



Mecanismos de protección de datos en videojuegos

Alumno:

Benito Palacios Sánchez

Tutor:

Dr. D. Pedro García Teodoro
Dpto. Teoría de la Señal, Telemática y
Comunicaciones

15 de julio de 2015

Objetivo

Analizar, estudiar y documentar algoritmos de protección de datos implementados en videojuegos.

Índice de contenidos

- 1 Introducción
- 2 Traducciones no oficiales
 - Metodología
 - Saga Pokémon
- 3 Contenido con derechos de autor
 - Libros electrónicos
 - Bandas sonoras
- 4 Servicios en línea
 - Multijugador
 - Contenidos descargables
- 5 Recomendaciones
- 6 Conclusiones

Índice de contenidos

- 1 **Introducción**
- 2 Traducciones no oficiales
 - Metodología
 - Saga Pokémon
- 3 Contenido con derechos de autor
 - Libros electrónicos
 - Bandas sonoras
- 4 Servicios en línea
 - Multijugador
 - Contenidos descargables
- 5 Recomendaciones
- 6 Conclusiones

Motivación

- Los videojuegos son una clave de nuestra cultura actual.
- Su industria es la segunda con más ganancias.
- Preocupación por protección anti-copias, derechos de autor, trampas.

The Gamer

34YRS

The average age of a gamer¹

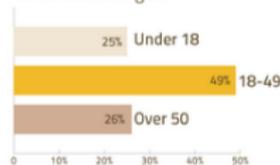
39YRS

The average age of most frequent game purchaser²

12YRS

Average number of years adult gamers have been playing computer/video games³

2010 Gamer Ages⁴



The 2010 average gamer spends 8 hours a week playing video games⁵

Figura: Estadísticas sobre jugadores en EE. UU. Fuente: <http://www.esrb.org> (2010).

Motivación

- Los videojuegos son una clave de nuestra cultura actual.
- Su industria es la segunda con más ganancias.
- Preocupación por protección anti-copias, derechos de autor, trampas.

The Industry

According to data compiled by the NPD Group, a global market research company, and released by the Entertainment Software Association, the computer and video game industry sold 273 million units in 2009 leading to an astounding

\$10.5
billion in revenue

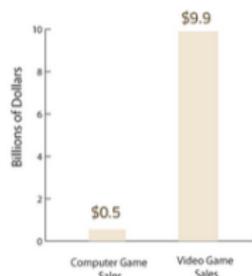


Figura: Estadísticas sobre la industria de videojuegos en EE. UU.
Fuente: <http://www.esrb.org> (2009).

Motivación

- Los videojuegos son una clave de nuestra cultura actual.
- Su industria es la segunda con más ganancias.
- Preocupación por protección anti-copias, derechos de autor, trampas.

The Industry

According to data compiled by the NPD Group, a global market research company, and released by the Entertainment Software Association, the computer and video game industry sold 273 million units in 2009 leading to an astounding

\$10.5
billion in revenue

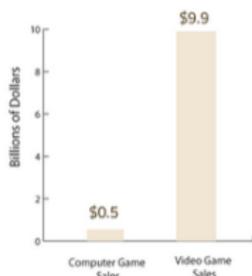


Figura: Estadísticas sobre la industria de videojuegos en EE. UU.
Fuente: <http://www.esrb.org> (2009).

ROM Hacking

Ingeniería inversa

La ingeniería inversa es el proceso de analizar un sistema para identificar sus componentes y relaciones y, crear una representación del sistema en otro formato o a un nivel más alto de abstracción.

ROM Hacking

Ingeniería inversa sobre videojuegos. El nombre viene realizar modificaciones (*hacks*) sobre juegos que suelen distribuirse en memorias de solo lectura (*Read Only Memory*).

ROM Hacking

Ingeniería inversa

La ingeniería inversa es el proceso de analizar un sistema para identificar sus componentes y relaciones y, crear una representación del sistema en otro formato o a un nivel más alto de abstracción.

ROM Hacking

Ingeniería inversa sobre videojuegos. El nombre viene realizar modificaciones (*hacks*) sobre juegos que suelen distribuirse en memorias de solo lectura (*Read Only Memory*).

Índice de contenidos

- 1 Introducción
- 2 Traducciones no oficiales
 - Metodología
 - Saga Pokémon
- 3 Contenido con derechos de autor
 - Libros electrónicos
 - Bandas sonoras
- 4 Servicios en línea
 - Multijugador
 - Contenidos descargables
- 5 Recomendaciones
- 6 Conclusiones

Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos ⇒ traducción no oficial.

Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos ⇒ traducción no oficial.



Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos ⇒ traducción no oficial.



Traducciones no oficiales y Pokémon

- Franquicia de *The Pokémon Company* fundada en 1995. Juegos desarrollados por *Game Freak*.
- Segunda franquicia más exitosa a nivel mundial.
- Nº seguidores + retrasos en lanzamientos ⇒ traducción no oficial.



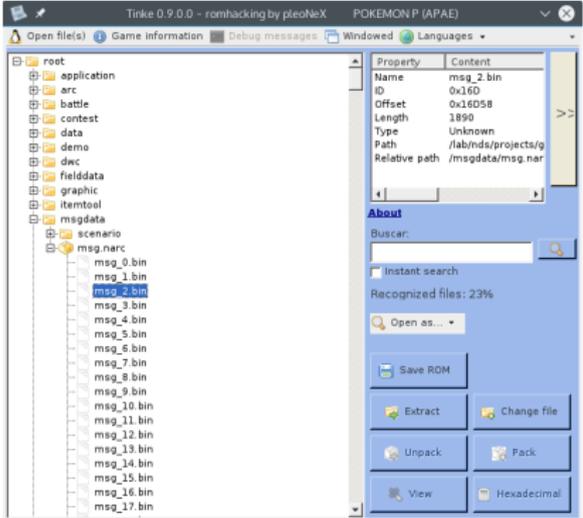
Ficheros en Nintendo DS

Sistema de ficheros en NDS.

Archivo binario con textos.

Ficheros en Nintendo DS

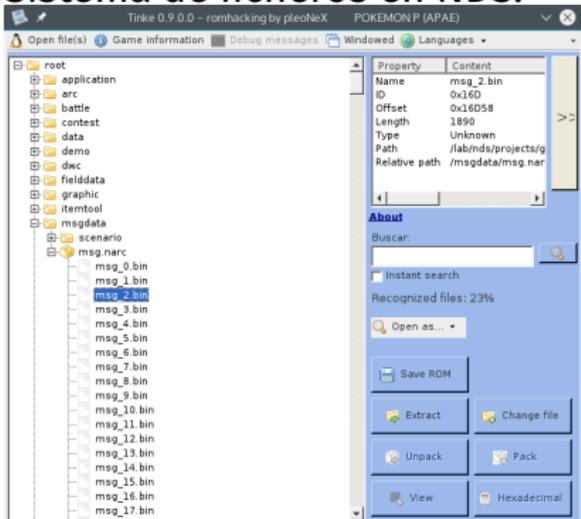
Sistema de ficheros en NDS.



