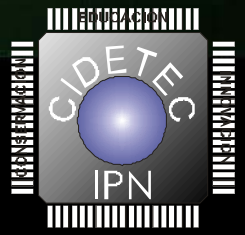
Introducción a la Criptografía

M. en C. Eduardo Rodríguez Escobar
CIDETEC - IPN



Contenido

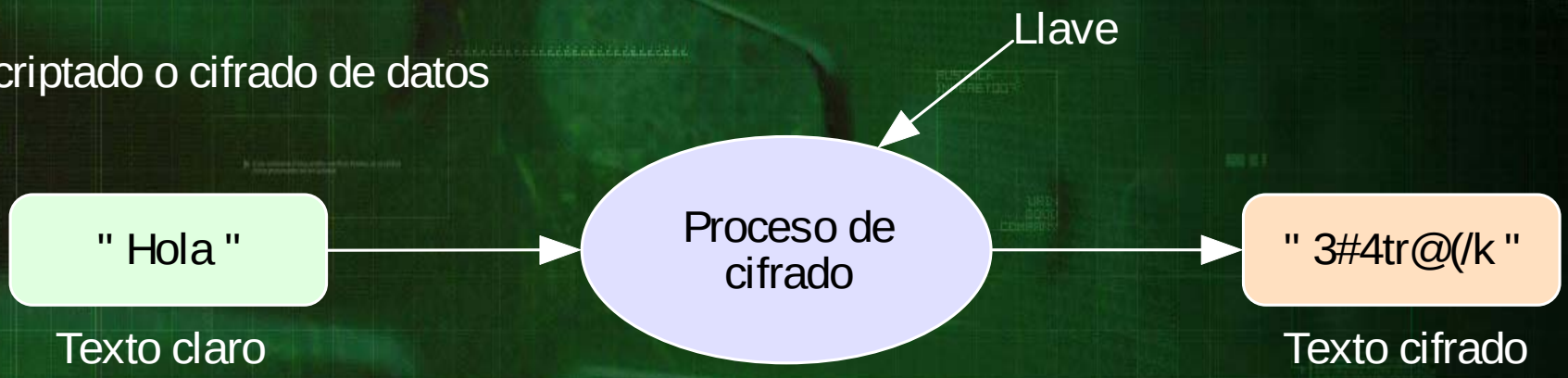
- Terminología.
- Proceso Criptográfico.
- Componentes de la Seguridad de Datos en un Sistema Criptográfico.
- Criptoanálisis.
- Clasificación de la Criptografía.
- Criptografía Clásica.
  - Por sustitución.
  - Por transposición.
  - De una sola vez.
- Época Intermedia.
  - Máquinas Cifradoras.
- Criptografía Moderna.
  - De flujo.
  - De Bloque.
  - De llave pública.

Terminología

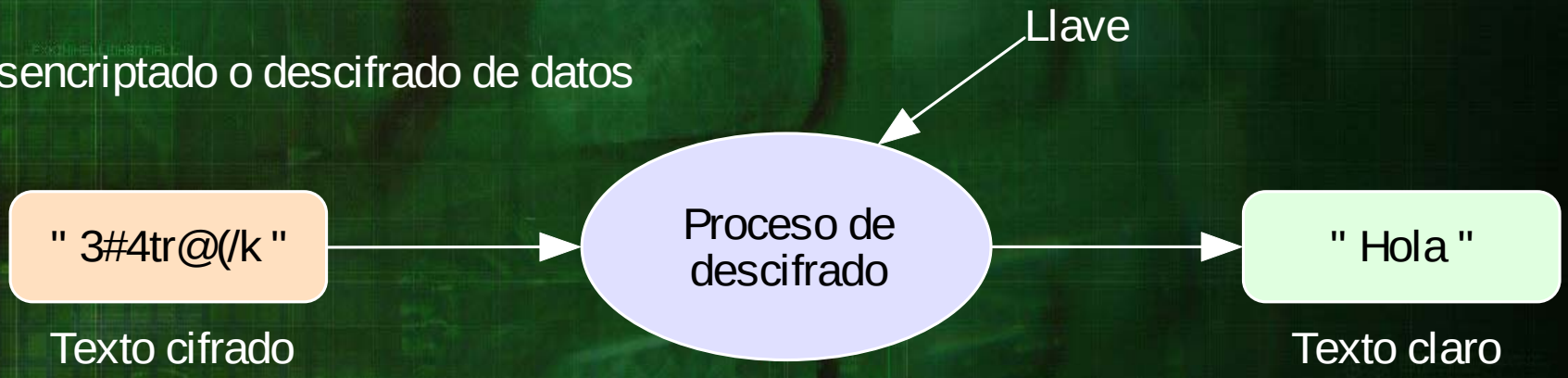
- Criptología: La palabra criptología proviene de las palabras griegas *Kryptos* y *Logos*, y significa estudio de lo oculto.
- Criptografía: Proviene de las palabras griegas *Kryptos* y *Graphos*, y significa “ocultado” (cifrado) de mensajes.
- Criptoanálisis: Arte y ciencia que intenta romper el cifrado (descubrir el texto claro).
- Texto claro: Mensaje que se puede leer.
- Cifrado o Encriptado: Proceso de transformación del texto claro que lo vuelve ilegible.
- Texto cifrado: Mensaje en texto claro que ha sido cifrado.
- Descifrar o Desencriptar: Proceso que permite obtener el texto claro a partir del texto cifrado.

