td><td>47</td><td>e1</td><td>82</td></tr><tr><td>f0</td><td>99</td><td>6a</td><td>66</td></tr><tr><td>a7</td><td>5f</td><td>33</td><td>66</td></tr><tr><td>ec</td><td>34</td><td>19</td><td>a1</td></tr></table>	ae	47	e1	82	f0	99	6a	66	a7	5f	33	66	ec	34	19	a1	<table border="1"><tr><td>6f</td><td>4e</td><td>1f</td><td>eb</td></tr><tr><td>aa</td><td>0b</td><td>82</td><td>ef</td></tr><tr><td>a2</td><td>2d</td><td>64</td><td>06</td></tr><tr><td>27</td><td>86</td><td>7a</td><td>23</td></tr></table>	6f	4e	1f	eb	aa	0b	82	ef	a2	2d	64	06	27	86	7a	23
21	bb	de	27																																																																																		
02	0c	f5	51																																																																																		
93	45	9d	41																																																																																		
a2	63	d6	bf																																																																																		
fd	ee	57	cc																																																																																		
77	fe	e6	d1																																																																																		
dc	6e	5e	83																																																																																		
3a	fb	f6	08																																																																																		
fd	ee	57	cc																																																																																		
fe	e6	d1	77																																																																																		
5e	83	dc	6e																																																																																		
08	3a	fb	f6																																																																																		
ae	47	e1	82																																																																																		
f0	99	6a	66																																																																																		
a7	5f	33	66																																																																																		
ec	34	19	a1																																																																																		
6f	4e	1f	eb																																																																																		
aa	0b	82	ef																																																																																		
a2	2d	64	06																																																																																		
27	86	7a	23																																																																																		

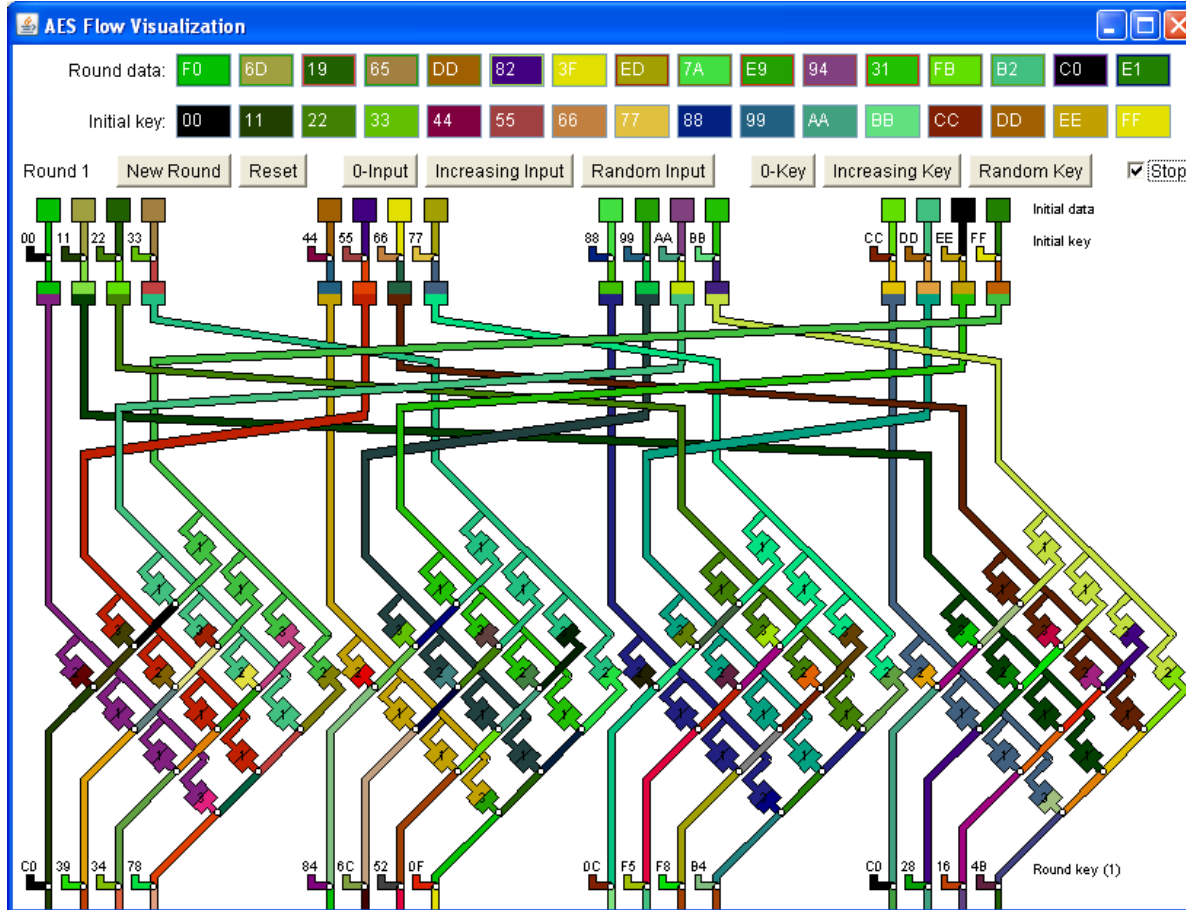
Menú: "Procedimientos Indiv." \ "Visualización de Algoritmos" \ "AES" \ "Animación Rijndael" o "Inspector Rijndael"

Ejemplos (15)

Visualización de AES (cifrado Rijndael) – usando Java

Visualización de flujo de Rijndael

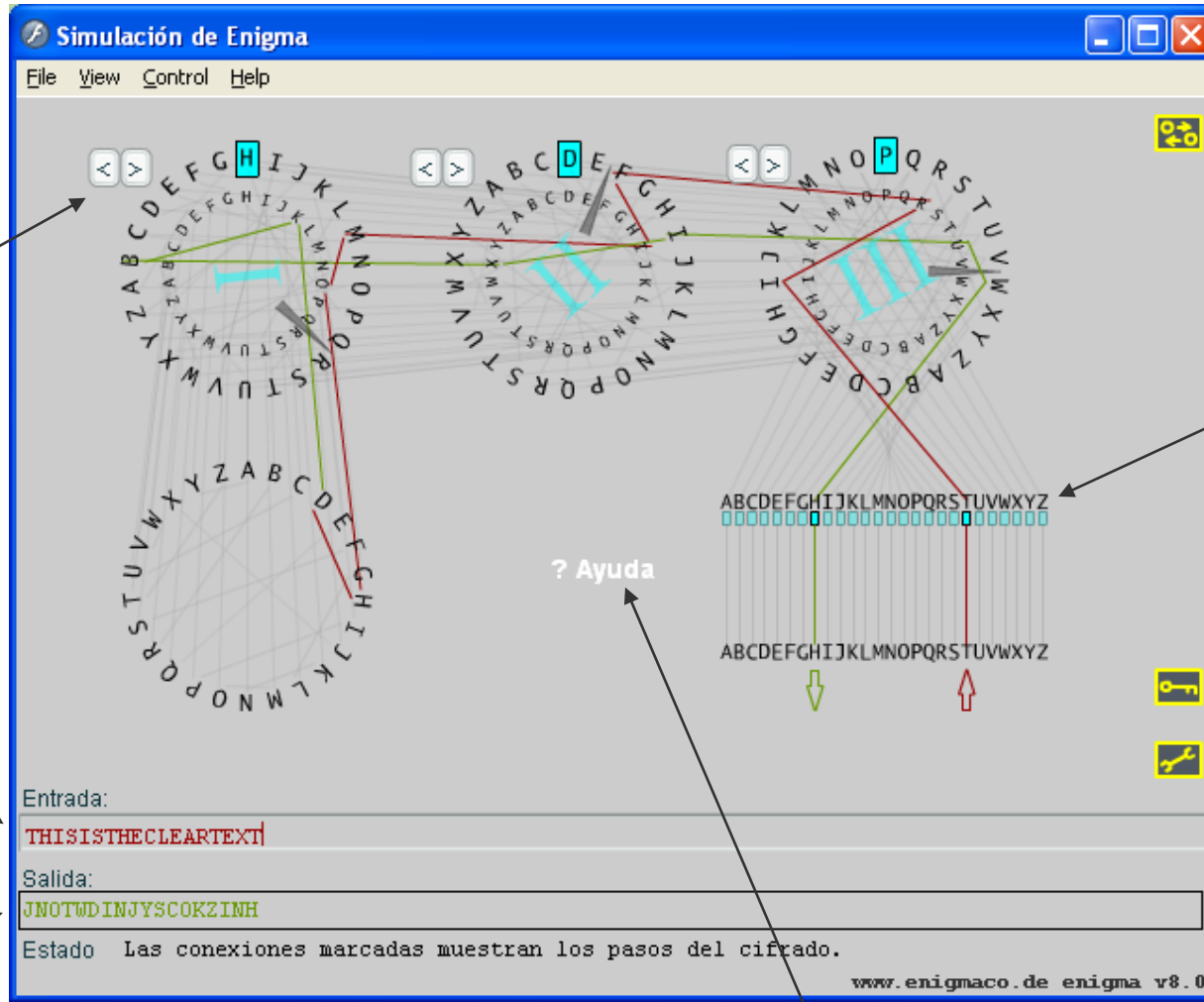
- Visualización de cambios por ronda a través de escala de colores.



Menú: “Procedimientos Indiv.” \ “Visualización de Algoritmos” \ “AES” \ “Animación Rijndael ...”

Ejemplos (16)

Visualización del cifrado de Enigma



Cambiar configuración del rotor

Entrada del texto claro

Salida del texto cifrado

Seleccionar rotores

Cambiar conectores

Mostrar configuración

Reiniciar Enigma al estado inicial o a un estado aleatorio

? Ayuda

Ayuda en línea adicional HTML

Ejemplos (17)

Visualización de E-Mail seguro usando S/MIME

Visualización S/MIME

- Centro de Control: Firmar/Cifrar mensajes con diferentes parámetros
- Animación: Desde la creación en el emisor hasta la lectura en el receptor

The image shows two overlapping windows from the S/MIME Visualization Control Center v1.0 application.

S/MIME Visualization Control Center v1.0

In this window you can dynamically configure parameters for secure email messaging.

The visualisation is then done in two steps (control center & flash animation):

- At the control center you choose whether to encrypt or sign an email and the appropriate parameters.
- After clicking the start button the chosen procedure is visualized with a flash animation.

You can open more than one flash animation at once with different parameters from the control center.

Signing or encrypting

Signing
 Encrypting

Text of the message

Receiver: bob@web.com
Sender: alice@wonderland.com
Subject: Message will be signed

Donec consequat, ipsum non volutpat placerat, ...

Note: In this demonstration the text field can only handle 50 characters, longer texts will be shortened.