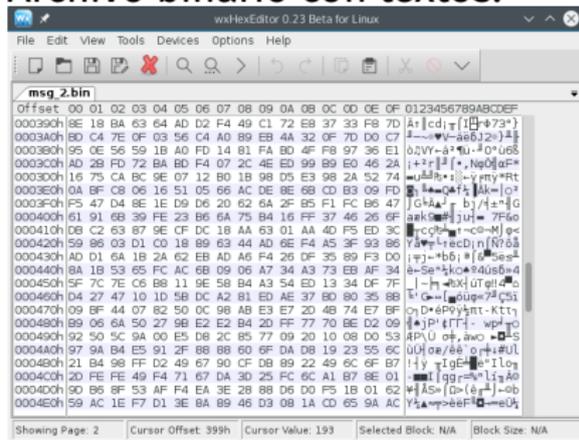
Archivo binario con textos.

Ficheros en Nintendo DS

Sistema de ficheros en NDS.



Archivo binario con textos.



Depuración de juegos

Emulador No\$gba para NDS.

Depuración de juegos

Emulador No\$gba para NDS.

The screenshot displays the No\$gba Debugger (Full Version) interface. The main window shows assembly code with columns for address, instruction, comment, and PC. A dialog box is open in the center with the text "¡Hola, hola! ¡Encantado de conocerte!". The bottom right shows a register window with values for r0 through r15 and cpsr.

Address	Instruction	Comment	PC
020CD854	E1D14ABA	ldch r4,[r1,#0xAA]	:3 3
020CD858	E1D10ABC	ldch r0,[r1,#0xAC]	:3 6
020CD85C	E1800804	orr r0,r0,r4,lsl #0x10	:1 7
020CD860	E5860018	str r0,[r6,#0x18]	:2 9
020CD864	E1D330B0	ldch r3,[r3]	:3 12
020CD868	E1D200B0	ldch r0,[r2]	:3 15
020CD86C	E1D119B8	ldch r1,[r1,#0x98]	:3 18
020CD870	E1830000	orr r0,r3,r0	:1 19
020CD874	E1800801	orr r0,r0,r1,lsl #0x10	:1 20
020CD878	E586001C	str r0,[r6,#0x1C]	:2 22
020CD87C	E28D0004	add r13,r13,#0x4	:1 23
020CD880	E8BD40F0	ldmfd r13!,{r4-r7,r14}	:2 25
020CD884	E12FFF1E	bx r14	:3 28
020CD888	04000006	strech r0,[0],-#0x6	:2 30
020CD88C	027FFC00	rshbeq r15,r15,#0x0	:3 33
020CD890	021D3954	andeqs r3,r13,#0x150000	:1 34
020CD894	04000600	strech r0,[0],-#0x600	:2 36
020CD898	04000130	strech r0,[0],-#0x130	:2 38
020CD89C	027FFF88	rshbeq r15,r15,#0x2A0	:3 41
020CD8A0	E3A00000	mov r0,#0x0	:1 42
020CD8A4	EE0270F90	ncr p15,0,r0,c7,c0,4 ;Wait For Interrupt	
020CD8A8	E12FFF1E	bx r14	:3 45
020CD8AC	E92D4000	stmfd r13!,{r14}	:1 46
020CD8B0	E24DD004	sub r13,r13,#0x4	:1 47
020CD8B4	EBFFF8AC	bl #0x20CD36C ;→	:3 50
020CD8B8	EBFFF8B4	bl #0x20CD8A0 ;→	:3 53
020CD8BC	EAF7FFF8	bl #0x20CD8B4 ;↑	:3 56
020CD8C0	E59F1004	ldr r1,-#0x4000247	:2 58
020CD8C4	E5C10000	strb r0,[r1]	:2 60
020CD8C8	E12FFF1E	bx r14	:3 63
020CD8CC	04000247	strech r0,[0],-#0x247	:2 65
020CD8D0	E92D4000	stmfd r13!,{r14}	:1 66
020CD8D4	E24DD004	sub r13,r13,#0x4	:1 67

Register	Value	n	Trace	Run/Next	GBA Specs	CPU Specs
r0	00000000	n				
r1	0000001F	z				
r2	00000000	c	Reload	Edit File	Screenshot	Upload
r3	00000000	v				
r4	00000000	i				
r5	00000000	f				
r6	00000000	t				
r7	00000000	l				
r8	00000000	q				
r9	00000000	C				
r10	00000000	P				
r11	00000000	F				
r12	00000000	U				
r13	021D3940					
r14	021DCAF4					
r15	020CD8A4					
cpsr	0000001F					

Búsqueda de textos con codificación no estándar

RelativeSearch.

Búsqueda de textos con codificación no estándar

RelativeSearch.

Found at: 00295826 2CFE6Bh 01 53 01 50 01 45 01 AD 01 DE 01 4C 01 53 01
 Found at: 00296052 2CFE7Ah 50 01 45 01 AB 01 00 E0 A9 01 2F 01 52 01 47
 Found at: 002CFE9E 2CFE89h 01 45 01 52 01 58 01 45 01 48 01 53 01 DE 01
 ----- 2CFE98h 48 01 49 01 DE 01 47 01 53 01 52 01 53 01 47
 [] 2CFEA7h 01 49 01 56 01 58 01 49 01 AB 01 BC 25 A9 01
 49 01 DE 01 48 01 53 01 5D 01 DE 01 50
 01 DE 01 46 01 4D 01 49 01 52 01 5A 01
 52 01 4D 01 48 01 45 01 DE 01 45 01 50
 01 51 01 59 01 52 01 48 01 53 01 00 E0
 49 01 DE 01 50 01 53 01 57 01 DE 01 3A
 01 4F 01 88 01 51 01 53 01 52 01 AB 01
 FF FF 44 55 00 80 50 00 00 00 A0 45 29
 46 29 02 5C 10 5C 10 5C 10 5C 10 5C 10
 52 10 5C 10 5C 10 5C 10 2C 46 29 02 5C
 0 98 46 29 02 5C 10 5C 10 04 47 29 02
 5C 10 70 47 29 02 40 10 40 10 DC 47 29
 0 40 10 48 48 29 02 40 10 40 10 B4 48

RelativeSearch

concerte

63 6F 6E 6F 63 65 72 74 65

Copy ASCII

Relative 2 Bytes

Puntos de interrupción en código

Punto de interrupción.