Proceso criptográfico

a) Encriptado o cifrado de datos



b) Desencriptado o descifrado de datos



Componentes de la Seguridad de Datos en un Sistema Criptográfico

- Privacidad o confidencialidad: Estar seguro que un mensaje o una conversación no pueda ser descifrada por un tercero.
- Integridad de datos: La información del mensaje no puede ser cambiado en el proceso de envío.
- Autenticación (remitente y la persona que va a recibir el correo, pueden confirmar la identifica-ción y el origen del mensaje).
- No-repudiación (el remitente no puede reclamar que no es el remitente).
- Función 1 a 1 (Existe una y solo una función que nos lleva del dominio X [texto claro] al dominio de Y [texto cifrado] y viceversa).

Criptoanálisis

- Objetivo: recuperar el texto claro sin tener acceso a la llave de cifrado.
- Un intento de criptoanálisis es llamado un ataque.
- El criptoanalista tiene conocimiento detallado del algoritmo y su implementación
  - Lo único secreto es la llave de cifrado.
  - No se puede depender del desconocimiento del algoritmo.

Clasificación de la Criptografía

- Clásica, convencional, simétrica o de clave secreta
- Moderna, asimétrica o de clave pública

Clasificación de la Criptografía …

- Criptografía clásica
  - Cifrados por sustitución
  - Cifrados por transposición
  - Rellenos de una sola vez
- Criptografía moderna
  - Algoritmos simétricos
  - Algoritmos asimétricos

Criptografía clásica

- Llamamos así a todos los sistemas de cifrado anteriores a la II Guerra Mundial, o lo que es lo mismo, al nacimiento de las computadoras electrónicas.
- Se basa en algoritmos sencillos y claves muy largas para “asegurar” seguridad. Presupone la existencia de claves previamente establecidas por ambas partes del proceso de comunicación.
- Perdieron su eficacia, debido a que son fácilmente criptoanalizables por los ordenadores.
- Todos los algoritmos criptográficos clásicos son simétricos

Criptografía clásica …

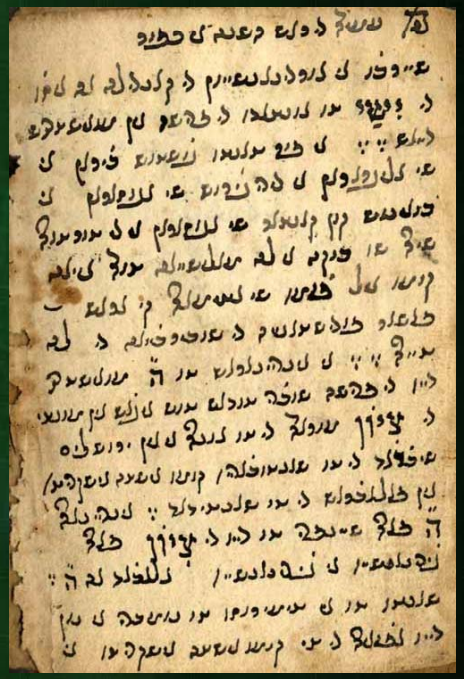
- Cifrados por sustitución

Se basan en la sustitución de cada letra por otra letra para disfrazarla, pero conservan el orden de los símbolos de texto normal.

- Atbash
- Cifrado del César
- Métodos de cifrado monoalfabéticos
- Métodos de cifrado polialfabéticos

Criptografía clásica …

- Cifrados por sustitución …
  - ❖ Atbash –Alfabeto hebreo al revés (500 AC)
    - Descubierto en los papiros de Qumran en el libro de Jeremías
    - Equivale a “A – Z”, “B – Y”, …



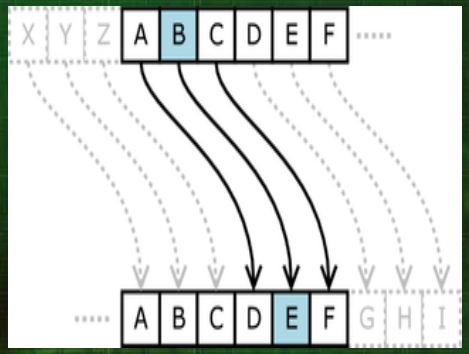
Letters from the top	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Letters from the bottom	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

gato → tzgl

Criptografía clásica …

- Cifrados por sustitución …

  - Cifrado del César (Imperio Romano, 49-60 AC)
    - letra = letra + 3



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
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

gato → jdwr

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado monoalfabéticos

- Sustituyen cada letra por otra que ocupa la misma posición en un alfabeto desordenado y esta correspondencia se mantiene a lo largo de todo el mensaje. Así se consiguen tantas claves como posibilidades de alfabetos hay.
- El problema está en cómo recordar la clave (el alfabeto desordenado).
- El mejor sistema de criptoanálisis para romper el algoritmo es el estadístico. Se puede romper vía análisis de frecuencia de letras

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado monoalfabéticos …

- El procedimiento es el siguiente:
- Se busca una palabra (clave) fácil de recordar y se le quitan las letras duplicadas.

