Key file confirmation

This command checks the key file.

It's like checking the contents and checking if the password is correct.

10:57			0000	?
	Pass	word I	Maker	
Making Pas	sword			
with Key	file			
	2	2 Keyword	I	
	File	e & Keywc	ord	
		2 File		
Keyfile U	tility			
	Cre	eating Key	file	
	Con	firming Ke	yfile	
	1		2	
<i>S</i> Pwd		Text		Guide
			_	

When you press the main "Confirming Keyfile" button, you will see the following view.

10:57	••	• • • •
	Password Maker	
Confirmin	g Keyfile	
Keyfile F	ïlename	
select		clear
Passwor	d (for decrypting Keyfile)	
input		clear
Content		
		clear
	Do Confirming Content	
n		

The user interface looks like this.

- Key file name
- Key file decryption password
- Contents value

The meaning is like this.



If you press the "Select" button at the bottom left of the text view of the key file file name, a table view like the one on the left will appear.

Select the file and press the "Decide" button on the toolbar to return.

10:58		÷ 🔲
	Password Maker	
Confirmin	g Keyfile	
Keyfile F	ilename	
Keyfile.k	кеу	
select		clear
Passwor	d (for decrypting Keyfile)	
input		clear
Content		
		clear
	Do Confirming Content	
^		

When you come back, it will be like this.



If you press the "Input" button at the bottom left of the text view for displaying the password, the view for entering the password as shown in the figure on the left will appear.



Enter the password and press the "Decide" button on the toolbar to return.

10:59		
	Password Maker	
Confirmin	g Keyfile	
Keyfile F	ilename	
Keyfile.k	key	
select		clear
Passwor	rd (for decrypting Keyfile)	
Aaaa		
input		clear
Content AAAAA AAAAAA	4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	AAAAA AAAAA
		clear
	Do Confirming Content	
^		

After entering the file name and password of the key file, press the "Do Confirming Content" button to display the values stored in the key file like this.

10:59				🔶 🔲
	F	asswo	ord Mał	ker
Confirming	g Ke	yfile		
Keyfile F Keyfile.k	ilena key	ime		
select				clear
Passwor	d (fo	r decryptir	ng Keyfile)	
Aaaa				
input				clear
Contont	су	Look Up	Translate	Share
	4AA/ 4AA/	\AAAAAA \AAAAAA	АААААААА АААААААА	АААААААА ААААААААА
				clear
	Do	o Confirr	ning Cont	ent
ŵ				

You can copy the displayed value this way.

11:00		(?
	Password Maker	
Confirmin	g Keyfile	
Keyfile F	ïlename	
Keyfile.	(ey	
select		clear
Passwor	d (for decrypting Keyfile)	
Aaaa		
input		clear
Content	~~~~~	
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	AAAAA
		clear
	Do Confirming Content	
<b>^</b>		

If you press the "Do Confirming Content" button and the value of the contents is displayed like this, then it can be said that

the password used for encryption is "Aaaa", and

the encrypted file Keyfile.key has not been tampered with.

In the following cases, the value of the contents will not be displayed:

The password used for decryption is incorrect.

The encryption file Keyfile.key has been tampered with.

😹 Stirling	- [Key	file.ke	ey]											_ 🗆 🗙
🏘 ファイル(E)	_ 編集(E)	)検索	・移動(	5) 設	定(2)	- Ż7	いと	ל <u>ש</u> יל	) /	~ルフ	°Ш			_ 8 ×
	$\circ \circ$	XB	R 🔈	) <b>=</b> [	M 😫	<b>849</b>	<b>#41</b>	en A→B	Ŗ	9				۹
ADDRESS	00 01	02 03	04 05	06 0	7 08	09	0A	0B	0C	0D	0E	0F	0123456789/	ABCDEF
00000000	0B 1E	A1 8B	A8 C2	F0 D	7 49	8B	A1	0F	05	65	44	35	<u>.</u> 卿ソ・I僑	šeD5
00000010	66 08	3F 8A	CO 6F	9F 3	F 67	B8	E5	98	C1	91	F8	53	_f.?澗o.?g舛	蝌甜S
00000020	54 29	1D A1	8B CA	9F 1	F OB	B6	18	3D	4C	90	7E	B2	T).。玉カ	.北厨イ
00000030	4C 73	26, 57	F5 BE	7E 4	0 A8	D8	C7	35	50	0F	АE	07	Ls,₩•~@ィリシ	⊼5P.∍.
00000040	D8 E	26 BE	5F 25	-13 C	7 28	86	76	8A	FB	06	4B	E3	ש.&t_%.⊼(•	棋.K羈
00000050	B1 B3	C8 EA	FC 05	C6 7	3 9A	CF	3E	BC	DA	C4	CO	D1		>シレトタム
00000060	44 4E	B0 71	22 1F	39-8	F 95	1B	77	CE	6F	F9	81	B1	DN-q″.9助.v	wto•7
00000070	CC 7B	25 44	AF 92	FE 8	B C3	ΕA	B3	D3	62	67	A3	70	7{%Dッ凝・	<del>t</del> bg_p
00000080	43 54	D9 19											CTル.	
ν <del>τ</del> °r							0x0	0000	000				上書 132 Bytes	s <i>li</i> ,

The contents of the file Keyfile.key used in this example are like this.