The screenshot displays the No\$gba Debugger interface. The main window shows assembly code with the following instructions and addresses:

Address	Instruction	Comment	PC
0200A6B8 4048	eor	r0,r1	:1 1
0200A6BA 9002	str	r0,[sp,#0x8]	:1 2
0200A6BC 9803	ldr	r0,[sp,#0xC]	:2 4
0200A6BE 4048	eor	r0,r1	:1 5
0200A6C0 0046	lsl	r6,r0,#0x1	:1 6
0200A6C2 9003	str	r0,[sp,#0xC]	:1 7
0200A6C4 1C20	mov	r0,r4	:1 8
0200A6C6 1C31	mov	r1,r6	:1 9
0200A6C8 F0CFAAC	bl	#0x2016A24	:4 13
0200A6CC 1C04	mov	r4,r0	:1 14
0200A6CE D02B	beq	#0x200A728	:3 17
0200A6D0 9400	str	r4,[sp]	:1 18
0200A6D2 9901	ldr	r1,[sp,#0x4]	:2 20
0200A6D4 9A02	ldr	r2,[sp,#0x8]	:2 22
0200A6D6 1C38	mov	r0,r7	:1 23
0200A6D8 1C33	mov	r3,r6	:1 24
0200A6DA F7CF99B	bl	#0x2006014	:4 28
0200A6DE 4A14	ldr	r2,#0x91BD3	:2 30
0200A6E0 1C6B	add	r3,r5,1	:1 31
0200A6E2 435A	mml	r2,r3	:2 33
0200A6E4 0412	lsl	r2,r2,#0x10	:1 34
0200A6E6 9803	ldr	r0,[sp,#0xC]	:2 36
0200A6E8 0C13	lsl	r3,r2,#0x10	:1 37
0200A6EA 1C21	mov	r1,r4	:1 38
0200A6EC 1E42	sub	r2,r0,1	:1 39
0200A6EE 2800	cmp	r0,#0x0	:1 40
0200A6F0 D00B	beq	#0x200A70A	:3 43
0200A6F2 4810	ldr	r0,#0x493D	:2 45
0200A6F4 9800	ldrh	r5,[r1]	:2 47
0200A6F6 405D	eor	r5,r3	:1 48
0200A6F8 900D	strh	r5,[r1]	:1 49
0200A6FA 181B	add	r3,r3,r0	:1 50
0200A6FC 041B	lsl	r3,r3,#0x10	:1 51
0200A6FE 1C15	mov	r5,r2	:1 52
0200A700 1C09	add	r1,r1,2	:1 53
0200A702 0C1B	lsl	r3,r3,#0x10	:1 54
0200A704 1E52	sub	r1,r2,1	:1 55
0200A706 2D00	cmp	r5,#0x0	:1 56
0200A708 D1F4	bne	#0x200A6F4	:3 59
0200A70A 980A	ldr	r0,[sp,#0x28]	:2 61

A breakpoint is set at address 022CF700, indicated by a red arrow and the text "<global memory change break> [022CF700]!". The right-hand side of the debugger shows the register window with the following values:

Register	Value
r0	0000493D
r1	022CF700
r2	0000001D
r3	0000212B
r4	022CFE90
r5	0000014D
r6	000000AC
r7	02294594
r8	00000000
r9	00000000
r10	00000000
r11	00000000
r12	020CA314
r13	027E3A98
r14	02006961
r15	0200A6FA
cpst	2000003F
apsr	00000000

Puntos de interrupción en código

Bucle de descifrado.

NoSgba Debugger (Fullversion)

File	Search	Run	Debug	Window	Utility	Options	Help
0200A6B8	4048	eor	r0,r1	:1	1		
0200A6BA	9002	str	r0,[sp,#0x8]	:1	2		
0200A6BC	9803	ldr	r0,[sp,#0xC]	:2	4		
0200A6BE	4048	eor	r0,r1	:1	5		
0200A6C0	0046	lsl	r6,r0,#0x1	:1	6		
0200A6C2	9003	str	r0,[sp,#0xC]	:1	7		
0200A6C4	1C20	mov	r0,r4	:1	8		
0200A6C6	1C31	mov	r1,r6	:1	9		
0200A6C8	F00CF9AC	bl	#0x2016A24	:>	4	13	
0200A6CC	1C04	mov	r4,r0		14		
0200A6CE	D02B	beq	#0x200A728	:↓	3	17	
0200A6D0	9400	str	r4,[sp]		18		
0200A6D2	9901	ldr	r1,[sp,#0x4]		20		
0200A6D4	9A02	ldr	r2,[sp,#0x8]		22		
0200A6D6	1C38	mov	r0,r7		23		
0200A6D8	1C33	mov	r3,r6		24		
0200A6DA	F7FCF89B	bl	#0x2006814	:>	4	28	
0200A6DE	4A14	ldr	r2,#0x91BD3		30		
0200A6E0	1C8B	sdd	r3,r5,1		31		
0200A6E2	435A	mll	r2,r3		32	33	
0200A6E4	0412	lsl	r2,r2,#0x10		34		
0200A6E6	9803	ldr	r0,[sp,#0xC]		36		
0200A6E8	0C13	lsl	r3,r2,#0x10		37		
0200A6EA	1C21	mov	r1,r4		38		
0200A6EC	1E42	sub	r2,r0,1		39		
0200A6EE	2800	cap	r0,#0x0		40		
0200A6F0	D0B8	beq	#0x200A70A	:↓	3	43	
0200A6F2	4810	ldr	r0,#0x483D		45		
0200A6F4	980D	lsl	r5,[r1]		47		
0200A6F6	405D	eor	r5,r3		48		
0200A6F8	800D	str	r5,[r1]		49		
0200A6FA	181B	add	r3,r3,r0		50		
0200A6FC	041B	lsl	r3,r3,#0x10		51		
0200A6FE	1C15	mov	r5,r2		52		
0200A700	1C89	add	r1,r1,2		53		
0200A702	0C1B	lsl	r3,r3,#0x10		54		
0200A704	1E52	sub	r2,r2,1		55		
0200A706	2D00	cap	r5,#0x0		56		
0200A708	D1F4	bne	#0x200A6F4	:↑	3	59	
0200A70A	980A	ldr	r0,[sp,#0x28]		61		

<global memory change break> [022CF700]!!!

r0	0000493D	n	Trace	Run Next	GBA Specs	CPU Specs
r1	022CF700	z	Reload	Edit File	Screenshot	Upload
r2	0000001D	c				
r3	0000212B	v				
r4	022CF730	y				
r5	0000014D	t				
r6	000000AC	f				
r7	02294504	q				
r8	00000000	u				
r9	00000000	p				
r10	00000000	C				
r11	00000000	U				
r12	020CA314					
r13	027E3A98					
r14	02006861					
r15	0200A6FA					
cpst	2000003F					
spst	00000000					

Puntos de interrupción en código

Inicialización de clave.