SEGURIDAD ➔ SEGURIDA

- Se añaden al final de la palabra las restantes letras del alfabeto (sin duplicar letras).

SEGURIDABCFHJKLMNOPQTVWXYZ

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado monoalfabéticos …

- Se ordenan en una matriz cuya primera fila es la palabra clave

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

- El nuevo alfabeto se lee por columnas y se alinea con el original:

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
s	b	n	y	e	c	o	z	g	f	p	u	h	q	r	j	t	i	k	v	d	l	w	a	m	x

- Ejemplo: el mensaje *ataque* se convertiría en SVSTDE
- Ejemplo: gato → osvq

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado polialfabéticos (siglo XV)

- Se usan varios cifradores sustitutivos monoalfabéticos, dependiendo de la posición de la letra en el texto.
- Leon Battista Alberti inventa y publica el primer cifrador polialfabético (1459)
  - Este cifrador no fue roto hasta el siglo XIX.

Criptografía clásica …

- Cifrados por sustitución …

❖ Métodos de cifrado polialfabéticos (siglo XV)

- Un ejemplo típico es el Cifrado de Vigènere:

  - Se basa en una tabla con un alfabeto por cada letra del abecedario

- Método:
  - Se busca una palabra clave fácil de recordar.
  - Se escribe la palabra debajo del texto en claro, repitiéndose tantas veces como sea necesario.
  - Cada letra del texto en claro se codifica con el alfabeto de la tabla marcado por la letra inferior, o sea, la letra de la clave que corresponde.

Criptografía clásica …

- Cifrados por sustitución …
- Métodos de cifrado polialfabéticos (siglo XV)

	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

- Ejemplo:
  - Clave:
    - ADIOS
  - Texto claro :
    - E S T O E S C R I P T O L O G I A
  - Clave sec.:
    - A D I O S A D I O S A D I O S A D
  - Criptograma:
    - E V B C W K F Z E H T R T C Y I D

gato → gdbe

Criptografía clásica …

- Cifrados por transposición

  - Se basa en la reordenación de las letras de un texto de acuerdo a una palabra clave escogida que no contiene letras repetidas.
  - Método:
    - Con la clave se numera las columnas, estando la columna 1 bajo la letra de la clave más cercana al inicio del alfabeto, y así sucesivamente.
      - El texto normal se escribe horizontalmente en filas.
      - El texto cifrado se lee por columnas, comenzando por la columna cuya letra clave es más baja
  - Se puede criptoanalizar efectuando un estudio estadístico sobre la frecuencia de aparición de pares y tripletas de símbolos

Criptografía clásica …

- Cifrados por transposición …
  - Ejemplo:
    - Texto normal:
      "Este es un trabajo para la asignatura de Redes"
  - Clave: Video
  - Texto cifrado:

T ROAAA E EUA STDD SSTJR NAR
NBPLIUEE EE AAAGR S

V	I	D	E	O
5	3	1	2	4
E	s	t	e	
e	s		u	n
	t	r	a	b
a	j	o		p
a	r	a		l
a		a	s	i
g	n	a	t	u
r	a		d	e
	R	e	d	e
s				

Criptografía clásica …

(México y la 1era. Guerra Mundial)

- El telegrama Zimmerman
  - 1917, Primera Guerra Mundial
  - Alemania usa submarinos para hundir barcos americanos.
    - Lo anterior puede provocar el que USA entre a la guerra.
  - Arthur Zimmermann, Ministro alemán del Exterior, se le ocurre como retrasar la entrada de USA en la guerra.
    - Propone una alianza con México y persuadir al Presidente Carranza para que invada USA reclamando Texas, Nuevo Mexico y Arizona.
    - Alemania apoyaría a México militar y financieramente.
    - El Presidente Mexicano debía persuadir a Japón para que ataque USA.