Load message text from file

Start signing

Choose sender's PSE

Internal PSE
 Personal PSE Load existing PSE

Control parameters

Signature algorithm: RSA
Hash function: SHA-1
transfer encoding: quoted-printable
MIME type: multipart/signed

S/MIME Animation

File View Control Help

The animation window shows a cartoon character (Alice) standing next to a computer monitor displaying an Outlook interface. Below the monitor is a navigation bar with buttons: Prologue, Compose E-Mail, Canonicalize, Transfer Encoding, Forwarding, Signing, Transport.

To ensure authenticity she makes use of the e-mail client's S/MIME features. One of these features enables her to attach a digital signature. Alice normally doesn't see her signature when she has composed the message, so let's take a look behind the scenes.

<< Prev. Chapter < Prev. Step Next Step > Next Chapter >> Close

Menú: "Procedimientos Indiv." \ "Protocolos" \ "Seguridad E-Mail con S/MIME..."

Ejemplos (18)

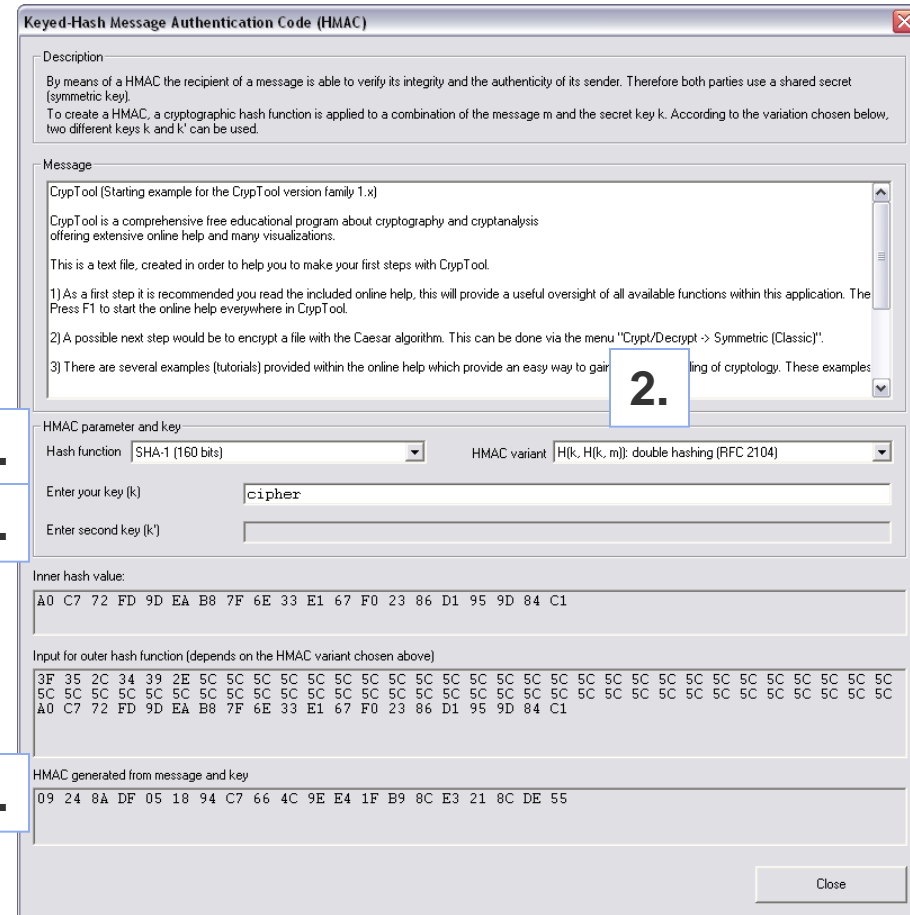
Generación de un código de autenticación de un mensaje (HMAC)

Código de Autenticación de Mensaje (HMAC)

- Asegura:
 - La integridad de un mensaje
 - La autenticación del mensaje
- Bases: una clave común
- Alternativa: Firma Digital

Generación de un MAC en CrypTool

1. Elija una función hash
2. Seleccione una variante de MAC
3. Introduzca una clave (dependiendo de la variante del MAC pueden ser dos claves)
4. Generación del MAC (automático)



Menú: "Procedimientos Individ." \ "Hash" \ "Generación de MACs"

Ejemplos (19)

Demostración Hash

Sensibilidad de las funciones hash a las modificaciones del texto claro

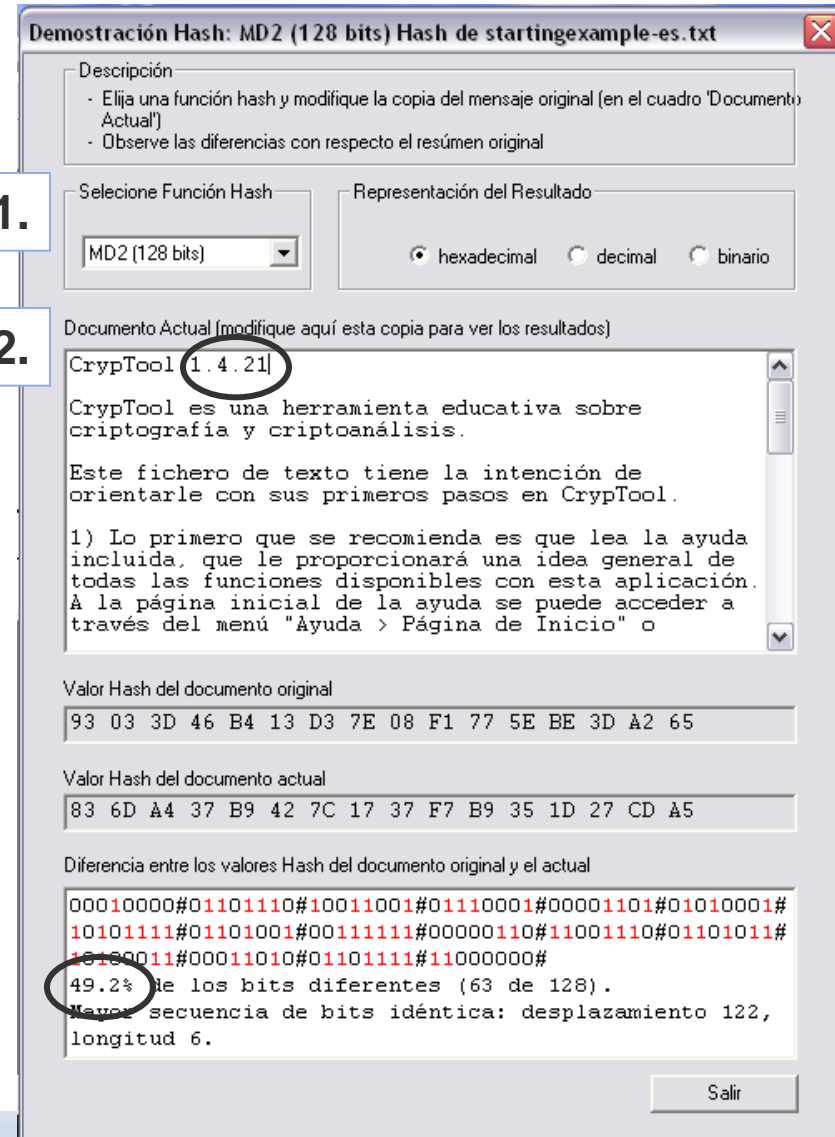
1. Seleccione una función hash
2. Modificar los caracteres del texto claro

Ejemplo:

Introduciendo un espacio después de “CrypTool” en el texto de ejemplo implica un cambio en 49,2% de los bits del valor hash generado.

Una buena función hash debe reaccionar sensiblemente frente a los más pequeños cambios en el texto claro – “efecto avalancha” (cambio pequeño, gran impacto).

Menú: “Procedimientos Individ.” / “Hash” / “Demostración Hash”



Ejemplos (20)

Herramienta para el aprendizaje de teoría de números

- **Teoría de Números** soportada por elementos gráficos y herramientas para probar
- **Temas:**
 1. Enteros
 2. Clases de Restos
 3. Generación de primos
 4. Criptografía de clave Pública
 5. Factorización
 6. Logaritmo Discreto

3.2 Fermat Test page 4 of 11

Each prime p passes a test that results from Fermat's [Little Theorem](#):
Try for a $b \in \{2, \dots, p-1\}$, if $b^{p-1} \equiv 1 \pmod{p}$.

This test is called **Fermat Test**. Unfortunately some composite numbers pass it as well.

Example: $341 = 11 \cdot 31$, even so is $2^{340} \equiv 1 \pmod{341}$.

A passed test gives no information, one repeats it with a different base b :

$n =$ $2^{n-1} \equiv 1 \pmod{n}$ Test passed
GCD(b, n) = 1 b

Definition: Let n be a composite number, b coprime to n .
If $b^{n-1} \equiv 1 \pmod{n}$, then one calls

- n **Pseudo Prime to Base b** ,
- b **Liar for** (the primality of) n ,

otherwise one calls b **Witness against** (the primality of) n .

Theorem: If there are any witnesses against n ,
then they make up at least 50% of all $b \in \{1, \dots, n\}$ coprime to n . [Proof](#)

(Go on to the next page.)

Menú: „Procedimientos Indiv.” \ „Teoría de Números - Interactiva“ \ „Herramienta para el aprendizaje sobre teoría de números”

Ejemplos (21)

Suma de puntos en curvas elípticas

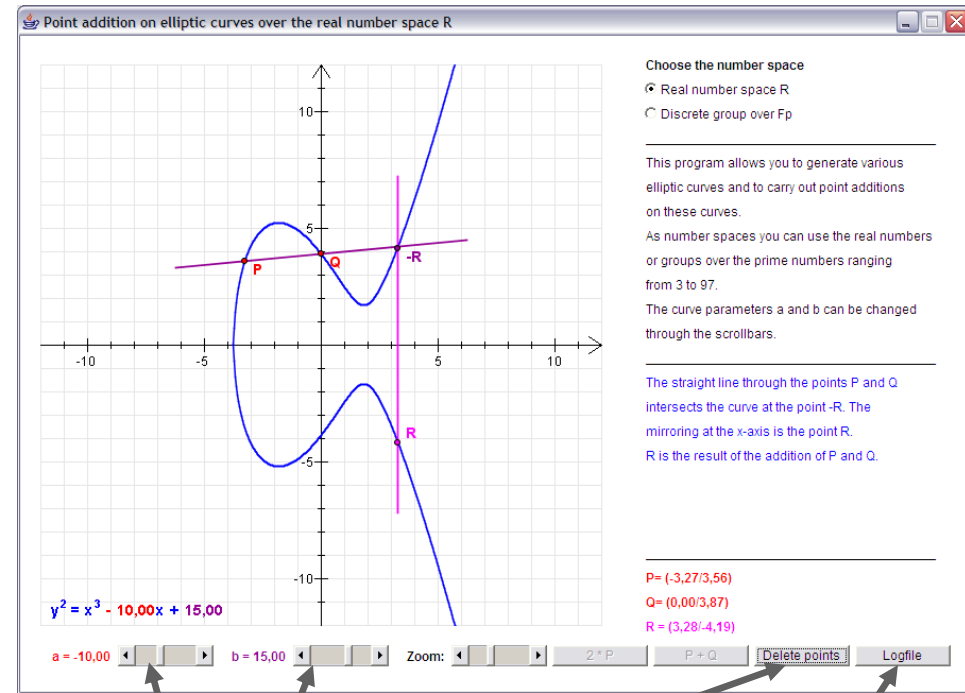
- Visualización de suma de puntos en curvas elípticas
- Bases para la criptografía basada en curvas Elípticas (ECC)