😹 Stirling	- [Key	file.k	ey]												_	
📑 ファイル(E)	編集(E	)検索	や 移り	動( <u>S</u> )	設定	20	- Ċ7	가*	<u>う(W</u>	0 1	<b>い</b> ルフ	°Ш			_	B×
	$\circ \circ$	<u></u> %	E	⊳()≡	<b>#</b> \$	ŧ	<b>#4</b>	<b>#41</b>	A→B	ŗŗ	9				°t /	۱
ADDRESS	00 01	02 03	04	05 06	-07	80	09	OA	0B	00	0D	0E	0F	01234567	89ABCE	)EF
00000000	0B 1E	A1 88	A8	C2 F0	D7	49	8B	A1	0F	05	65	44	35	卿ツ・	I僑∈	:D5
00000010	66 08	3F 8A	. CO	6F 9F	3F	67	B8	E5	98	C1	91	F8	53	f.?澗o.?	g/娴稆	若S
00000020	54 29	1D A1	8B	CA 9F	1F	0B	B6	18	3D	4C	90	7E	B2	T) <u>∓</u>	.力.=L履	詩イ 📲
00000030	4C 73	<u>20</u> 57	F5	BE 7E	40	A8	D8	C7	35	50	0F	АE	07	Ls <u>,</u> ₩∙~@	₁リヌ5P.	э.
00000040	D8 E	26 BE	5F	25 13	C7	28	86	76	8A	FB	06	4B	E3	IJ. <u>₿</u> セ_%.ヌ	(・棋.	K覊
00000050	B1 B3	C8 EA	FC	05 C6	73	9A	CF	3E	BC	DA	C4	CO	D1	「椋•.二s	墹>シレト	処
00000060	44 4E	B0 71	22	1F 39	8F	95	1B (	77	CE	6F	F9	81	B1	DN-q″.9₿	h.wħo	• 7
00000070	CC 7B	25 44	AF	92 FE	8B	C3	EA	B3	D3	62	67	A3	70	- 7{%Dッ凑	≣• Đa	gL:
00000080	43 54	D9 19												CTル.		
選択:0x000	00042~0	x00000	042 (	Dx1(1)B	ytes			0x0(	0000	)043				上書 132 B	ytes	

The value of the 66th byte (0x42) is

26.

😹 Stirling	- [Key	file.ke	ey *]							_ 🗆	×
🃴 ファイル(E)	編集(E)	)検索	・移動(§	5) 設知	Ē( <u>0</u> ) ⊅	ィントウ	(W) - ′	ヘルフ°(	H)	_ 5	Ľ
	<b>n</b> e	X Ba	E 💊	)= <b>/</b>	1 🕸 (14)	<b>#41</b>	, CC	-			<u> </u>
ADDRESS	00 01	02 03	04 05	06 07	08 09	0 A 0	B OC	0D (	DE OF	0123456789ABCDEF	-
00000000	0B 1E	A1 8B	A8 C2	F0 D7	49 8B	A1 0	IF 05	65 4	44 35	卿ツ・I僑eDst	5
00000010	66 08	3F 8A	CO 6F	9F 3F	67 B8	E5 9	18 C1	91 F	-8 53	f.?澗o.?g舛科諾S	S
00000020	54 29	1D A1	8B CA	9F 1F	0B B6	18-3	D 4C	90 1	7E B2	T).。玉九.毛厨~	1
00000030	4C 73	20, 57	F5 BE	7E 40	A8 D8	C7 3	5 50	0F /	AE 07	Ls,W•~@ィリヌ5P.∍.	.
00000040	D8 E	27 BE	5F 25	13 C7	28 86	76-8	A FB	06 4	4B E3	り.' <u>セ</u> ぷ.ヌ(・棋.Kā	靍
00000050	B1 B3	C8 EA	FC 05	C6 73	9A CF	3E B	IC DA	C4 (	CO D1	ウネ゙・.ニs墹>シレトタノ	4
00000060	44 4E	BO 71	22 1F	39 8F	95 1B	77 0	Έ6F	F9 8	81 B1	DN-q″.9助.w标o・フ	ק
00000070	CC 7B	25 44	AF 92	FE 8B	C3 EA	B3 D	13 62	67 /	43 70	7{%Dy凝・モbgjr	>
00000080	43 54	D9 19								CTル.	
ντί						0x000	00043	更新	<b>f</b>	上書 132 Bytes	

### 26 27

Let's change the value above. This means that it has been inverted by 1 bit.

It means that it has been tampered with.