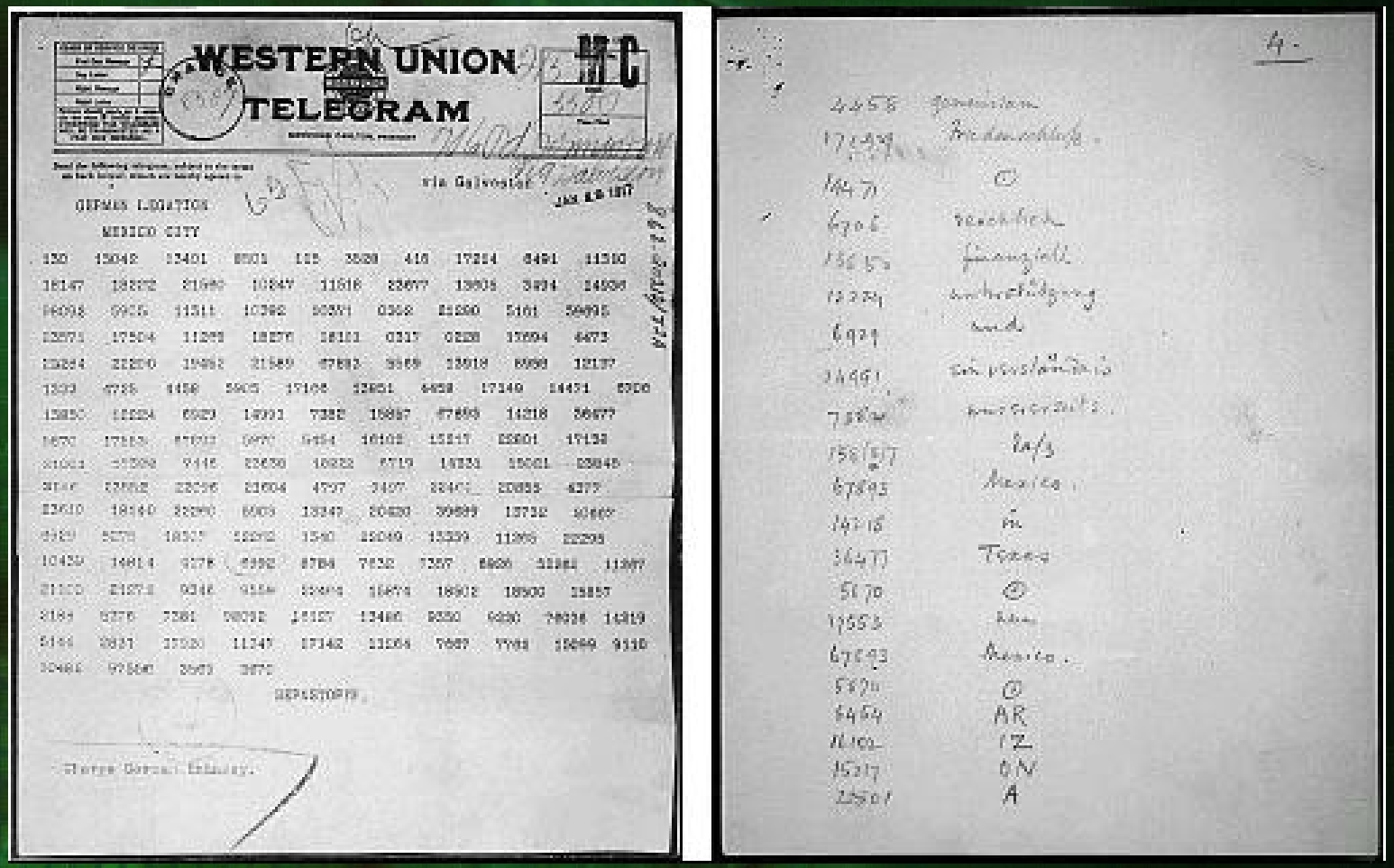
Criptografía clásica …

(México y la 1era. Guerra Mundial)

- El telegrama Zimmerman …
  - Telegrama enviado vía el cable del Atlántico.
    - Mensaje del 17 de enero de 1917.
    - Los criptoanalistas británicos Montgomety & de Grey descifran parte del mensaje.
      - Usan el code book de un diplomático alemán.
      - El libro se obtuvo de los bienes confiscados a Wihelm Wassmus, el Vicecónsul alemán en Persia, el cual dejo sus oficinas apresudaramente cuando las fuerzas británicas avanzaron.
      - El telegrama completo es obtenido posteriormente del mismo Zimmerman.

Criptografía clásica …

- El telegrama Zimmerman …



Criptografía clásica …

- El telegrama Zimmerman …

"Tenemos la intención de comenzar la guerra submarina sin restricciones a partir del primero de febrero. Se intentará, no obstante, que los Estados Unidos se mantengan neutrales. Para el caso de que no sea posible lograrlo, ofrecemos a México una alianza sobre las siguientes bases: guerra conjunta, tratado de paz conjunto, generosa ayuda financiera y acuerdo por nuestra parte de que Méjico podrá reconquistar los territorios de Tejas, Nuevo Méjico y Arizona perdidos en el pasado. Dejo los detalles a su excelencia. Sírvase usted comunicar lo anteriormente dicho al presidente, en el más absoluto secreto, tan pronto como la declaración de guerra contra Estados Unidos sea algo seguro, y sugiérale que invite inmediatamente, por iniciativa propia, a Japón para unirse y que haga de intermediario entre nosotros y Japón. Sírvase advertir al presidente que el uso despiadado de nuestros submarinos ofrece ahora la perspectiva de que Inglaterra sea forzada a la paz en pocos meses.