Ejemplo 1

- Marcar un punto P en la curva
- Marcar un punto Q en la curva
- Presionar el botón “P+Q”:
 - La línea recta que une los puntos P y Q e interseca a la curva en el punto -R
 - Reflejando en el eje de las X el resultado está en el punto R

Ejemplo 2

- Marcar el punto P en la curva
- Presionar el botón “2*P”:
 - La tangente al punto P que interseca a la curva en el punto -R
 - Reflejando en el eje X el resultado está en el punto R



Cambiar parámetros de la curva

Eliminar puntos

Cargar archivo de cálculos

Menú: “Procedimientos Indiv.” \ “Teoría de Números – Interactiva” \ “Suma de Puntos en Curvas Elípticas”

Ejemplos (22)

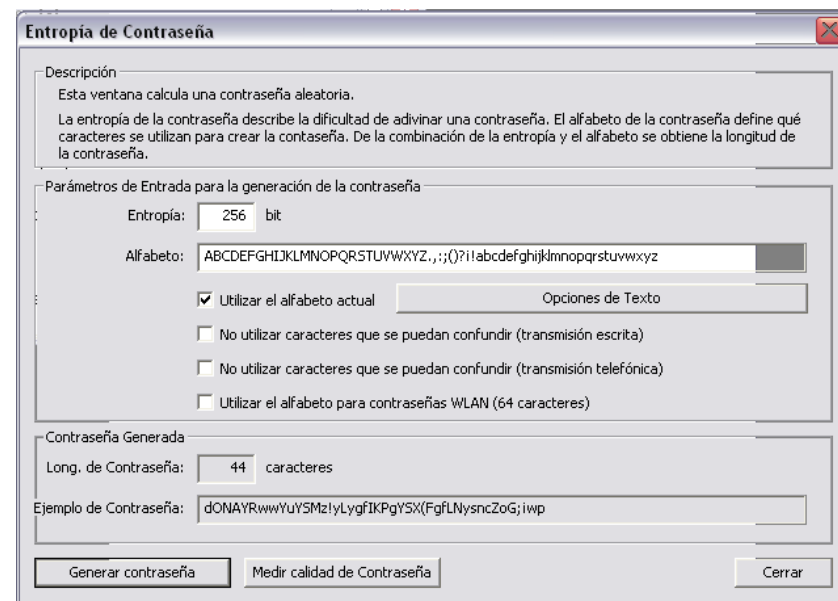
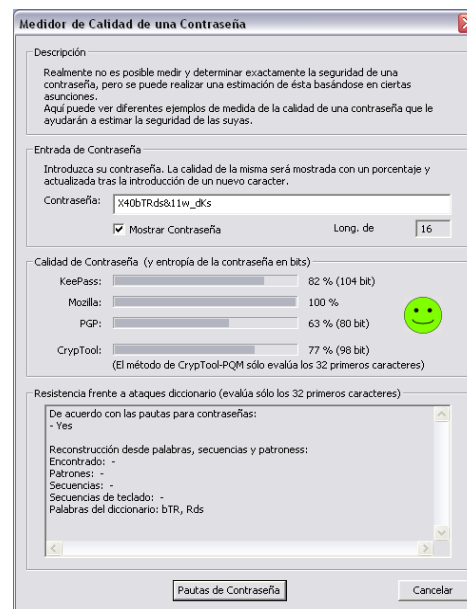
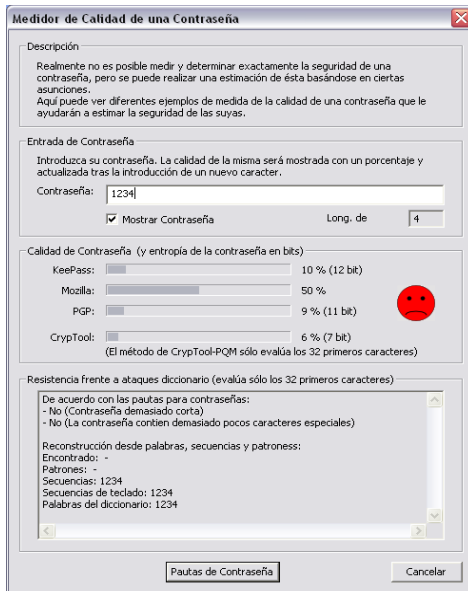
Medidor de Calidad de Contraseñas (Password Quality Meter “PQM”) 1

Funciones

- Medida de la calidad de contraseñas
- Comparar con PQMs en otras aplicaciones: KeePass, Mozilla y PGP
- Medida experimental con el algoritmo de CrypTool
- Ejemplo: Entrada de una contraseña (mientras se muestra la contraseña)

Password: **1234**

Password: **X40bTRds&11w_dks**



Menú: “Procedimientos Indiv.” \ “Herramientas” \ “Medidor de Calidad de Contraseñas” Menú: “Procedimientos Indiv.” \ “Herramientas” \ “Entropía de Contraseña”

Ejemplos (22)

Medidor de Calidad de Contraseñas (Password Quality Meter “PQM”) 2

Conclusiones del Medidor de Calidad de Contraseñas

- La calidad de la contraseña depende principalmente de la **longitud de la contraseña**.
- Se puede alcanzar una mayor calidad en la contraseña utilizando **distintos tipos de caracteres**: mayúsculas/minúsculas, números y caracteres especiales (**espacio de contraseña**)
- **Entropía de Contraseña** como indicador de la aleatoriedad de los caracteres de la contraseña o del espacio de contraseña (una mayor entropía aparece en una calidad de contraseña mejorada)
- Las contraseñas **NO deben existir en un diccionario** (nota: una comprobación con diccionario aún no se ha implementado en CrypTool).

Calidad de una contraseña desde la perspectiva de un atacante

- Ataque a una contraseña (con número de intentos ilimitado):
 1. **Ataque diccionario** clásico
 2. Ataque diccionario **con variantes** (p.ej. Combinaciones con números de 4 cifras: Verano2007)
 3. **Ataque por fuerza bruta** probando todas las combinaciones posibles (con parámetros adicionales como limitaciones en los tipos de conjuntos de caracteres)
- ⇒ Una buena contraseña se debe elegir para que los ataques 1. y 2. no la comprometan. Con respecto a los ataques de fuerza bruta, son importantes la longitud de la contraseña (al menos 8 caracteres) así como los conjuntos de caracteres utilizados.

Ejemplos (23)

Análisis por Fuerza Bruta 1

Análisis por fuerza bruta

Análisis por fuerza bruta optimizado bajo la suposición de que la clave se conoce parcialmente.

Ejemplo – Análisis con DES (ECB)

Intento de encontrar el resto de la clave para descifrar el texto cifrado (Suposición: el texto claro es un bloque de 8 caracteres ASCII)

Clave (Hex)

68ac78dd40bbefd*
0123456789ab****
98765432106*****
0000000000*****
000000000000****
abacadaba*****
dddddddddd*****

Texto Cifrado (Hex)

66b9354452d29eb5
1f0dd05d8ed51583
bcf9ebd1979ead6a
8cf42d40e004a1d4
0ed33fed7f46c585
d6d8641bc4fb2478
a2e66d852e175f5c

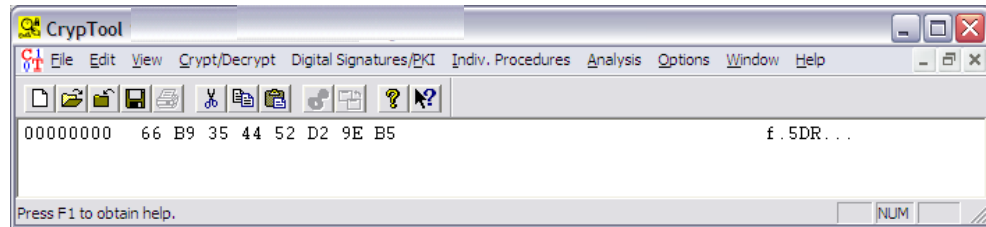


Ejemplos (23)

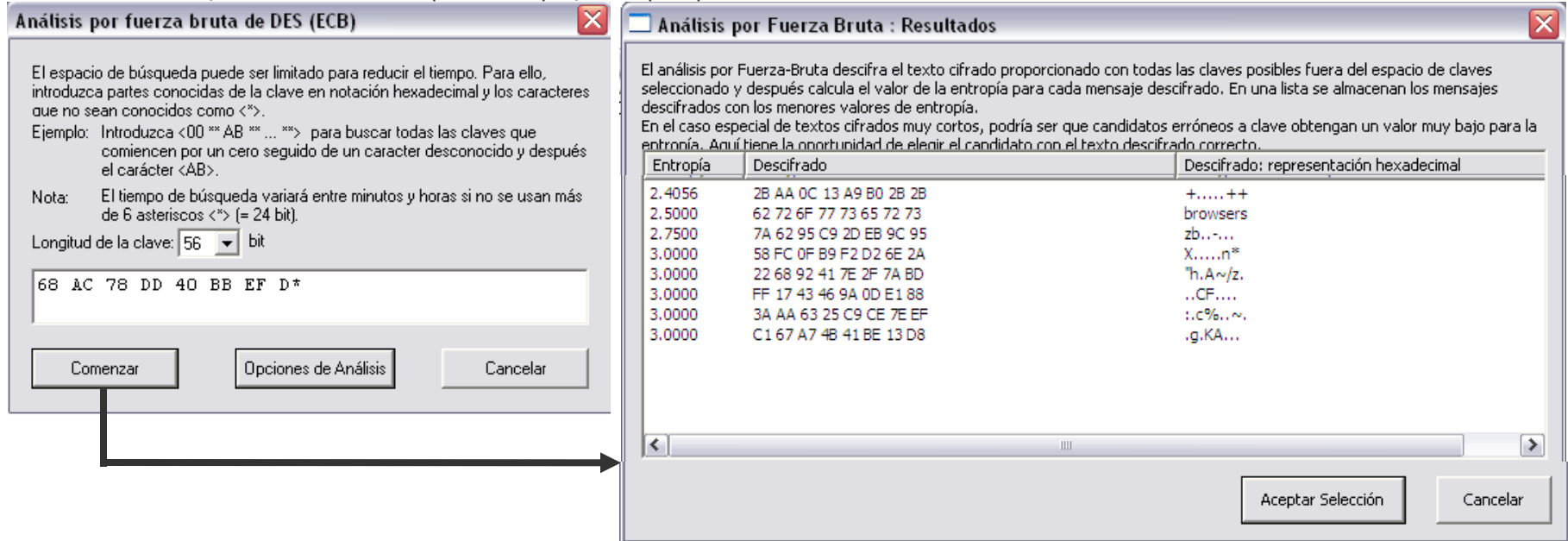
Análisis por Fuerza Bruta 2

1. Entrada de texto cifrado
2. Utilizar análisis por fuerza bruta
3. Introducir parte de la clave conocida
4. Empezar análisis por fuerza bruta
5. Análisis de los resultados: una baja entropía evidencia un posible descifrado. Sin embargo, a causa del texto claro corto utilizado en este ejemplo, el resultado correcto no es el que tiene la entropía más baja.