No\$gba Debugger (Fullversion)

File	Search	Run	Debug	Window	Utility	Options	Help
0200A6B8	4048	eor	r0,r1	:1	1		
0200A6BA	9002	str	r0,[sp,#0x8]	:1	2		
0200A6BC	9803	ldr	r0,[sp,#0xC]	:2	4		
0200A6BE	4048	eor	r0,r1	:1	5		
0200A6C0	0046	lsl	r6,r0,#0x1	:1	6		
0200A6C2	9003	str	r0,[sp,#0xC]	:1	7		
0200A6C4	1C20	mov	r0,r4	:1	8		
0200A6C6	1C31	mov	r1,r6	:1	9		
0200A6C8	F00CF9AC	bl	#0x2016A24	:>	4	13	
0200A6CC	1C04	mov	r4,r0		14		
0200A6CE	D02B	beq	#0x200A728	:↓	17		
0200A6D0	9400	str	r4,[sp]	:1	18		
0200A6D2	9901	ldr	r1,[sp,#0x4]	:2	20		
0200A6D4	9A02	ldr	r2,[sp,#0x8]	:2	22		
0200A6D6	1C38	mov	r0,r7	:1	23		
0200A6D8	1C33	mov	r3,r6	:1	24		
0200A6DA	F7CFB9B	bl	#0x2006014	:>	4	28	
0200A6DE	4A14	ldr	r2,#0x91BD3	:2	30		
0200A6E0	1C6B	add	r3,r5,1		31		
0200A6E2	435A	add	r2,r3	:2	33		
0200A6E4	0412	lsl	r2,r2,#0x10	:1	34		
0200A6E6	9803	ldr	r0,[sp,#0xC]	:2	36		
0200A6E8	0C13	lsl	r3,r2,#0x10	:1	37		
0200A6EA	1C21	mov	r1,r4	:1	38		
0200A6EC	1E42	sub	r2,r0,1	:1	39		
0200A6EE	2800	cap	r0,#0x0	:1	40		
0200A6F0	D0B8	beq	#0x200A70A	:↓	43		
0200A6F2	4810	ldr	r0,#0x493D	:2	45		
0200A6F4	980D	ldrh	r5,[r1]	:2	47		
0200A6F6	405D	eor	r5,r3	:1	48		
0200A6F8	800D	strh	r5,[r1]	:1	49		
0200A6FA	181B	add	r3,r3,r0	:1	50		
0200A6FC	041B	lsl	r3,r3,#0x10	:1	51		
0200A6FE	1C15	mov	r5,r2	:1	52		
0200A700	1C89	add	r1,r1,2	:1	53		
0200A702	0C1B	lsl	r3,r3,#0x10	:1	54		
0200A704	1E52	sub	r2,r2,1	:1	55		
0200A706	2D00	cap	r5,#0x0	:1	56		
0200A708	D1F4	bne	#0x200A6F4	:↑	59		
0200A70A	980A	ldr	r0,[sp,#0x28]	:2	61		

<global memory change break> [022CF700]!!!

r0	0000493D	n	Trace	Run Next	GBA Specs	CPU Specs
r1	022CF700	z	Reload	Edit File	Screenshot	Upload
r2	0000001D	c				
r3	0000212B	v				
r4	022CF730	w				
r5	0000014D	t				
r6	000000AC	f				
r7	02294504	d				
r8	00000000	q				
r9	00000000	u				
r10	00000000	p				
r11	00000000	C				
r12	020CA314					
r13	027E3A98					
r14	02006861					
r15	0200A6FA					
cpst	2000003F					
spst	00000000					

Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);  
for (int i=0; i<data.Length; i++){  
    data[i] = data[i] ^ clave;  
    clave = (ushort)(clave + 0x493D);  
}
```

Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];  
for (int i=data.Length - 1; i>=0; i--){  
    data[i] = data[i] ^ clave;  
    clave = (uint)(clave * 0x41C64E6D + 0x6073);  
}
```

Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    clave = (ushort)(clave + 0x493D);
}
```

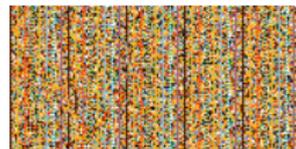
Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
    data[i] = data[i] ^ clave;
    clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```

Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    clave = (ushort)(clave + 0x493D);
}
```



Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
    data[i] = data[i] ^ clave;
    clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```

Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    clave = (ushort)(clave + 0x493D);
}
```



Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];
for (int i=data.Length - 1; i>=0; i--){
    data[i] = data[i] ^ clave;
    clave = (uint)(clave * 0x41C64E6D + 0x6073);
}
```

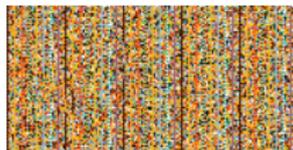
Cifrado XOR en Pokémon Perla y Diamante

Textos: codificados y cifrados

```
ushort clave = 0x91BD3 * (num + 1);  
for (int i=0; i<data.Length; i++){  
    data[i] = data[i] ^ clave;  
    clave = (ushort)(clave + 0x493D);  
}
```

Imágenes: cifrado del bloque de datos

```
uint clave = data[data.Length - 1];  
for (int i=data.Length - 1; i>=0; i--){  
    data[i] = data[i] ^ clave;  
    clave = (uint)(clave * 0x41C64E6D + 0x6073);  
}
```



Archivos ofuscados en Pokémon Blanco y Negro

- Archivos ofuscados:
 - Sin nombre ni clasificación.
- Textos:
 - Codificación UTF-16.
 - Cifrado XOR, moviendo 3 bits de la clave.

```

ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    ushort temp = clave & 0x1FFF;
    clave = (temp<<3) | (clave>>13)
}

```

- Imágenes:
 - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro



- Archivos ofuscados:

- Sin nombre ni clasificación.

- Textos:

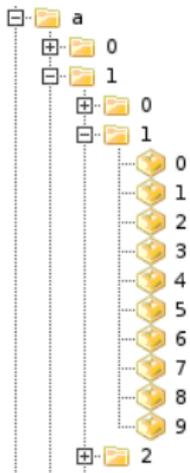
- Codificación UTF-16.
- Cifrado XOR, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;  
for (int i=0; i<data.Length; i++){  
    data[i] = data[i] ^ clave;  
    ushort temp = clave & 0x1FFF;  
    clave = (temp<<3) | (clave>>13)  
}
```

- Imágenes:

- Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro



- Archivos ofuscados:
 - Sin nombre ni clasificación.

- Textos:

- Codificación UTF-16.
- Cifrado XOR, moviendo 3 bits de la clave.

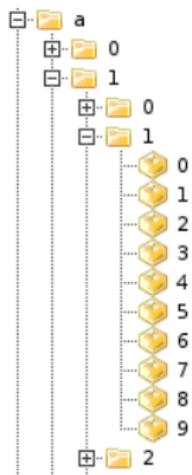
```

ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    ushort temp = clave & 0x1FFF;
    clave = (temp<<3) | (clave>>13)
}
  
```

- Imágenes:

- Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro



- Archivos ofuscados:

- Sin nombre ni clasificación.

- Textos:

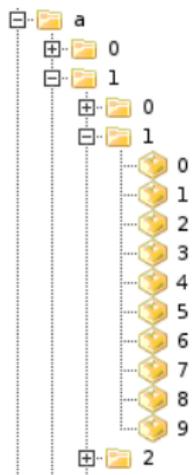
- Codificación UTF-16.
- Cifrado XOR, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;  
for (int i=0; i<data.Length; i++){  
    data[i] = data[i] ^ clave;  
    ushort temp = clave & 0x1FFF;  
    clave = (temp<<3) | (clave>>13)  
}
```

- Imágenes:

- Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro

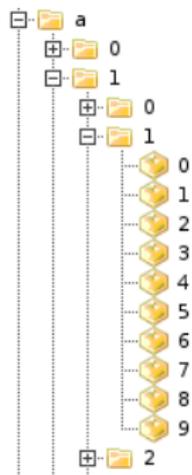


- Archivos ofuscados:
 - Sin nombre ni clasificación.
- Textos:
 - Codificación UTF-16.
 - Cifrado XOR, moviendo 3 bits de la clave.

```
ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    ushort temp = clave & 0x1FFF;
    clave = (temp<<3) | (clave>>13)
}
```