Acuse recibo. Zimmermann. Fin del telegrama."

Criptografía clásica …

- Rellenos de una sola vez
  - One Time Pad

Mensaje	s	e	c	r	e	t	o	
	18	5	3	17	5	20	15	(posición alfabética)
OTP	-15	8	1	12	19	5	6	(desplazamiento)
	3	13	4	3	24	25	21	(nueva posición)
	c	m	d	c	x	y	u	(mensaje encriptado)

  - Es 100% seguro si el OTP se usa una sola vez y se compone de números aleatorios no pre-decibles.

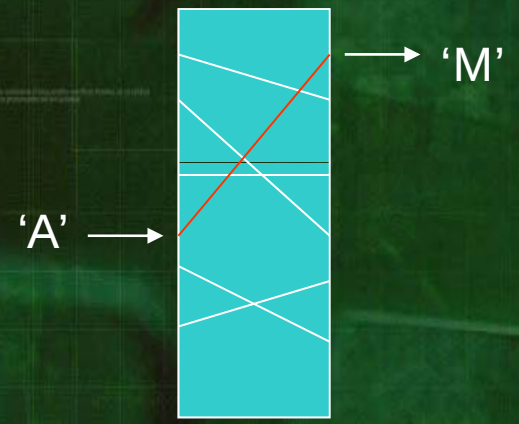
Criptografía clásica …

- Rellenos de una sola vez
  - One Time Pad
  - Usado por:
    - Espías de la URSS y de la CIA
    - “teléfono rojo” Washington – Moscú
  - Muchos algoritmos dicen ser seguros por ser un OTP
    - Si el OTP no es realmente aleatorio, no es OTP
    - Pseudo-OTP = pseudo-seguridad
  - Máquinas cifradoras trataron de parecerse a un OTP, primero mecánicamente y luego electrónicamente

Época intermedia

Máquinas Cifradoras (1920)

- Componente básica = rotor alambrado

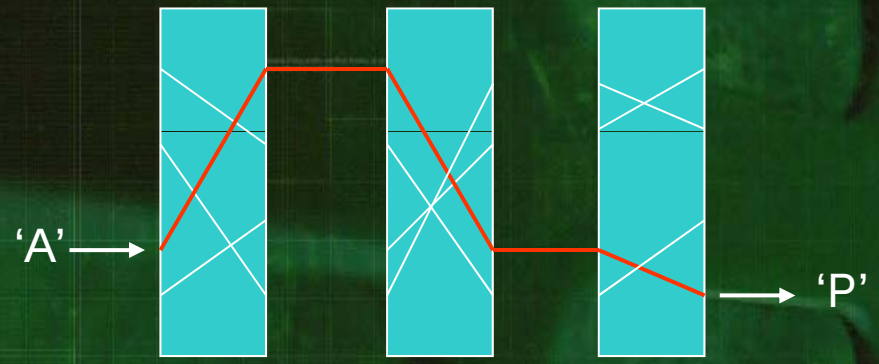


- El rotor rota después de cada letra
  - sustitución polialfabética, período=26

Época intermedia

Máquinas Cifradoras …

- Se pueden encadenar varios rotores



• Cada uno hace rotar al siguiente cuando completa una vuelta

Época intermedia

Máquinas Cifradoras…

- Dos rotores
  - Período = 676 (26 x 26)
- Tres rotores
  - Período = 17.576 (26 x 26 x 26)
- Llave = alambrado del rotor (por lo general, fijado cuando se fabrica el rotor)
- Llave = posición inicial de los rotores

Época intermedia

Rotores Famosos

- Converter M-209 (EE.UU.)
- TYPEX (Inglaterra)
- Rojo, Púrpuro (Japón)
- Enigma (Alemania)

- Muchos libros escritos sobre Enigma
  - *Seizing the Enigma,* Kahn
  - *Ultra Goes to War,* Levin
  - *The Hut Six Story,* Welchman
  - *The Ultra Secret,* Winterbothm

Criptografía Moderna

- Cifradores de flujo
  - RC4
- Cifradores de Bloque
  - DES
- Cifrado de Llave Pública (asimétrica)

Criptografía Moderna …

- Cifradores de flujo

  - Se usa una llave binaria de flujo con un XOR.

```
Texto claro                1 0 0 1 0 1 1
Llave de flujo             0 1 0 1 1 0 1
Texto cifrado (XOR)        1 1 0 0 1 1 0
Llave de flujo             0 1 0 1 1 0 1
Texto claro (XOR)          1 0 0 1 0 1 1
```

  - Dos XOR’s con un mismo bit se cancelan.