Utiliza "Ver" \ "Mostrar como código hexadecimal"



Menú: "Análisis" \ "Cifrado Simétrico (moderno)" \ "DES (ECB)"



Ejemplos (24)

Escítala / Rail Fence

Escítala y Rail Fence

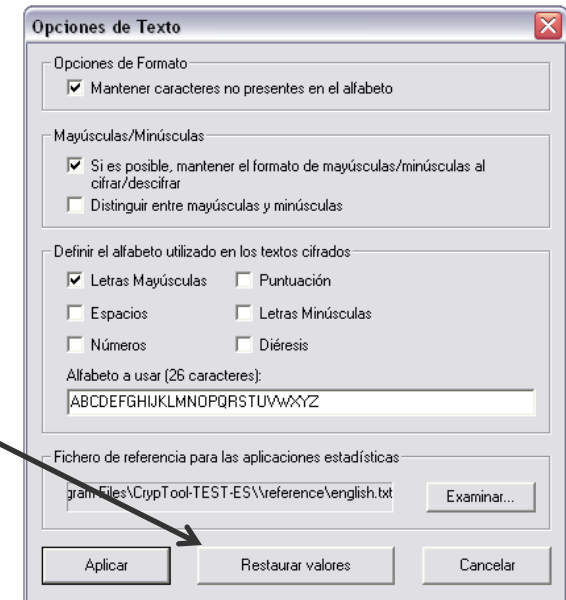
- Transposiciones mezclan el orden de las letras en el texto claro
- **Parámetro de Transposición**
 - Número de esquinas (Escítala)
 - Número de líneas (Rail Fence)
 - Offset



Menú: “Cifrado/Descifrado” \ “Simétrico (clásico)” \ “Escítala/Rail Fence ...”

Opciones de Texto

- Opciones generales de texto (Menú: “Opciones” \ “Opciones de Texto...”)
- Opciones de formato para texto claro y cifrado
- Distinción entre mayúsculas y minúsculas
- Alfabeto para el procesamiento de texto (muestra los caracteres que deben ser cifrados/descifrados)
- Vuelva a establecer los valores por defecto a través del botón “Restaurar valores”
- Cree los patrones de referencia estática en forma dinámica.



Ejemplos (25)

Cifrado Hill / Análisis Hill (1)

Cifrado Hill

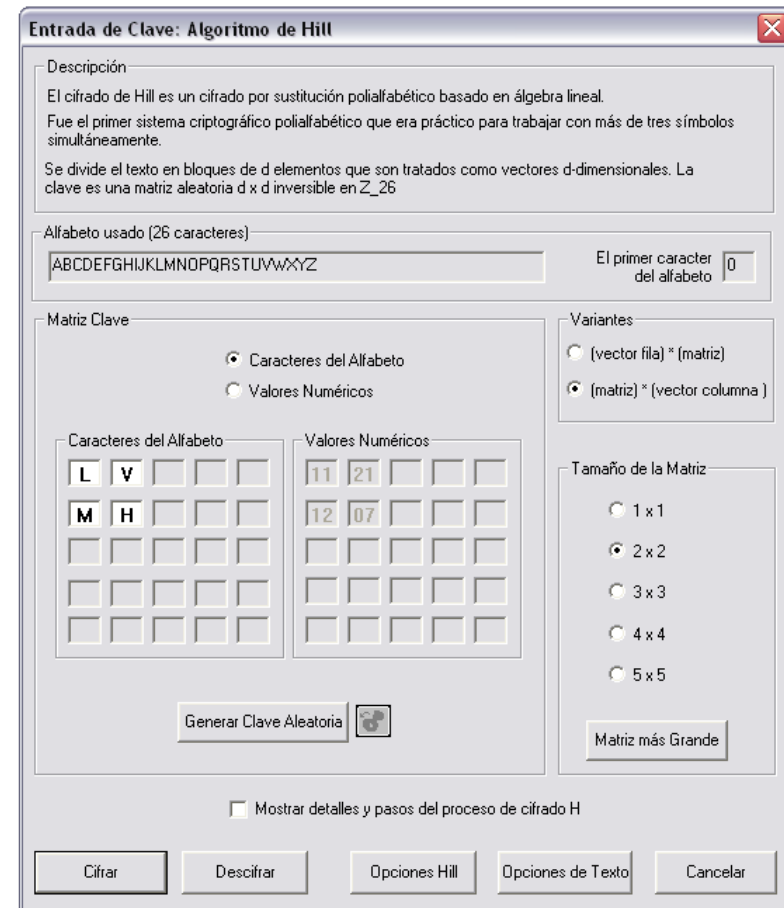
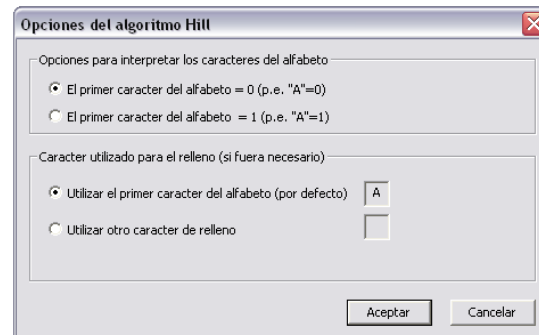
- Cifrado de sustitución poligráfico
- Basado en álgebra lineal

Clave

- Caracteres de alfabeto (Ver opciones de texto) o valores numéricos
- Ingresar clave o generar una aleatoria
- Seleccionar parámetro de multiplicación
- Tamaño de la matriz
- Opciones

Menú:

“Cifrar/Descifrar” \
“Simétrico (clásico)” \
“Hill ...”



Ejemplos (25)

Cifrado Hill / Análisis Hill (2)

Cifrado Hill

- Texto de ejemplo con la clave: LVMH

Análisis Hill (texto claro conocido)

1. Texto claro / texto cifrado - Largo

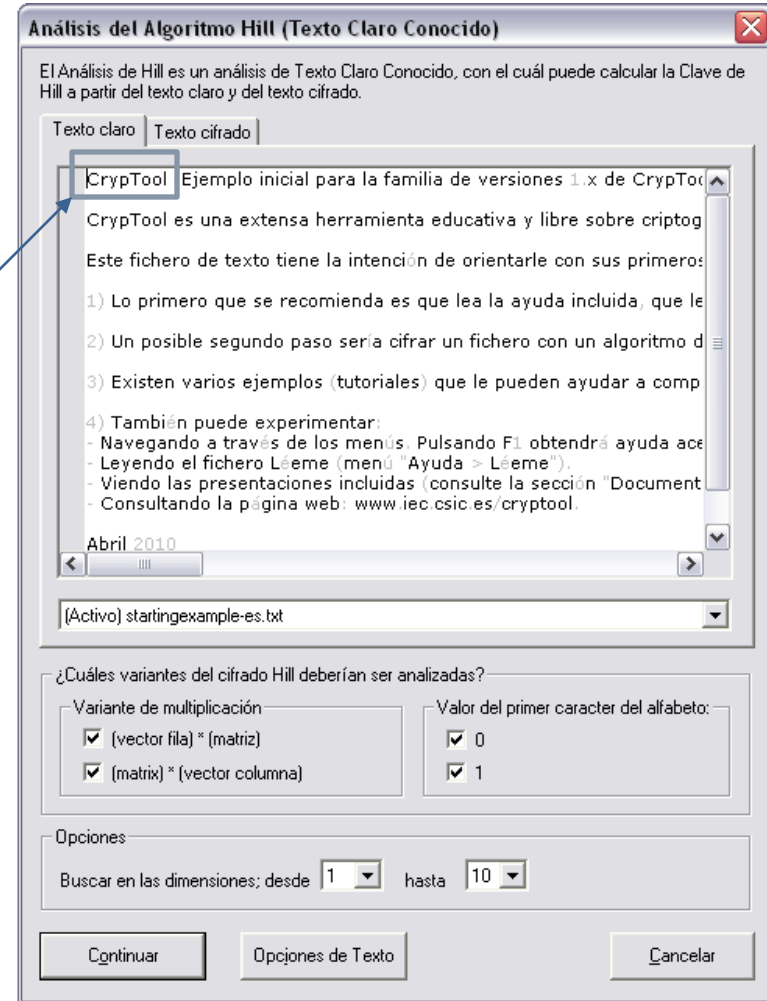
- Seleccionar texto plano (startingexample-es.txt)
- Seleccionar texto cifrado
(Cifrado Hill de <startingexample-es.txt>)
- “Continuar” para buscar la clave

2. Texto claro / texto cifrado - Reducido

- Eliminar todo, excepto el inicio del texto claro (“CrypTool”)
- Reducir texto cifrado a “PnhdJovl”
- “Continuar” encuentra la clave correcta