- Imágenes:
 - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro



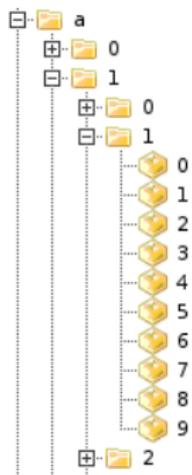
- Archivos ofuscados:
 - Sin nombre ni clasificación.
- Textos:
 - Codificación UTF-16.
 - Cifrado XOR, moviendo 3 bits de la clave.

```

ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    ushort temp = clave & 0x1FFF;
    clave = (temp<<3) | (clave>>13)
}
  
```

- Imágenes:
 - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro



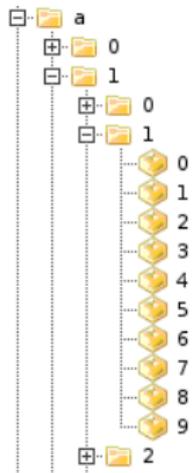
- Archivos ofuscados:
 - Sin nombre ni clasificación.
- Textos:
 - Codificación UTF-16.
 - Cifrado XOR, moviendo 3 bits de la clave.

```

ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    ushort temp = clave & 0x1FFF;
    clave = (temp<<3) | (clave>>13)
}
  
```

- Imágenes:
 - Cambio de formato.

Archivos ofuscados en Pokémon Blanco y Negro



- Archivos ofuscados:
 - Sin nombre ni clasificación.
- Textos:
 - Codificación UTF-16.
 - Cifrado XOR, moviendo 3 bits de la clave.

```

ushort clave = (num + 3) * 0x2983;
for (int i=0; i<data.Length; i++){
    data[i] = data[i] ^ clave;
    ushort temp = clave & 0x1FFF;
    clave = (temp<<3) | (clave>>13)
}
  
```

- Imágenes:
 - Cambio de formato.



Mecanismos en otros juegos

Algoritmos de protección encontrados en otros juegos:

- *Pokémon HeartGold y SoulSilver*: Igual que *Pokémon Perla y Diamante*.
- *Pokémon Conquest*: Cifra y codifica textos. Imágenes con formatos no estándar.
- *Ninokuni - El Mago de las Tinieblas*: Cifra estadísticas de personajes y monstruos. Añade algoritmos de integridad en el archivo de guardado.

Mecanismos en otros juegos

Algoritmos de protección encontrados en otros juegos:

- *Pokémon HeartGold y SoulSilver*: Igual que *Pokémon Perla y Diamante*.
- *Pokémon Conquest*: Cifra y codifica textos. Imágenes con formatos no estándar.
- *Ninokuni - El Mago de las Tinieblas*: Cifra estadísticas de personajes y monstruos. Añade algoritmos de integridad en el archivo de guardado.

Mecanismos en otros juegos

Algoritmos de protección encontrados en otros juegos:

- *Pokémon HeartGold y SoulSilver*: Igual que *Pokémon Perla y Diamante*.
- *Pokémon Conquest*: Cifra y codifica textos. Imágenes con formatos no estándar.
- *Ninokuni - El Mago de las Tinieblas*: Cifra estadísticas de personajes y monstruos. Añade algoritmos de integridad en el archivo de guardado.

Índice de contenidos

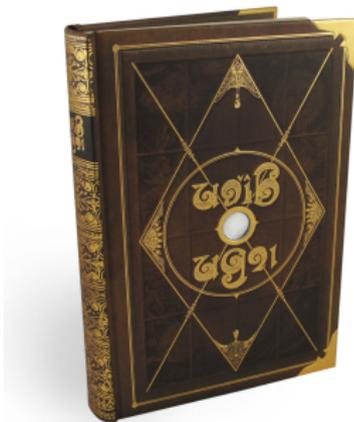
- 1 Introducción
- 2 Traducciones no oficiales
 - Metodología
 - Saga Pokémon
- 3 Contenido con derechos de autor**
 - Libros electrónicos
 - Bandas sonoras
- 4 Servicios en línea
 - Multijugador
 - Contenidos descargables
- 5 Recomendaciones
- 6 Conclusiones

Ninokuni: La ira de la Bruja Blanca

- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
 - El resto de ficheros (texto, audio, etc) sí están cifrados.

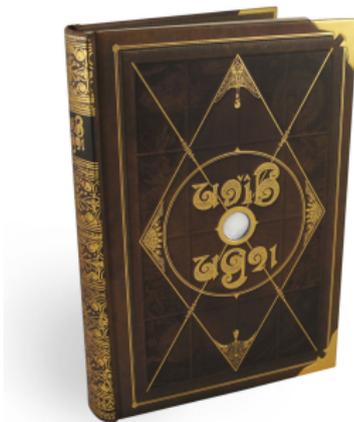
Ninokuni: La ira de la Bruja Blanca

- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
 - El resto de ficheros (texto, audio, etc) sí están cifrados.



Ninokuni: La ira de la Bruja Blanca

- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
 - El resto de ficheros (texto, audio, etc) sí están cifrados.



Ninokuni: La ira de la Bruja Blanca

- Versión para PS3 con ligeros cambios. Llegó a América y Europa.
- Libro digitalizado en alta calidad.
- No hay algoritmos de protección, pero su formato no es estándar.
 - El resto de ficheros (texto, audio, etc) sí están cifrados.



Guitar Hero: On Tour



- **Ficheros comprimidos con formato propietario. ✓**
 - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: Vorbis OGG. ✗

Guitar Hero: On Tour



- Archivos comprimidos con formato propietario. ✓
 - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: Vorbis OGG. ✗

```
LDR    R1, =aInvalidWindowS      ; "invalid window size"
MOV    R0, #0x1B
STR    R1, [R9,#0x18]
STR    R0, [R8]
```

Figura: Mensajes de error en el código. ✗

Guitar Hero: On Tour



- Ficheros comprimidos con formato propietario. ✓
 - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: Vorbis OGG. ✗

```
LDR    R1, =aInvalidWindowS      ; "invalid window size"
MOV    R0, #0x1B
STR    R1, [R9,#0x18]
STR    R0, [R8]
```

Figura: Mensajes de error en el código. ✗

Guitar Hero: On Tour



- Ficheros comprimidos con formato propietario. ✓
 - El algoritmo ocupa 1.900 instrucciones máquina. ✓
- No hay compresión en las siguientes ediciones. ✗
- Formato canciones: Vorbis OGG. ✗

```
LDR    R1, =aInvalidWindowS      ; "invalid window size"
MOV    R0, #0x1B
STR    R1, [R9,#0x18]
STR    R0, [R8]
```

Figura: Mensajes de error en el código. ✗

Duet



- Juego para plataformas móviles (Android, iOS).
- La banda sonora se vende en iTunes por 3.99€.
- Se encuentra desprotegida en la carpeta del juego en formato estándar.