Criptografía Moderna …

- Cifradores de flujo…
  - Desventajas:
    - Conociendo la llave de flujo y el texto cifrado, se obtiene el texto claro, y
    - Conociendo el texto claro y el texto cifrado, se obtiene la llave de flujo
    - En una operación XOR, conociendo 2 de los 3 elementos, se obtiene el tercero
  - Luego, nunca se puede volver a usar la misma llave.
  - No es buena idea usar este tipo de cifrador.

Criptografía Moderna …

- Cifradores de flujo…
- RC4
  - Cifrador de flujo optimizado para una eficiente implementación en software.
  - Con llave de 2048 bits y resultado de 8 bits.
  - Algoritmo era un secreto industrial de RSADSI. En 1994 se le sometió a ingeniería inversa y su código fuente fue publicado en Internet.

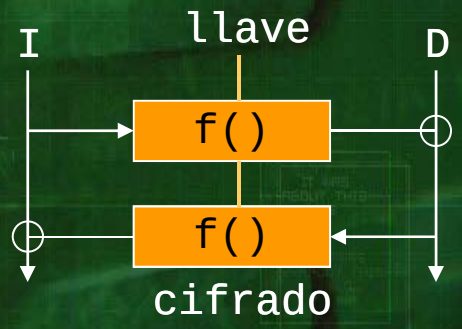
```
while (length--) {
    x++; sx = state[x]; y += sx;
    sy = state[y]; state[y] = sx; state[x] = sy;
    *data++ ^= state[ (sx+sy) & 0xFF ];
}
```

Criptografía Moderna …

- Cifradores de flujo...
- RC4...
  - Es extremadamente rápido.
  - Se usa en SSL, Lotus Notes, cifrado de password en Windows, MS Access, Adobe Acrobat, PPTP, Oracle Secure SQL, ...
    - Se suele usar de manera que hace posible recuperar la llave de cifrado.
    - Todos los productos de Microsoft que lo usan lo han implementado mal al menos una vez.
  - Demuestra que un cifrador no puede ser usado como caja negra mágica.
  - Recomendación: evitarlo ya que es fácil equivocarse.

Criptografía Moderna …

- Cifradores de Bloque
  - Cifran un bloque de datos de tamaño fijo con una llave de cifrado de tamaño fijo.
  - Se originan a comienzo de los 70's en IBM, que desarrollaba sistemas seguros para los Bancos.
  - El primero conocido fue Lucifer, con llave y bloque de 128 bits.
    - Nunca fue seguro en ninguna de sus versiones



Criptografía Moderna …

- Cifradores de Bloque…
  - Función f() es una transformación simple, no necesariamente reversible.
  - Cada paso se llama un round.
  - Mientras más rounds se tengan, más seguro es (hasta un cierto límite).
  - El más famoso ejemplo de este diseño es DES:
    - 16 rounds.
    - Llave de 56 bits.
    - Bloque de 64 bits (I,D = 32 bits).

Criptografía Moderna …

- DES (Data Encryption Standard)
  - En 1972, NBS (National Bureau of Standards), ahora NIST (National Institute of Standards and Technology) inicia un programa para proteger datos en los computadores y lograr la transmisión segura de datos en una red.
  - En mayo de 1973, NBS publica un requerimiento de un algoritmo criptográfico que:
    - Ofrezca un alto nivel de seguridad,
    - Se especifique completamente y sea entendible,
    - La seguridad dependa sólo de la llave,
    - Debe estar disponible para todos los usuarios,
    - Debe ser eficiente, implementable electrónicamente a un costo razonable,
    - Debe ser factible de validar y se debe poder exportar
  - Ningún algoritmo presentado cumplía todo esto.

Historia de DES…

- En agosto de 1974, se publica un segundo llamado:
  - IBM presentó a Lucifer.
  - Aparentemente cumplía con todo.
  - NBS le pide a la NSA (National Security Agency) ayuda en la evaluación de la seguridad del algoritmo.
  - En marzo de 1975, NBS publica el algoritmo (modificado por la NSA) y pide comentarios
    - Muchos comentarios sospechaban de la NSA (cambio del largo de la llave de 112 a 56 bits, detalles del algoritmo)
  - En noviembre de 1976, DES es adoptado como un estándar federal en los EE.UU.

Rol de la NSA en DES

- Mucho tiempo después, se supo que:
  - Hubo un malentendido entre la NSA y la NBS.
  - La NSA pensó que DES se iba a implementar en hardware solamente.
  - El estándar habla de hardware, pero la publicación del algoritmo era tan detallada que permitió implementarlo en software.
  - Off the record, NSA dijo que DES fue uno de los errores más grandes que cometió y que nunca habría dejado que se publicara si hubiesen sabido que se iba a implementar en software.
  - Ahora el mundo tenía un algoritmo sancionado como seguro por la NSA, algo inédito.