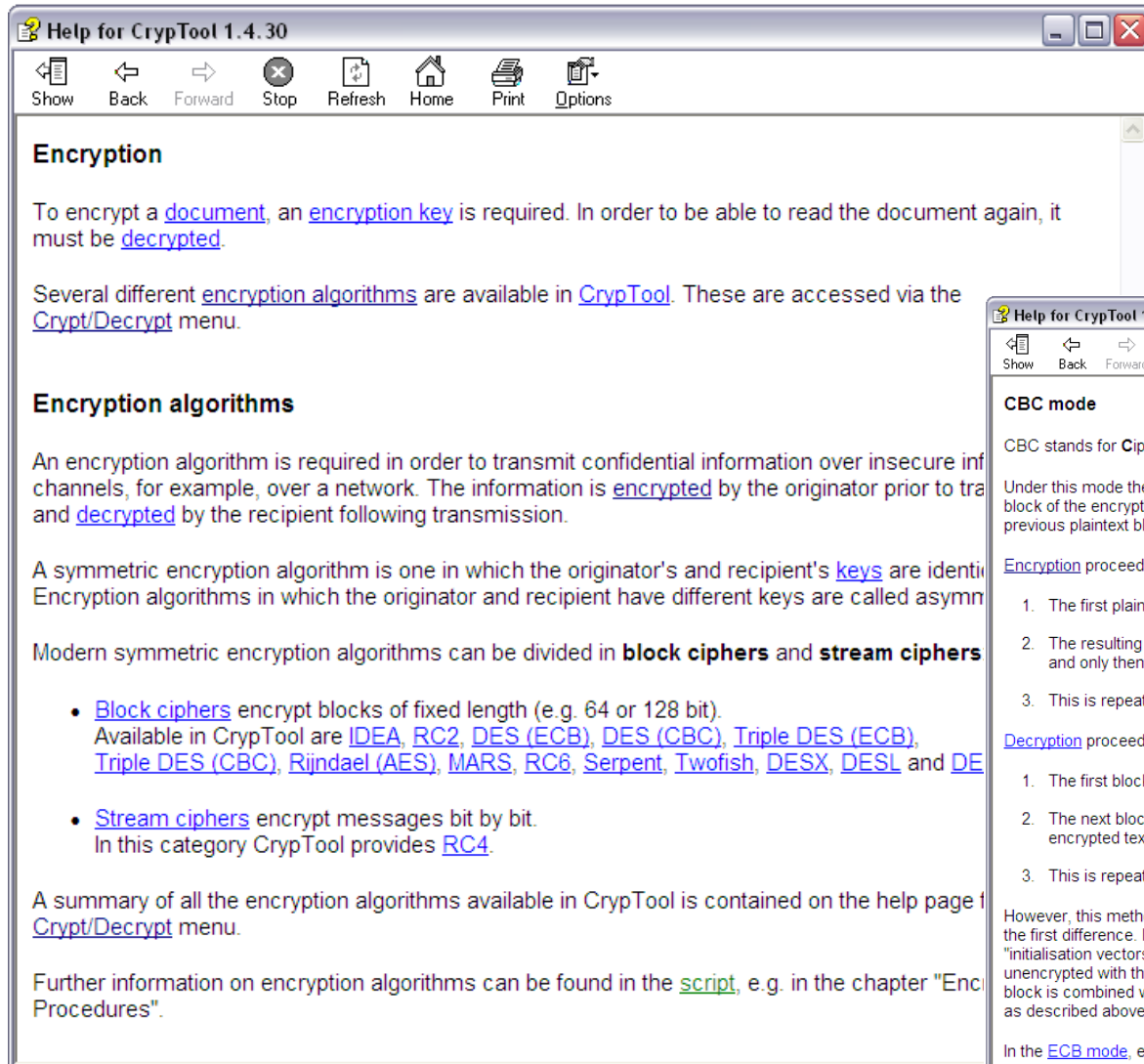
¿Qué cantidad de texto claro/cifrado es necesario para encontrar la clave de cifrado correcta?

Menú: “Análisis” \ “Simétrico (clásico)” \ “Texto claro conocido” \ “Hill...”

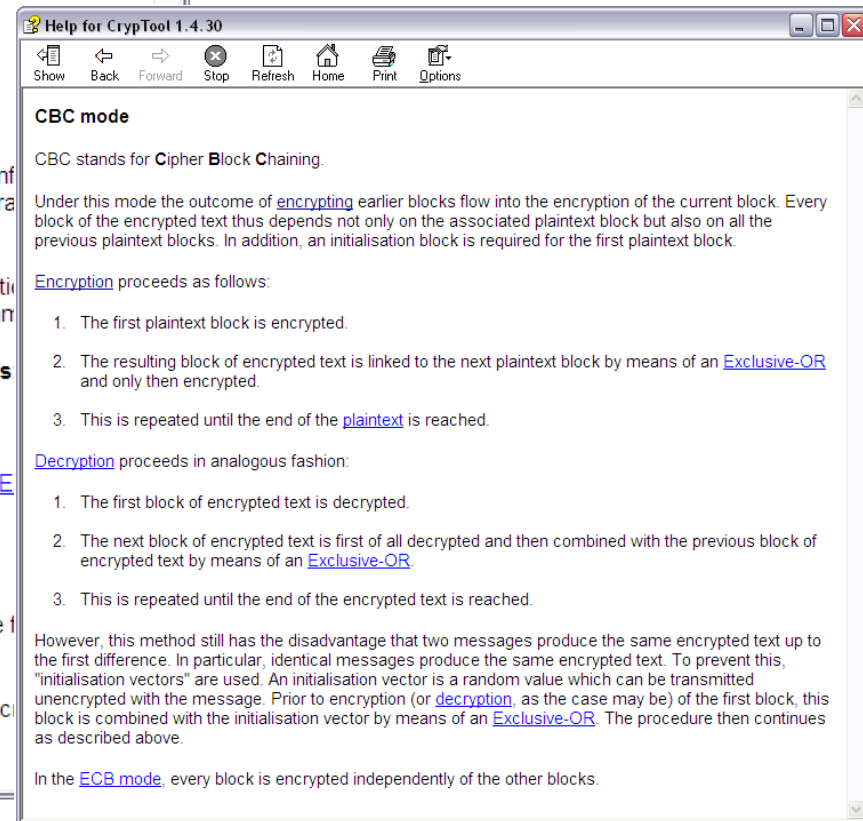


Ejemplos (26)

Ayuda Online de CrypTool (1)



Menú: "Ayuda" \ "Página de Inicio"



Ejemplos (26)

Ayuda Online de CrypTool (2)

Help for CrypTool 1.4.30

Hide Back Forward Stop Refresh Home Print Options

Contents Index Search

Type in the keyword to find:

lattice reduction

- Lattice reduction
- Liability (exclusion)
- License terms
- Line wrap
- Links
- Literature
- MARS encryption algorithm
- MD2 hash value
- MD4 hash value
- MD5 hash value
- Menu (overview of all menus)
- Mirac1
- Modular transformation
- Modulo operator
- Monalphabetic substitution encryp
- Network authentication
- N-gram
- Nihilist encryption algorithm
- NIST
- Normal distribution
- NSA
- NTL
- Number Shark
- Number system
- Number theory
- Offset
- One-time pad
- OpenGL
- OpenPGP
- OpenSSL
- Options
- Overview / Subsumption / Broader C
- Padding
- Parent window
- Password
- Pattern search

Display

Menu Lattice Based Attacks on RSA (Menu [Individual Procedures](#) \ RSA Cryptosystem)

The menu **Lattice Based Attacks on RSA** contains the following commands:

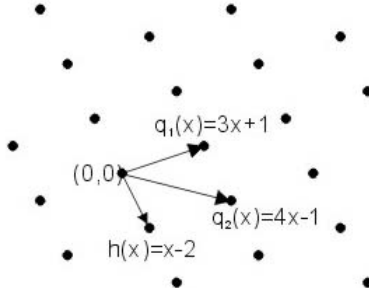
Factoring with a Hint	Attacks RSA with lattice reduction algorithms, if a part of one of the primes of N is known.
Attack on Stereotyped Messages	Attacks RSA with lattice reduction algorithms, if a part of the original cleartext of an intercepted ciphertext is known and if e is small.
Attack on Small Secret Keys	Attacks RSA with lattice reduction algorithms, if d is too small compared to N.

All attacks presented here are based on a common approach: first the task of breaking RSA is transformed into finding the root of a polynomial modulo an integer (mostly N) but to find such a root is a difficult problem.

To solve this problem further polynomials are generated which are known to have the same root. From the coefficients of these polynomials a latticebase is built. This is then reduced with, i.e. the LLL-algorithm to find a small vector.

From this newly found short vector a new polynomial is built. It can be proven that if the vector is short enough, the polynomial has the desired root not only modulo N, but also over the integers.

Example:



The polynomial $q_1(x) = 3x+1$ has a root x_0 modulo 7. It is supposed, that the polynomial $q_2(x) = 4x-1$ has the same root x_0 modulo 7. From these polynomials the vectors $b_1=[3 \ 1]$ and $b_2=[4 \ -1]$ are built. All integer linear combinations of these vectors form points in a lattice. The Figure on the left shows a part of this lattice. Each point of the lattice now can again be interpreted as a polynomial having the desired root. A short vector of the lattice is $b_3=[1 \ -2]$ from which the polynomial $h(x) = x-2$ is built. this polynomial has a root in $x_0=2$ over the integers as well als modulo 7. That $x_0=2$ is also a root of the polynomials $q_1(x)$ and $q_2(x)$ modulo 7 can be easily established.

$$(3x_0+1=7 \text{ modulo } 7 = 0)$$

Ejemplos (26)

Ayuda Online de CrypTool (3)

Help for CrypTool 1.4.30

Hide Back Forward Stop Refresh Home Print Options

Contents Index Search

Type in the keyword to find:

base

- Base64 coding
- BC
- Binary exclusive-OR
- Birthday attack / birthday paradox
- Bit length
- Block cipher
- Blocks
- Books
- Bounding box
- Brute-force attack
- Byte addition
- Caesar encryption algorithm
- Card game
- Cascade
- Cascading cipher
- CBC mode
- Certificate
- Challenge
- Challenge-response demonstration
- Chi² distribution
- Chinese remainder theorem
- Chosen-plaintext attack
- Ciphertext
- Ciphertext-only attack
- Clipboard
- Codings
- Coin toss
- Column transposition
- Compress
- Congruence generator
- Contact
- Context / Substitution / Overlap
- Copyright
- Correlation
- Cryptanalysis
- Crypto competitions / Cryptography

Display

Comparison of Base64 and UU coding

The encoding procedures of [Base64](#) and [UUencode](#) are quite similar, which is shown by the following figure:

Step 1: Splitting the data stream -- same procedure in both encodings.

Step 2: Representation of the 6 bit values -- different procedures.

Base64 **UUencode**

Dividing of 3 x 8 bit to 4 x 6 bit.