Duet

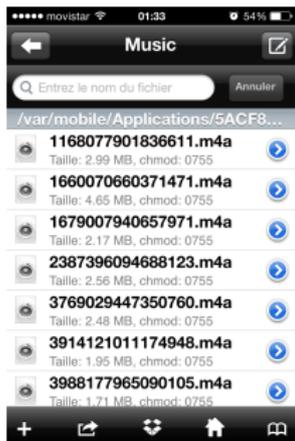


- Juego para plataformas móviles (Android, iOS).
- La banda sonora se vende en iTunes por 3.99€.
- Se encuentra desprotegida en la carpeta del juego en formato estándar.

Duet



- Juego para plataformas móviles (Android, iOS).
- La banda sonora se vende en iTunes por 3.99€.
- Se encuentra desprotegida en la carpeta del juego en formato estándar.



Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en e-books. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en e-books. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en e-books. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en e-books. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en e-books. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Mecanismos en otros juegos

Información en otros juegos estudiados:

- *100 Classic Book Collection*: Sin protección en e-books. ✗
- *Elite Beat Agents*: Sin protección en canciones. ✗
- *Guitar Rock*: Sin protección en canciones. ✗
- Música de juegos de Level-5: Codificación propietaria. ✓
- Vídeos de *Ninokuni* para PS3: Codificación MPEG. ✗
- Vídeos en NDS: Codificación propietaria desconocida. ✓

Índice de contenidos

- 1 Introducción
- 2 Traducciones no oficiales
 - Metodología
 - Saga Pokémon
- 3 Contenido con derechos de autor
 - Libros electrónicos
 - Bandas sonoras
- 4 Servicios en línea**
 - **Multijugador**
 - **Contenidos descargables**
- 5 Recomendaciones
- 6 Conclusiones

Captura de paquetes

Estrategia *man-in-the-middle*

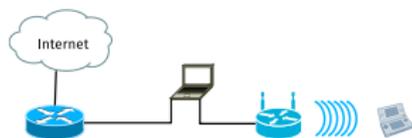


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet, u32 len);
void save_adhocPacket(u8* packet,
    u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

HandleDebugEvent_Execute() en
debug.cpp.

Captura de paquetes

Estrategia *man-in-the-middle*



Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet, u32 len);
void save_adhocPacket(u8* packet,
    u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

HandleDebugEvent_Execute() en
debug.cpp.

Captura de paquetes

Estrategia *man-in-the-middle*



Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet, u32 len);
void save_adhocPacket(u8* packet,
    u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

HandleDebugEvent_Execute() en
debug.cpp.

Captura de paquetes

Estrategia *man-in-the-middle*



Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet, u32 len);
void save_adhocPacket(u8* packet,
    u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

HandleDebugEvent_Execute() en
debug.cpp.

Captura de paquetes

Estrategia *man-in-the-middle*

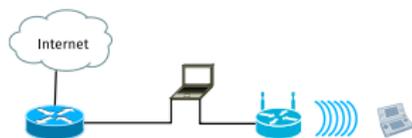


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet, u32 len);
void save_adhocPacket(u8* packet,
    u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

HandleDebugEvent_Execute() en
debug.cpp.

Captura de paquetes

Estrategia *man-in-the-middle*

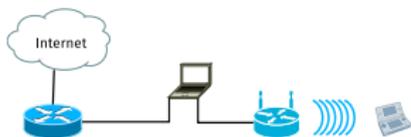


Figura:
Man-in-the-middle

Modificación DeSmuME.

- Paquetes PCAP.

```
void create_packet();
void save_packet(u8* packet, u32 len);
void save_adhocPacket(u8* packet,
    u32 len, void* addr, bool isSent);
```

- Exportar paquetes.

HandleDebugEvent_Execute() en
debug.cpp.

```
Reading: /store/Juegos/NDS/Ninokuni [CLEAN].nds
Found in Overlay9_2.bin at 0x020986B8
Press Enter to continue.
-----
```

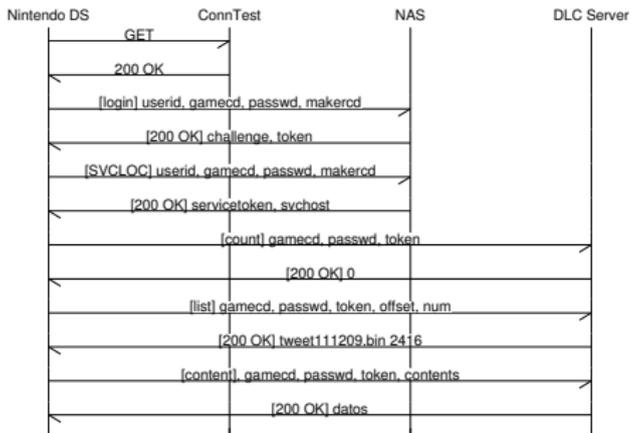
Figura: *RC4Finder*.

Servidores para Nintendo DS

Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

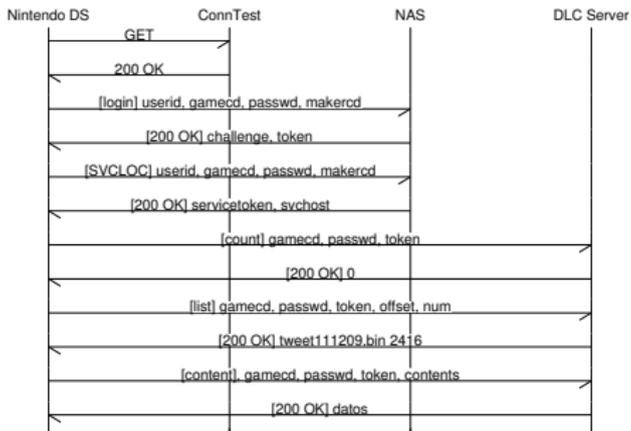
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

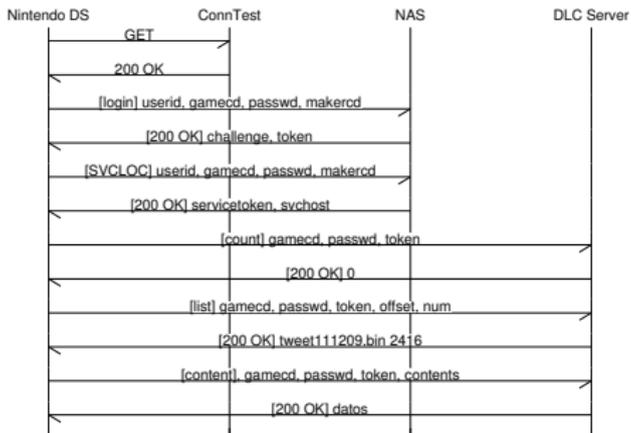
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