Revisiones de DES

- Cada 5 años, NBS debía ratificar a DES como estándar o proponer cambios:
  - En 1983, DES fue ratificado sin problemas.
  - En 1987, la NSA dijo que no iba a ratificar el estándar y propuso reemplazarlo por una serie de algoritmos secretos que sólo estarían disponible en hardware controlado. Los bancos reclamaron que el uso de DES era masivo y no podía ser reemplazado. Fue ratificado pero NBS dijo que sería la última ratificación...
  - En 1993, NBS (ahora llamada NIST) se ve obligada a ratificar nuevamente DES al no haber alternativa. En esta ratificacion aparece el llamado 3DES o triple-DES, con una seguridad de 2^{168} y empleado actualmente como standard bancario.

DES...

- Existen 4 formas “oficiales” (FIPS PUB 81) de extender DES para cifrar más de 64 bits:
  - ECB (Electronic Code Book): cada bloque de 64 bits se cifra individualmente. Dos bloques en claro idénticos generan el mismo bloque cifrado.
  - CBC (Cipher Block Chaining): se hace XOR de cada bloque con el bloque cifrado anterior antes de cifrar. Al primer bloque se le hace xor con un valor secreto inicial de 64 bits. Dos bloques en claro idénticos no generan el mismo bloque cifrado. Es más robusto que ECB.
  - CFB (Cipher Feedback Block) y OFB (Output Feedback Block) permiten cifrar “n” bits donde n es arbitrario con una extensión del DES original.

Cifrado de Llave Pública

- Nuevo paradigma de cifrado publicado en 1976.
- Basado en la Teoría de Números.
- Seguridad de estos algoritmos se basa en dificultad de factorizar números grandes.
- Varios algoritmos de este tipo han sido inventados, pero sólo unos pocos han demostrado ser seguros hasta ahora.
- Dos llaves: una pública y una privada (secreta)
  - Todo lo que se cifra con una llave sólo se puede descifrar con la otra llave.
- RSA es el más conocido.
  - Rivest, Shamir y Adleman (1978, MIT)

RSA

- Llave pública y privada se obtienen de números primos grandes (100-200 dígitos y más).
- Quebrar RSA equivale a factorizar el productos de dos de estos números primos.
- Para generar ambas llaves, se escogen 2 números primos grandes aleatorios p y q (del mismo tamaño).
- Se calcula el producto $n = pq$
- $\Phi(n)=(p - 1)(q - 1)$ ya que p y q son primos
- Se escoge la llave de cifrado e tal que:
  - $e < (p - 1)(q - 1)$ y es primo relativo de $(p - 1)(q - 1)$

RSA vs. DES

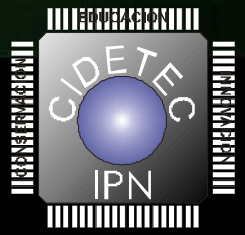
- Las llaves RSA (512, 1024, 2048 bits) son mucho más grandes que las llaves DES
  - Una llave RSA de 1024 bits equivale más o menos a una llave 3DES (112 bits) en cuanto a la dificultad en adivinar la llave.
- RSA en software es 100 veces más lento que DES
  - Nunca podrá ser tan rápido como DES por los algoritmos involucrados y el tamaño de las llaves.
  - RSA no se puede usar directamente para cifrar tráfico en una red de alta velocidad (10, 100 Mbps o más).