Byte 1			Byte 2			Byte 3																	
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓																							
Character 1						Character 2						Character 3						Character 4					

Get the characters from Base64 coding table. (defined in an IETF standard)

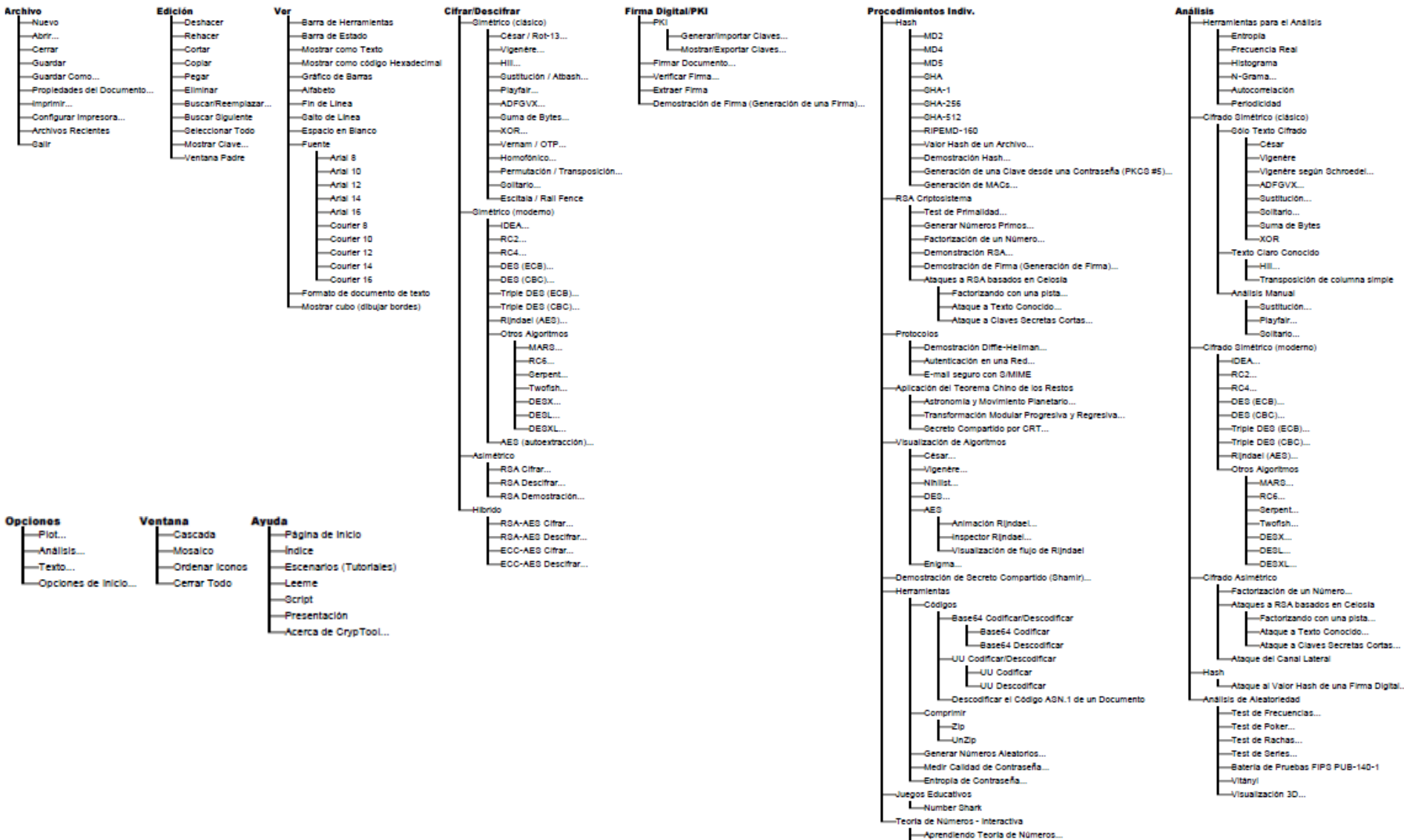
Get the characters, increased by decimal 32, from the ASCII char set.

Because of the similar encoding procedure, there are also shared advantages and drawbacks:

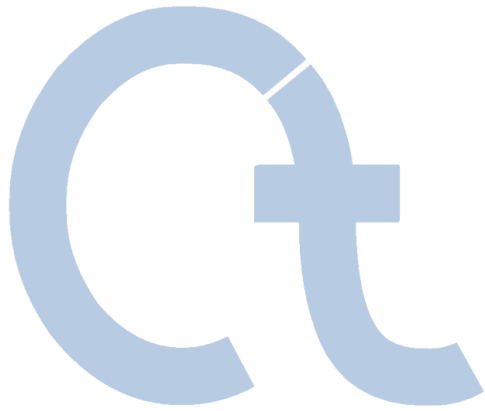
Advantages	Drawbacks
<ul style="list-style-type: none">Arbitrary binary data can be represented with a 6-bit	

Ejemplos (26)

Vista de árbol de menús de CrypTool 1.4.30



Contenido



I. CrypTool y Criptología – Visión General

II. Características de CrypTool

III. Ejemplos

IV. Proyecto / Perspectiva / Contacto

Apéndice



Desarrollo de CrypTool en el Futuro (1)

Plan después de la publicación de 1.4.30 (ver archivo Léeme)

- CT1 Test FIPS para investigar partes de tamaño mayor a 2500 bytes
- JCT Acuerdos de clave tri-partita
- JCT Visualización de la interoperabilidad de los formatos S/MIME y OpenPGP
- JCT Análisis de entropía
- JCT Grille, Vigenère Autoclave, Criptoanálisis interactivo de Cifrados clásicos
- JCT Cifrados de análisis de transposición usando el algoritmo ACO
- JCT Visualización de las pruebas de cero conocimiento
- JCT Visualización del acuerdo de clave Quantum, Protocolo BB84
- JCT Visualización del ataque SETUP contra la generación de claves RSA (Kleptografía)
- JCT Action-History con característica adicional para crear y reproducir cualquier cifrado (cascada)

- CT2 Visualización comprensible del tema de los números primos
- CT2 GNFS (Tamiz general del campo del número)
- CT2 Cifrado y criptoanálisis automatizado de la máquina Enigma y tal vez de Sigaba
- CT2 Ataque del Cubo (I. Dinur y A. Shamir, "Cube Attacks on Tweakable Black Box Polynomials", 2008)
- CT2 Demonstración de la falsificación de la firma RSA de Bleichenbacher
- CT2 Demonstración virtual de números de tarjetas de crédito (enfoque contra del abuso en tarjetas de crédito)
- CT2 Cifrado WEP y análisis WEP
- CT2 Búsqueda masiva de patrones
- CT2 Framework para criptoanálisis distribuido
- CT2 Demonstración de seguridad de SOA (mensajes SOAP a través de seguridad WS entre los participantes)
- CT2 Framework para crear y analizar cifrados de flujo LFSR

- CT2/JCT Creación de una versión en línea de comandos para un procesado por lotes
- CT2/JCT Moderna arquitectura *pure* plugin con plugins cargados

- Todo Parametrización adicional / Incrementando la flexibilidad de los algoritmos presentes

- Ideas Visualización del protocolo SSL // Demonstración de criptografía visual

CT1 = CrypTool 1.x

Nuevas versiones:

CT2 = CrypTool 2.0

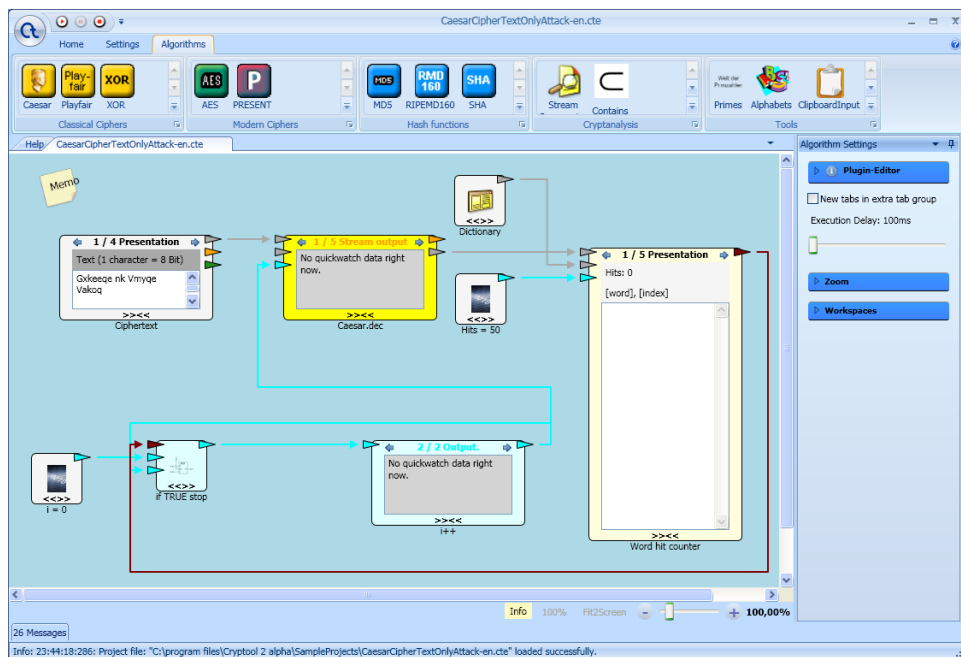
JCT = JCrypTool
(Ambos presentados a continuación)



Desarrollo de CrypTool en el Futuro (2)

En desarrollo: Las dos versiones sucesoras de CT v1 (ver archivo Léeme)

1. JCT: Portabilidad y rediseño de CrypTool en Java / SWT / Eclipse 3.6 / RPC
 - ver: <http://jcryptool.sourceforge.net>
 - Release Candidate RC3 está disponible para desarrolladores y usuarios (Julio 2010)
2. CT2: Portabilidad y rediseño de la versión en C++ con C# / WPF / VS2010 / .NET 4.0
 - Sucesor directo de las versiones actuales: perite programación visual, etc.
 - Descargar de: <http://cryptool2.vs.uni-due.de/index.php?page=14&lm=1&ql=4>
 - La versión Beta3 está disponible desde Agosto 2010 (Actualizada continuamente desde Junio de 2008)

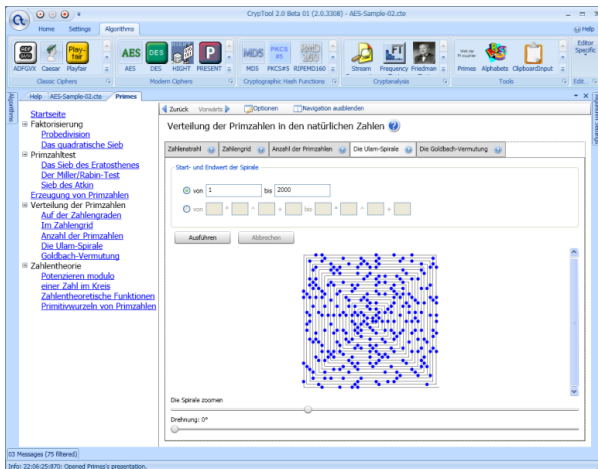
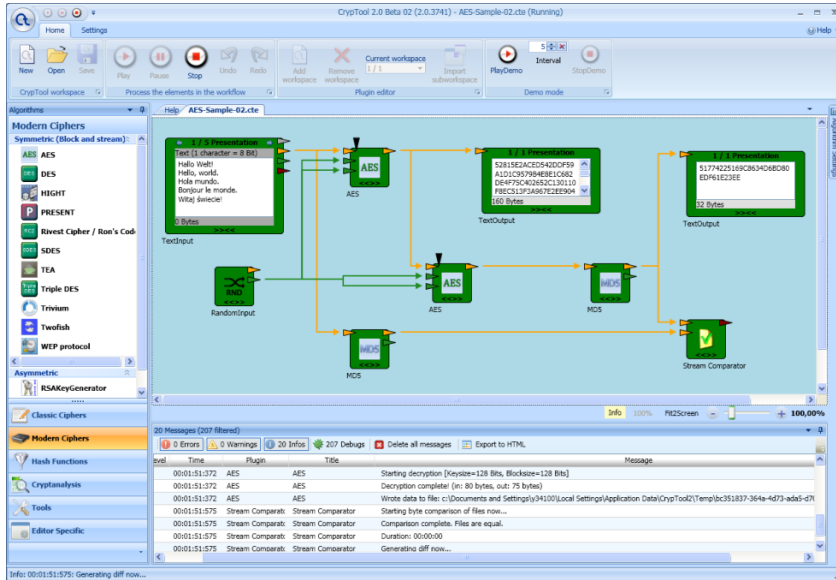