😹 Stirling	- [Keyfile_:	2nd.key]			_ 🗆 🗙
🃑 ファイル(E)	編集( <u>E</u> ) 検察	索·移動( <u>S</u> ) 設	と定( <u>0</u> ) ウィントゥ(W	) ヘルプ(円)	_ 8 ×
0 🖻 🔒	<mark>२</mark> ८ ४ ष		🙀 🙀 HAL HAT 🎎		M 📑 📲
ADDRESS	00 01 02 03	3 04 05 06 0	07 08 09 0A 0B	OC OD OE OF	0123456789ABCDEF
00000000	OB 1E A1 8E	3 A8 C2 F0 D	07 49 8B A1 OF	05 65 44 35	卿ツ・I僑eD5
00000010	66 08 3F 84	A CO 6F 9F 3	3F 67 B8 E5 98	C1 91 F8 53	f.?澗o.?g舛耕諾S
00000020	54 29 1D A1	I 8B CA 9F 1	F OB B6 18 3D	4C 90 7E B2	T).。玉九.毛厨イ
00000030	40 73 26 57	7 F5 BE 7E 4	40 A8 D8 C7 35	50 OF AE 07	Ls,₩•~@ィリヌ5P.∍.
00000040	D8 E <b>(</b> 27)BE	E 5F 25 13 C	7 28 86 76 8A	FB 06 4B E3	リ.' <u>セ</u> ぷ.ヌ(・棋.K覊
00000050	B1 B3 C8 E/	A FC 05 C6 7	73 9A CF 3E BC	DA C4 C0 D1	妳∙.ニs墹>シレトタム
00000060	44 4E B0 71	I 22 1F 39 8	3F 95 1B 77 CE	6F F9 81 B1	DN-q″.9助.wħo・7
00000070	CC 7B 25 44	1 AF 92 FE 8	B C3 EA B3 D3	62 67 A3 70 -	7{%Dy凝・tbgjp
00000080	43 54 D9 19	)			CTル.
レディ			0x00000	043	上書 132 Bytes //

### file name: Keyfile_2nd.key

Save it as this file name.



Send it back to iPhone and try decrypting Keyfile_2nd.key.

11:14	**	\$ <b>•</b>
	Password Maker	
Confirmin	g Keyfile	
Keyfile F	ïlename	
Keyfile_	2nd.key	
select		clear
Passwor	d (for decrypting Keyfile)	
Aaaa		
input		clear
Content		
		clear
	Do Confirming Content	
♠		

Even if you press the "Do Confirming Content" button, the value of the contents will not be displayed.

This is because it was detected that it had been tampered with (broken).

11:15

### **Password Maker**

#### Keyfile.key

0b 1e a1 8b a8 c2 f0 d7 49 8b a1 0f 05 65 44 35 66 08 3f 8a c0 6f 9f 3f 67 b8 e5 98 c1 91 f8 53 54 29 1d a1 8b ca 9f 1f 0b b6 18 3d 4c 90 7e b2 4c 73 2e 57 f5 be 7e 40 a8 d8 c7 35 50 0f ae 07 d8 e7 26 be 5f 25 13 c7 28 86 76 8a fb 06 4b e3 b1 b3 c8 ea fc 05 c6 73 9a cf 3e bc da c4 c0 d1 44 4e b0 71 22 1f 39 8f 95 1b 77 ce 6f f9 81 b1 cc 7b 25 44 af 92 fe 8b c3 ea b3 d3 62 67 a3 70 43 54 d9 19

#### 11:15

 $\hat{\boldsymbol{s}}$ 



## **Password Maker**

#### Keyfile_2nd.key

0b 1e a1 8b a8 c2 f0 d7 49 8b a1 0f 05 65 44 35 66 08 3f 8a c0 6f 9f 3f 67 b8 e5 98 c1 91 f8 53 54 29 1d a1 8b ca 9f 1f 0b b6 18 3d 4c 90 7e b2 4c 73 2c 57 f5 be 7e 40 a8 d8 c7 35 50 0f ae 07 d8 e7 27 be 5f 25 13 c7 28 86 76 8a fb 06 4b e3 b1 b3 c8 ea fc 05 c6 73 9a cf 3e bc da c4 c0 d1 44 4e b0 71 22 1f 39 8f 95 1b 77 ce 6f f9 81 b1 cc 7b 25 44 af 92 fe 8b c3 ea b3 d3 62 67 a3 70 43 54 d9 19 In this way, even if the contents of Keyfile.key are inverted by one bit, it can be detected.

11:15	<b>?</b>	
Password Maker		
Confirming Keyfile		
Keyfile Filename		
Keyfile.key		
select	clear	
Password (for decrypting Keyfile)		
Aaab		The password is Aaab.
input	clear	
Content		
	clear	
Do Confirming Content		
♠		

In this way, even if the decryption password is incorrect, it can be detected.

The value before encryption cannot be retrieved. This key file can detect such a thing. In that case, decryption will not be performed. Password generation using the key file is not performed.

A password is generated using a strange key file. Such a thing never happen.