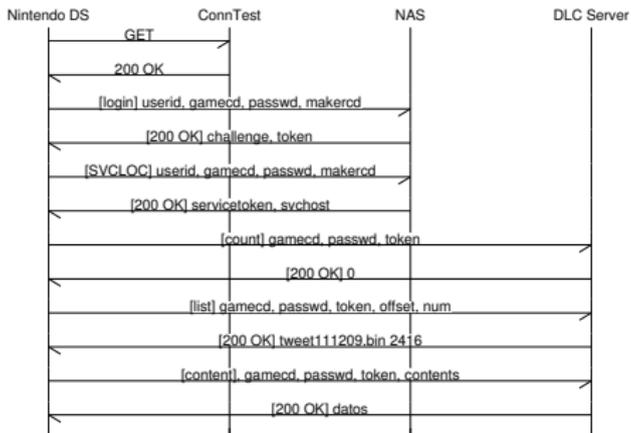
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

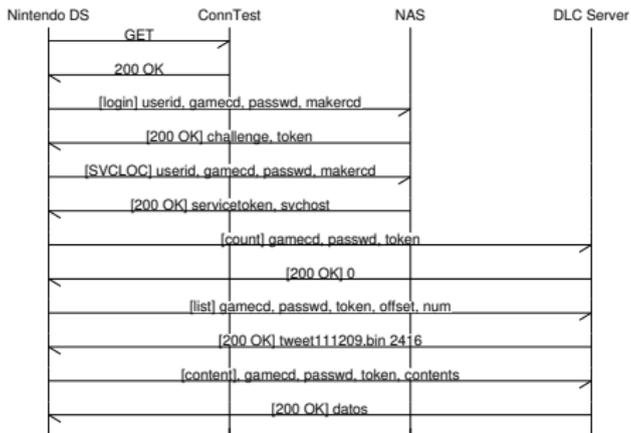
Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

Servidores para Nintendo DS



Vulnerabilidades:

- Puerto 80 del NAS abierto.
- Contraseña no usada.
- Autenticación simple.

Preguntados



Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

Preguntados



Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

Preguntados



Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

Preguntados



Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

```
{*id*:4980,*category*:"HISTORY",*text*:"..C..mo se denominaba en la Edad Media al hijo  
tenido fuera del matrimonio?","answers":  
[*Fogardo*,"Bastardo","Hu..rfano","Primog..nito"],*correct_answer*:1,*media_type*:"NORMAL  
"},{*question*:{*id*:4004,*category*:"GEOGRAPHY",*text*:"..Qu.. colores tiene la bandera  
de M..xico?","answers":["Azul, amarillo y rojo","Azul, verde y rojo*,"Blanco, verde y  
rojo*,"Amarillo, verde y  
rojo*],*correct_answer*:2,*media_type*:"NORMAL"},*powerup_question*:
```

Figura: Preguntas, respuesta y solución de una partida

Preguntados



Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

```
{*id*:4980,"category":"HISTORY","text":"..C..mo se denominaba en la Edad Media al hijo  
tenido fuera del matrimonio?","answers":  
[*Fogardo","Bastardo","Hu..rfano","Primog..nito"],*correct_answer*:1,"media_type":"NORMAL  
"},{*question":{"id":4004,"category":"GEOGRAPHY","text":"..Qu.. colores tiene la bandera  
de M..xico?","answers":["Azul, amarillo y rojo","Azul, verde y rojo","Blanco, verde y  
rojo","Amarillo, verde y  
rojo"],*correct_answer*:2,"media_type":"NORMAL"},"powerup_question":
```

Figura: Preguntas, respuesta y solución de una partida

Preguntados



Trivial para plataformas móviles.

Vulnerabilidades:

- Comunicación HTTP.
- Solución enviada antes de preguntar.

```
{*id*:4980,"category":"HISTORY","text":"..C..mo se denominaba en la Edad Media al hijo  
tenido fuera del matrimonio?","answers":  
["Fogardo","Bastardo","Hu..rfano","Primog..nito"],"correct_answer":1,"media_type":"NORMAL  
"},{"question":{"id":4004,"category":"GEOGRAPHY","text":"..Qu.. colores tiene la bandera  
de M..xico?","answers":["Azul, amarillo y rojo","Azul, verde y rojo","Blanco, verde y  
rojo","Amarillo, verde y  
rojo"],"correct_answer":2,"media_type":"NORMAL"},"powerup_question":
```

Figura: Preguntas, respuesta y solución de una partida

Duet



- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet



- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet



- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet



- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

Duet



- Niveles extras por 0,99€.
- BD con preferencias sin proteger.
- Ya incluidos pero desactivados.
- Se puede activar a mano.

306	TFPremiumUnlocked	0	12	1
307	TFEncoreUnlocked	0	12	1

Figura: Filas con estado de los contenidos extras

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Download Play

Compartir demos con comunicación inalámbrica ad-hoc.

Problema:

- Envío de código de una consola a otra.
- El código principales se firman con RSA.

Solución de Nintendo:

- Comprobar integridad con HMAC.
- Solo si con *Download Play*.

Índice de contenidos

- 1 Introducción
- 2 Traducciones no oficiales
 - Metodología
 - Saga Pokémon
- 3 Contenido con derechos de autor
 - Libros electrónicos
 - Bandas sonoras
- 4 Servicios en línea
 - Multijugador
 - Contenidos descargables
- 5 Recomendaciones**
- 6 Conclusiones

Seguridad en ficheros

- **Empaquetar ficheros.**
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en ficheros

- Empaquetar ficheros.
 - Implementaciones largas (1.900 líneas).
 - Compresión diferente en cada cabecera.
- Ofuscar nombre de ficheros y directorios.
- Cifrado XOR.
 - No usar claves estáticas.
- Codificación de caracteres no estándar.
 - Desordenar caracteres.
 - Cifrado del archivo de tipografía.
- Nuevos formatos frente a cifrado.

Seguridad en comunicaciones

- **HTTPS vs HTTP.**
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- **HTTPS vs HTTP.**
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- **HTTPS vs HTTP.**
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Seguridad en comunicaciones

- HTTPS vs HTTP.
 - Cerrar puertos de servidores.
 - Diseño del protocolo.
- Autenticación con contraseña vs reto.
 - Comprobar la contraseña.
- Cifrado y comprobación de integridad en descargas.
 - Proteger activación de contenido descargado.
- Transmisión segura de código entre dispositivos.

Índice de contenidos

- 1 Introducción
- 2 Traducciones no oficiales
 - Metodología
 - Saga Pokémon
- 3 Contenido con derechos de autor
 - Libros electrónicos
 - Bandas sonoras
- 4 Servicios en línea
 - Multijugador
 - Contenidos descargables
- 5 Recomendaciones
- 6 Conclusiones

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender \LaTeX .

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender \LaTeX .

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender \LaTeX .

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender \LaTeX .

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender \LaTeX .

Conclusiones

Objetivos alcanzados:

- Identificar problemas no tratados en la literatura.
- Desarrollar software.
- Aprender conceptos de bajo nivel en software y hardware incluyendo el lenguaje ensamblador ARM.
- Diseñar metodologías de ingeniería inversa y captura de paquetes.
- Analizar 21 juegos.
- Aprender \LaTeX .

Trabajo futuro

● Estudios:

- Seguridad en videoconsolas y sus *exploits*.
- Algoritmos de integridad en archivos de guardado.
- Mecanismos anti-copia físicos y digitales.
- Protocolos de micropagos en videojuegos.
- Seguridad de aplicaciones de ordenador (*Steam*).