CrypTool 2 (CT2)

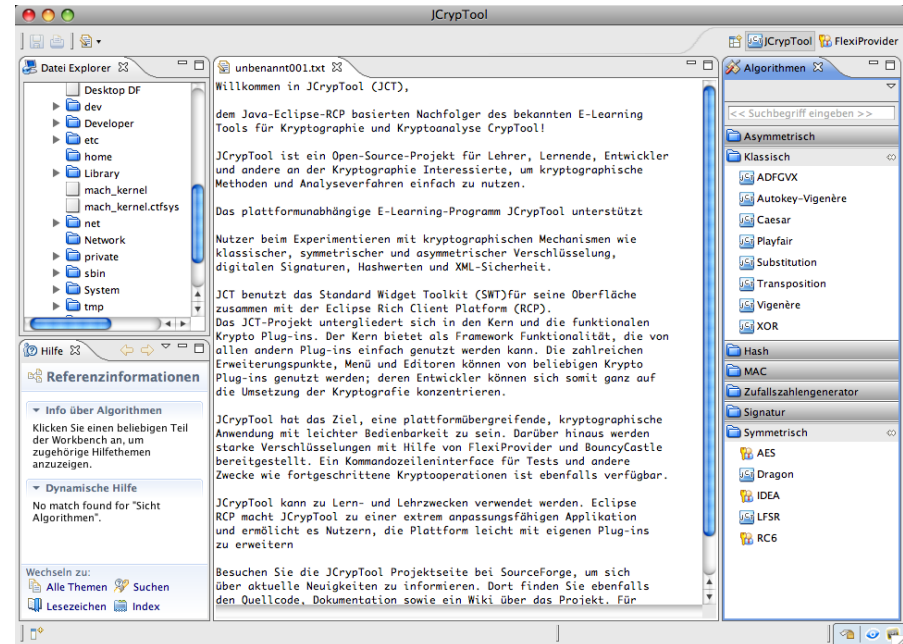


JCryptTool (JCT)

Desarrollo de CrypTool en el Futuro (3)



CrypTool 2 (CT2)



JCrypTool (JCT)

CrypTool como un “Framework”

Propuesta

- Reutilizar el amplio conjunto de algoritmos, incluyendo las librerías y los elementos de la interfaz como base
- Entrenamiento gratuito en Frankfurt, cómo empezar con el desarrollo de CrypTool
- Ventaja: Tu propio código no “desaparece”, se mantendrá

Entorno de desarrollo actual para CT1: **Microsoft Visual Studio C++ , Perl, Subversion Source-Code Management**

- Hasta CrypTool 1.4.30: Visual C++ .NET (= VC++ 9.0)(= Visual Studio 2008 Standard)
- Descripción para desarrolladores: ver readme-source.txt
- Descarga: de fuentes y binarios de las publicaciones. Para obtener los archivos fuente de las betas actuales, por favor vea el repositorio de subversiones.

Entornos de desarrollo para CT2 y JCT

- CT2 – versión C# : .NET con Visual Studio 2010 Express Edition (gratis) y WPF
- Java – versión Java: Eclipse 3.6, RCP, SWT (gratis)



CrypTool – Petición de Colaboración

Toda colaboración con el proyecto se agradece enormemente

- Realimentación de información, críticas, sugerencias e ideas
- Integración de algoritmos adicionales, protocolos, análisis (consistencia y completitud)
- Desarrollo de asistencia (programación, diseño, traducción, prueba)
 - Para el proyecto C/C++ actual
 - Para los nuevos proyectos (preferencialmente)
 - Proyecto C# : “CrypTool 2.0” = CT2
 - Proyecto Java : “JCrypTool” = JCT
 - Especialmente se invita al desarrollo adicional a las Universidades que utilizan CrypTool para propósitos educativos.
- Ejemplos de tareas abiertas se encuentran en las páginas de desarrollo respectivas:
 - CT2: Ver la lista: <http://cryptool2.vs.uni-due.de>, voluntarios, tareas actuales
 - JCT: Ver: wiki <http://sourceforge.net/apps/mediawiki/jcryptool/index.php?title=CurrentDevelopment>
- Las colaboraciones significativas se pueden referenciar por nombre (en la ayuda, Léeme, ventana Acerca de, o en la página web de CrypTool).
- Actualmente CrypTool posee más de 6000 descargas al mes (de las cuales un poco más del 50% se realiza sobre la versión en inglés).
- Las versiones Betas de las dos herramientas sucesoras (JCT y CT2) registran ya más de 1000 descargas mensuales.

CrypTool – Resumen

- EL programa de aprendizaje electrónico para criptología
- Un proyecto de Código Abierto con más de 10 años de éxito
- Más de 400.000 descargas
- Uso internacional en escuelas, universidades, así como empresas y agencias del gobierno
- Amplia ayuda online y documentación
- Disponible gratuitamente y con soporte multi-idioma

Prof. Bernhard Esslinger

Universidad de Siegen
Facultad 5, Computación y Sistemas de Información

Deutsche Bank S.A.
Director, IT Security Manager

esslinger@fb5.uni-siegen.de

www.cryptool.org

www.cryptool.com

www.cryptool.de

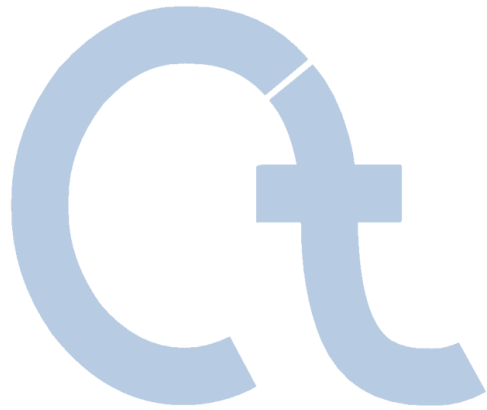
www.cryptool.es

www.cryptool.pl

Contactos adicionales: ver Léeme en la carpeta CrypTool



Contenido



- I. CrypTool y Criptología – Visión General
- II. Características de CrypTool
- III. Ejemplos
- IV. Proyecto / Perspectiva / Contacto

Apéndice

(Bibliografía adicional, sitios relacionados, descargas, etc.)

Bibliografía Adicional

Para introducirse en la Criptología

- Simon Singh, *“Los códigos secretos”*, 2000, Doubleday
- J. Ortega y Miguel Ángel López Guerrero, *“Introducción a la Criptografía”*, 2006
- Jorge Ramió, *“Libro Electrónico de Seguridad Informática y Criptografía”*
- Johannes Buchmann, *“Introduction to Cryptography”*, 2nd edition, 2004, Springer [inglés]
- Paar / Pelzl: *„Understanding Cryptography – A Textbook for Students and Practitioners “*, 2009, Springer [inglés]
- Klaus Schmeih, *“Codeknacker gegen Codemacher. Die faszinierende Geschichte der Verschlüsselung”*, 2nd edition, 2007, W3L [alemán]
- [HAC] Menezes / van Oorschot / Vanstone, *“Handbook of Applied Cryptography”*, 1996, CRC Press
- van Oorschot / Wiener, *“Parallel Collision Search with Application to Hash Functions and Discrete Logarithms”*, 1994, ACM [inglés]
- Bibliografía adicional sobre criptografía – ver también la página web de CrypTool y la bibliografía de la ayuda online de CrypTool (p.ej. por Wätjen, Salomaa, Brands, Schneier, Shoup, Stamp/Low, ...)
- La importancia de la criptografía en el amplio contexto de la seguridad en TI y la gestión de riesgos
 - Ver p.ej. Kenneth C. Laudon / Jane P. Laudon / Detlef Schoder, *“Wirtschaftsinformatik”*, 2005, Pearson, chapter 14 [alemán]
 - Ver Wikipedia (http://en.wikipedia.org/wiki/Risk_management) [inglés]
 - Página de CrypTool: <http://cryptool.com/index.php/en/cryptool-for-awareness-aboutmenu-74.html>

CRYPTOOL

Acerca de | Características | Capturas de pantalla | Documentación | Descargar

Latest stable version: 1.4.21 [Download](#)

Acerca de

Introducción a Cryptool
Cryptool en la Educación
Cryptool para el conocimiento
Cobertura en los medios
Premios
Colaboradores
Proyectos Relacionados
Contacto

Introducción a Cryptool

Cryptool es una aplicación de aprendizaje electrónico gratuita para Windows. Puede utilizarla para aplicar y analizar algoritmos criptográficos. La versión actual de Cryptool se utiliza en todo el mundo. Soporta tanto los métodos actuales de enseñanza en escuelas y universidades como la concienciación de los empleados.

La versión actual ofrece, **entre otras cosas**, lo siguiente:

- Numerosos algoritmos criptográficos, clásicos y modernos (cifrado y descifrado, generación de clave, contraseñas seguras, autenticación, protocolos seguros, ...)
- Visualización de varios métodos (p.ej. César, Enigma, RSA, Diffie-Hellman, firmas digitales, AES)
- Criptoanálisis de ciertos algoritmos (p.ej. Vigenère, RSA, AES)
- Métodos de medida criptoanalítica (p.ej. entropía, n-grams, autocorrelación)
- Métodos auxiliares (p.ej. tests de primalidad, factorización, codificación en base64)
- Tutorial sobre teoría de números.
- Ayuda detallada on-line.
- Script con más información sobre criptografía.

Desde su uso original para la formación en seguridad de una compañía, Cryptool ha evolucionado en un destacado

Descarga

"In the field of educating IT-professionals, this tool has received much support and wonder increase their knowledge. In the field of theoretical background, it has been a great help."

[Download Cryptool 1.4.x](#) | [Download Cryptool 2.0 Beta](#) | [Download JCrypTool Beta](#)

Acerca de

- [Introducción a CrypTool](#)
- [CrypTool en la Educación](#)
- [CrypTool para Concientizar](#)
- [Cobertura en los medios](#)
- [Premios](#)
- [Colaboradores](#)
- [Proyectos Relacionados](#)
- [Contacto](#)

Características

- [Características de CrypTool](#)
- [Hoja de Ruta](#)

Medios

- [Screenshots](#)
- [Screencast](#)

Documentación

- [Presentación](#)
- [Script](#)
- [Historia de la Criptografía](#)
- [Enlaces](#)

www.cryptool-online.org

Los miembros de la familia de CryptTool.

Sitios relacionados:

- **CrypTool (CT1)**
- **CT2** – para desarrolladores
- **JCT** – para desarrolladores
- **CrypTool-Online + CrypTool-Mobil**
Pruebe métodos criptográficos en su navegador y en su teléfono móvil.
- **CryptoPortal** para profesores (actualmente sólo en alemán)
- **Mystery Twister C3 (MTC3)**
Concurso de desafíos criptográficos

CrypTool-Online - Mozilla Firefox

http://www.cryptool-online.org/en

CRYPTOOL-ONLINE

About Ciphers Codings Cryptanalysis Highlights CrypTool-Homepage

Start

What is CrypTool-Online?