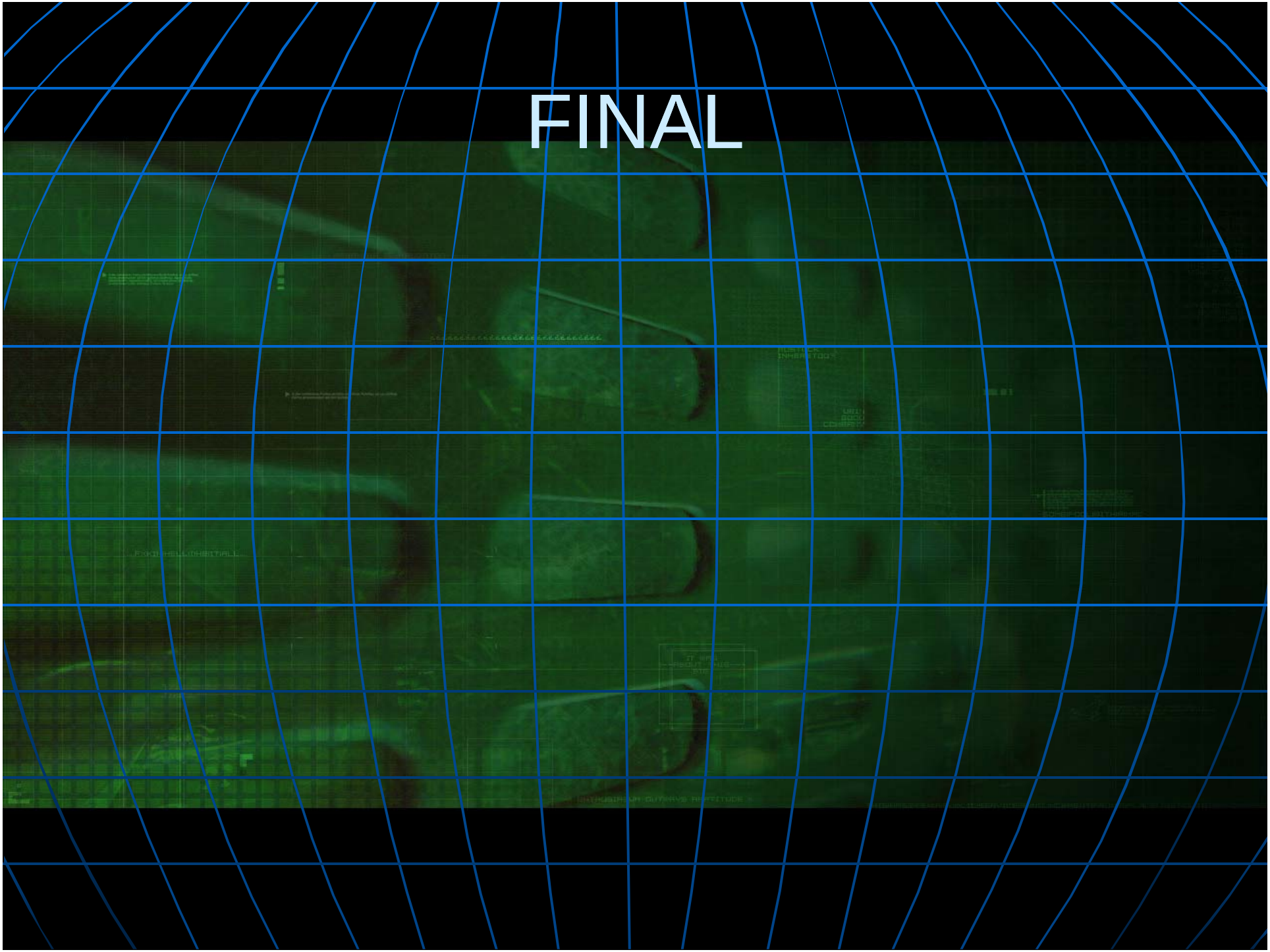
MD5 (Message Digest)

- Es una versión mejorada de MD4 (1990) que Ron Rivest (de RSA) presentó en 1992.
- MD5 procesa el mensaje en bloques de 512 bits que se dividen en 16 sub-bloques de 32 bits c/u.
- El resultado son 4 números de 32 bits que se concatenan para entregar el valor de hash de 128 bits.
- El mensaje original se expande para tener un largo múltiple de 512 bits menos 64.
  - El relleno es un bit en 1 seguido de bits en 0.
  - Al final se agregan 64 bits que representan el largo del mensaje, lo que deja el largo en un múltiple de 512 bits.

Introducción a la Criptografía

M. en C. Eduardo Rodríguez Escobar
CIDETEC - IPN




FINAL

Criptoanálisis …

- Existen 4 tipos generales de ataques:
  - Ataque de sólo texto cifrado: el criptoanalista tiene el texto cifrado de varios mensajes, todos cifrados con el mismo algoritmo. Debe recuperar el texto claro del mayor número de mensajes o deducir la o las llaves de cifrado.
  - Ataque de texto claro conocido: tiene el texto claro y el correspondiente texto cifrado de varios mensajes. Debe deducir la llave o llaves de cifrado, o bien deducir un algoritmo para descifrar cualquier otro mensaje cifrado con la misma llave.

Criptoanálisis …

- Ataque de texto claro elegido: No sólo tiene acceso al texto cifrado y texto claro de varios mensajes, sino que puede elegir el texto claro que quiera cifrar para facilitar la deducción de la llave.
- Ataque adaptivo de texto claro elegido: variación del anterior. No sólo puede elegir el texto claro a cifrar, sino que lo puede modificar basado en los resultados de los cifrados previos (por ej, puede cifrar un subconjunto de un texto previamente cifrado).

Criptoanálisis …

- Existen otras 3 variaciones de ataques:
  - Ataque de texto cifrado elegido: El criptoanalista puede descifrar cualquier texto cifrado y obtener el texto claro correspondiente. Debe deducir la llave de descifrado.
  - Ataque de llaves relacionadas: El criptoanalista conoce una relación entre dos llaves (pero no las llaves en sí). Elige un texto en claro y puede conocer el resultado de cifrar ese texto con las dos llaves. Debe deducir las dos llaves.
  - Ataque de compra de llave: El criptoanalista “compra” (vía chantaje, tortura, amenaza, etc) la llave. Es un ataque muy poderoso y muchas veces la mejor manera de conseguir la llave.