● Desarrollos:

- Implementar mecanismos estudiados.
- Explorador de juegos avanzado.
- Depurador de código remoto.

Trabajo futuro

- Estudios:

- Seguridad en videoconsolas y sus *exploits*.
- Algoritmos de integridad en archivos de guardado.
- Mecanismos anti-copia físicos y digitales.
- Protocolos de micropagos en videojuegos.
- Seguridad de aplicaciones de ordenador (*Steam*).

- Desarrollos:

- Implementar mecanismos estudiados.
- Explorador de juegos avanzado.
- Depurador de código remoto.

Trabajo futuro

- Estudios:

- Seguridad en videoconsolas y sus *exploits*.
- Algoritmos de integridad en archivos de guardado.
- Mecanismos anti-copia físicos y digitales.
- Protocolos de micropagos en videojuegos.
- Seguridad de aplicaciones de ordenador (*Steam*).

- Desarrollos:

- Implementar mecanismos estudiados.
- Explorador de juegos avanzado.
- Depurador de código remoto.

Trabajo futuro

- Estudios:

- Seguridad en videoconsolas y sus *exploits*.
- Algoritmos de integridad en archivos de guardado.
- Mecanismos anti-copia físicos y digitales.
- Protocolos de micropagos en videojuegos.
- Seguridad de aplicaciones de ordenador (*Steam*).

- Desarrollos:

- Implementar mecanismos estudiados.
- Explorador de juegos avanzado.
- Depurador de código remoto.

Trabajo futuro

● Estudios:

- Seguridad en videoconsolas y sus *exploits*.
- Algoritmos de integridad en archivos de guardado.
- Mecanismos anti-copia físicos y digitales.
- Protocolos de micropagos en videojuegos.
- Seguridad de aplicaciones de ordenador (*Steam*).

● Desarrollos:

- Implementar mecanismos estudiados.
- Explorador de juegos avanzado.
- Depurador de código remoto.

Trabajo futuro

- Estudios:

- Seguridad en videoconsolas y sus *exploits*.
- Algoritmos de integridad en archivos de guardado.
- Mecanismos anti-copia físicos y digitales.
- Protocolos de micropagos en videojuegos.
- Seguridad de aplicaciones de ordenador (*Steam*).

- Desarrollos:

- Implementar mecanismos estudiados.
- Explorador de juegos avanzado.
- Depurador de código remoto.

Trabajo futuro

- Estudios:
 - Seguridad en videoconsolas y sus *exploits*.
 - Algoritmos de integridad en archivos de guardado.
 - Mecanismos anti-copia físicos y digitales.
 - Protocolos de micropagos en videojuegos.
 - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
 - Implementar mecanismos estudiados.
 - Explorador de juegos avanzado.
 - Depurador de código remoto.

Trabajo futuro

- Estudios:
 - Seguridad en videoconsolas y sus *exploits*.
 - Algoritmos de integridad en archivos de guardado.
 - Mecanismos anti-copia físicos y digitales.
 - Protocolos de micropagos en videojuegos.
 - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
 - Implementar mecanismos estudiados.
 - Explorador de juegos avanzado.
 - Depurador de código remoto.

Trabajo futuro

- Estudios:
 - Seguridad en videoconsolas y sus *exploits*.
 - Algoritmos de integridad en archivos de guardado.
 - Mecanismos anti-copia físicos y digitales.
 - Protocolos de micropagos en videojuegos.
 - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
 - Implementar mecanismos estudiados.
 - Explorador de juegos avanzado.
 - Depurador de código remoto.

Trabajo futuro

- Estudios:
 - Seguridad en videoconsolas y sus *exploits*.
 - Algoritmos de integridad en archivos de guardado.
 - Mecanismos anti-copia físicos y digitales.
 - Protocolos de micropagos en videojuegos.
 - Seguridad de aplicaciones de ordenador (*Steam*).
- Desarrollos:
 - Implementar mecanismos estudiados.
 - Explorador de juegos avanzado.
 - Depurador de código remoto.

Gracias por su atención

Repositorio en GitHub: <https://github.com/pleonex/AiroRom>

Índice de contenidos

7 Apéndice

- Metodología
- Traducciones no oficiales
- Contenidos con derechos de autor
- Servicios en línea

7 Apéndice

- Metodología
- Traducciones no oficiales
- Contenidos con derechos de autor
- Servicios en línea

Andrew Huang - Hacking the Xbox. An introduction to Reverse Engineering

In general, I hack because it is quite satisfying to know that somebody's life was made better by something I built. I feel it is my obligation to apply my talents and return to society what it has given me. I also enjoy the challenge of exploration. I want to understand electronics as deeply as I can. Black boxes frustrate me; nothing gets my curiosity going more than a box that I'm not allowed to open or understand. As a result, I have a fiduciary interest in cryptography and security methods.

Averiguar codificación desde tipografía

Pokémon Perla y Diamante

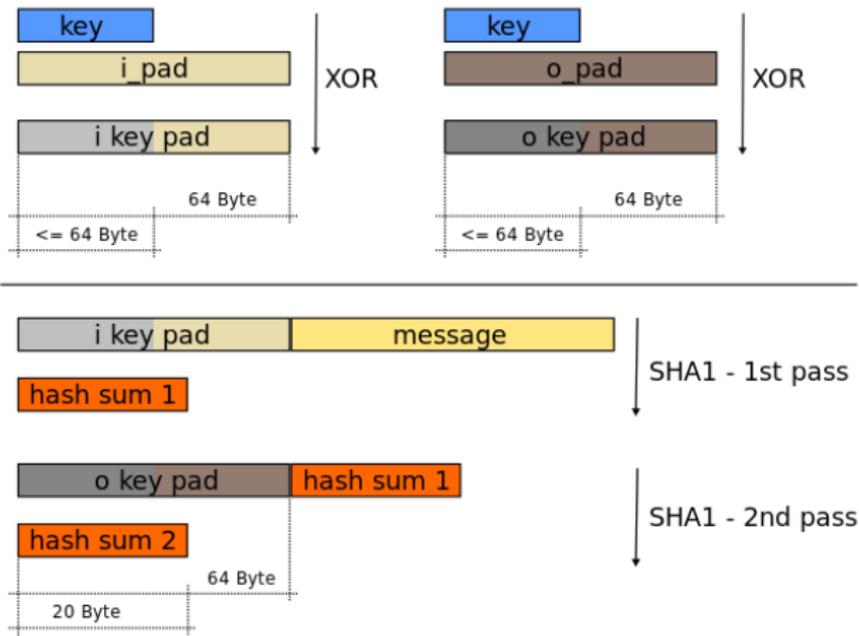
Ninokuni: El Mago de las Tinieblas

100 Classic Book Collection

Elite Beat Agents

Guitar Rock

HMAC



Servidores de Nintendo

Token generando aplicando MD5 a:

- MD5 del *challenge*_{NAS}.
- *challenge*_{consola}.
- 48 espacios en blanco.
- *challenge*_{servidor}.
- *token*_{NAS}.
- MD5 del *challenge*_{NAS}.

100 Classic Book Collection

Ninokuni: El Mago de las Tinieblas