Ciphers
How do classical ciphers work?

Cryptanalysis
How do I obtain the clear text without the decryption key?

Codings
Where are codings used and how do they work?

Highlights
Other interesting topics, e.g. "what are secure passwords?"

Encrypt directly within your browser

CrypTool-Online provides an exciting insight into the world of **cryptology**. A great variety of ciphers, encryption methods and analysis tools are introduced, often together with illustrated examples. Our emphasis is on making explanations easy to understand with the goal to further the general interest in cryptology and cryptanalysis. Therefore, this website also provides applets to experiment with the introduced methods and to learn the principles in an **interactive way**.

You can learn the fundamentals of historically relevant ciphers in a little while (e.g. the Enigma, which significantly affected the progress of World War II), and also use the tools provided on this website to **encrypt messages yourself**. You can also decrypt and analyze already encrypted messages to educate yourself about the weaknesses of the different ciphers.

CrypTool-Online is the online version of the free e-learning program **CrypTool**. While CrypTool online is primarily intended for studying the fundamentals of classic ciphers, the download version of CrypTool is also suitable for working with longer texts and conducting high performance analyses on encrypted messages.

- **Ciphers** (among others: ADFGVX, Alberti, Bifid, Caesar, Enigma, Four-Square, Freemason, Navajo, Nihilist, Playfair, Vigenère)
- **Coding methods** (ASCII, Bacon, Base64, Code39, Huffman, Morse [you can listen, guess and learn])
- **Analysis tools** (among others: Autocorrelation, Frequency analysis, n-gram analysis)
- **Highlights** (among others: AES, Password generator, Password check, Matrix Screensaver)

Links Contact Imprint Sitemap

Copyright © 1998 - 2009 CrypTool Project / Contributors

CrypTool-Mobile

CrypTool-Online optimized for smartphones

CrypTool-Online provides an excellent introduction to the world of **cryptology**. A great variety of ciphers, encryption methods and cryptanalysis tools are introduced, often together with illustrated examples and explanations to help in making explanations easy to understand with the goal to further interest in cryptology and cryptanalysis. Therefore, this website provides interactive applets to experiment with the different ciphers in an **interactive way**.

You can learn the fundamentals of classic ciphers in a little while (e.g. the Enigma, which significantly affected the world of cryptology during World War II), and also use the tools provided on this website to encrypt and decrypt messages yourself. You can also decrypt and analyze already encrypted messages and learn about the weaknesses of the different ciphers.

CrypTool-Online is the online version of the free e-learning program **CrypTool**. While Cryptool online is primarily intended for studying the fundamentals of classic ciphers, the download version of Cryptool is also suitable for working with longer texts and conducting high performance analyses on encrypted messages.

Navigation

- Navigation
- CrypTool-Mobile
- Ciphers
 - ADFGVX
 - test ADFGX
 - test ADFGVX
 - Alberti
 - test it
 - AMSCO
 - test it
 - Autokey
 - test it
 - Beaufort
 - test it
 - Bifid
 - test it
 - Caesar / Rot-13
 - test it
 - Enigma
 - test it

Navigation

Copyright © 1998 - 2010 Cryptool Project / Contributors

Viva la
criptografía
desde su
Smartphone

CRYPTOPORTAL
für Lehrer

Über Unterrichtsmaterial Linksammlung Registrierung Cryptool Einloggen

Filterkriterien

Land:
alle Länder

Schultyp:
alle Schultypen

Autor:
alle Autoren

Material enthält folgenden Text:

Filtern Zurücksetzen

Unterrichtsmaterial

[1] **Die Stromchiffre A5**

Autor: PS
Land: Deutschland - alle Bundesländer
Schultyp: Gymnasien

In dieser Ausarbeitung zum Seminar IT-Sicherheit wird der auf der Verschaltung von linear rückgekoppelten Schieberegistern (LFSR) basierende Algorithmus A5 und die bisher gefundenen [...]

[a5_thesis.pdf](#) 8 mal heruntergeladen

[2] **Die wichtigsten Verfahren der Kryptologie**

Autor: HW
Land: Deutschland - Berlin
Schultyp: alle Schultypen

Die Präsentation besteht aus zwei Folien. In der ersten wird die Entwicklung der klassischen Kryptographie (von Caesar bis zum one-time-pad) dargestellt. In der zweiten wird ein Überblick zur [...]

[Krypto-Entwicklung.ppt](#) 15 mal heruntergeladen

[3] **Kryptografie für Jedermann**

Autor: Consultant
Land: Deutschland - alle Bundesländer
Schultyp: alle Schultypen

Einführung in die Kryptografie, Erläuterungen zu populären kryptografischen Primitiven und Protokolle [...]

[Originalpraesentation.pdf](#) 14 mal heruntergeladen

El portal para profesores se encuentra sólo en alemán. Se acepta gustosamente ayuda para su versión en español o en inglés.

http://www.mysterytwisterc3.org/

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST beta

PEOPLE THAT ALREADY JOINED C3:
39
[Register here](#)

C3 PARTNERS

Start Challenges Forum MysteryTwister I Login EN DE

About C3 Partners

FOUR LEVELS OF CHALLENGES

MysteryTwister C3 offers something for everybody by featuring four levels of challenges, from pen-and-paper riddles to highly sophisticated mathematical mysteries.

[Register here](#)

The three levels

- Level I Challenges - Pen & Paper**
Level I challenges are very similar to standard puzzles from newspapers and can be solved with little cryptographic background. You don't need a computer for solving level I challenges. All you need is a little bit of creative thinking and probably some paper and a pencil. Solving a level I challenge probably needs the solver within minutes or even seconds. The algorithms needed are usually built into tools of those kind of cryptosystems. Hence, if you are a beginner in the area of cryptology (e.g., a student), but nevertheless interested in this mysterious topic of cryptology, give challenges of level I a try. A feeling of success is almost guaranteed after a very short time.
- Level II Challenges - Programming skills required**
Level II challenges require some background knowledge in cryptology and usually some computational power. Additionally, the tasks needed are most likely not yet in a ready-to-use fashion available in cryptology tools like CryptTool. Therefore, you first need to understand the problem and second you need to write a computer program, which might not be a single line of code implementation, in total it might take a few hours to days to solve a level II challenge. Hence, if you consider yourself well armed with cryptology knowledge (e.g., being a student participating in a cryptology course at the university), give challenges in level II a try. The feeling of success will not come easy, but it will be worthwhile.
- Level III Challenges - Large amount of computing power could be useful**
Level III challenges require profound background in cryptanalysis and usually a lot of computational power at your disposal. The problems given in this level represent current research questions which we believe to be highly difficult. Therefore practicable solutions might or might not exist.

What is MTC3?

C3? MysteryTwister C3 (MTC3), successor of the famous **MysteryTwister** site, is an international cryptography competition. A variety of tasks and challenges are offered at four levels of difficulty. These challenges can be as easy as deciphering a Caesar cipher (Level I) and as hard as breaking a modern encryption algorithm like AES (Level III). Some of the challenges are still today unsolved (Level X). The various topics covered by the MTC3 challenges are intended to offer a survey of cryptology for everyone. The **four levels** of difficulty in MTC3 offer cryptographic challenges for a student just starting to learn about cryptography as well as for experts with many years of experience and plenty of resources at their disposal.

Mystery Twister C3 es un concurso de desafíos criptográficos.

¡Descargue el software y el CrypTool Script!

CRYPTOOL

Acerca de Características Medios **Documentación** Descargas

Última versión CT1 estable: 1.4.21 [Download](#)

Beta estable 1.4.30
Descargar & probar ahora!

Documentación

- Presentación
- Script**
- Historia de la Criptografía
- Links

Script

Versión Actual: 10ª edición, Enero 2010
[Descarga el script](#)

En este script proporcionado con la aplicación CrypTool encontrará matemáticamente para el uso en procedimientos criptográficos. Los autores y son, por lo tanto, independientes los unos de los otros. Al bibliográficas y enlaces web.

CRYPTOOL

Acerca de Características Medios Documentación **Descargas**

Última versión CT1 estable: 1.4.21 [Download](#)

Beta estable 1.4.30
Descargar & probar ahora!

Descarga

[Download CrypTool 1.4.x](#) [Download CrypTool 2.0 Beta](#) [Download JCrypTool Beta](#)

CrypTool 1.4.21
(Para esta versión de CrypTool en español, favor descargar adicionalmente los archivos de ayuda [aquí](#))

La versión actual publicada para usuarios es CrypTool 1.4.21 (publicada el 11 de Julio de 2008).

Esta versión necesita un entorno Win32. El programa contiene algunas funciones que llaman a aplicaciones Java. Para poder ejecutar estas aplicaciones, deberá tener instalada una máquina virtual Java (JRE 1.5 ó superior).

El código de la versión publicada (etiqueta "CrypTool_1_4_21") y los códigos actuales de desarrollo están disponibles en el repositorio. Todo el mundo tiene acceso de lectura a este [repositorio](#) (Usuario y contraseña: anonymous).

CrypTool 1.4.x está disponible en Inglés, alemán, español y polaco:

- [CrypTool 1.4.21 - Inglés](#)
- [CrypTool 1.4.21 - Alemán](#)
- [CrypTool 1.4.21 - Español](#)
- [CrypTool 1.4.10 - Polaco](#)

script-en.pdf - Adobe Reader

1 (1 von 281) 66,9%

Leesezeichen

- Overview
- Contents Overview
- Contents
- Preface to the 10th Edition of the CrypTool Script
- Introduction -- How do the Script and the Program Play together?
- 1 Encryption Procedures
- 2 Paper and Pencil Encryption Methods
- 3 Prime Numbers
- 4 Introduction to Elementary Number Theory with Examples
- 5 The Mathematical Ideas behind Modern Cryptography
- 6 Hash Functions and Digital Signatures
 - 6.1 Hash functions
 - 6.2 RSA signatures
 - 6.3 DSA signatures
 - 6.4 Public key certification
- Bibliography
- 7 Elliptic Curves
- 8 Crypto 2020 --- Perspectives for Long-Term Cryptographic Security
- A Appendix
 - A.1 CrypTool Menus
 - A.2 Authors of the CrypTool Script
 - A.3 Movies and Fictional Literature with Relation to Cryptography, Books for Kids with Simple Ciphers
 - A.4 Learning Tool for Elementary Number Theory
 - A.5 Using Sage with this Script
- GNU Free Documentation License
- List of Figures
- List of Tables
- List of Crypto Procedures
- List of Sage Code Examples
- Index

The CrypTool Script

Cryptography, Mathematics, and More

Prof. Bernhard Esslinger
and the CrypTool Development Team

10th Edition

Background reading
for CrypTool the free e-learning program
(with number theory code samples for Sage)