PKCS#1 v.1.5 encryption (using public key)

This command does encryption with RSA public key cipher in a padding in PKCS#1 v.1.5 format.

It is the most basic encryption in RSA public key cipher.

With this encryption, when using a a key of 2,048 bits in length, you can encrypt up to 245 bytes in length.

A plain text whose length exceeds 245 bytes can not be encrypted with this command.

When using a key of 1,024 bits in length, it will be up to 117 bytes in length.

Specifically, it is up to (number of bytes of key length) - 11.

Padding in PKCS#1 v.1.5 format requires a minimum of 11 bytes for padding.

7.2.1 Encryption operation

RSAES-PKCS1-V1_5-ENCRYPT $((n, e), M)$

Input:	(n, e)	recipient's RSA public key (k denotes the length in octets of the modulus n)
	M	message to be encrypted, an octet string of length $mLen$, where $mLen \leq k - 11$
Output:	C	ciphertext, an octet string of length k
Error:	"message too long"	
Steps:		

This is a copy from the specification of PKCS#1, but this 11 is that minimum padding.

The user interface will be something like this.

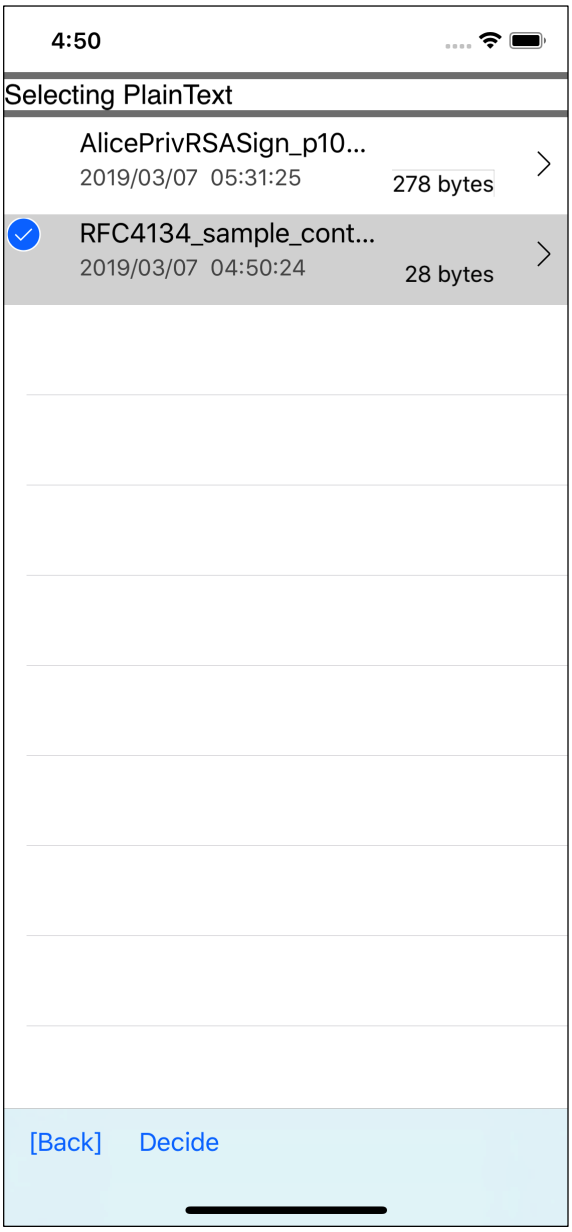
Plain text file name to be encrypted

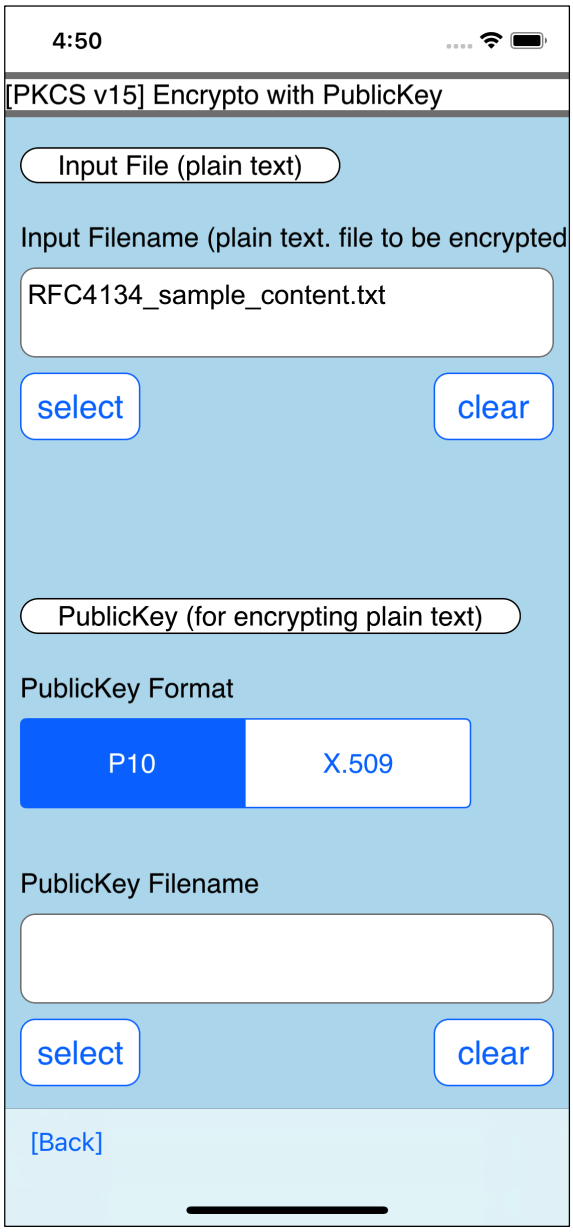
Type of public key

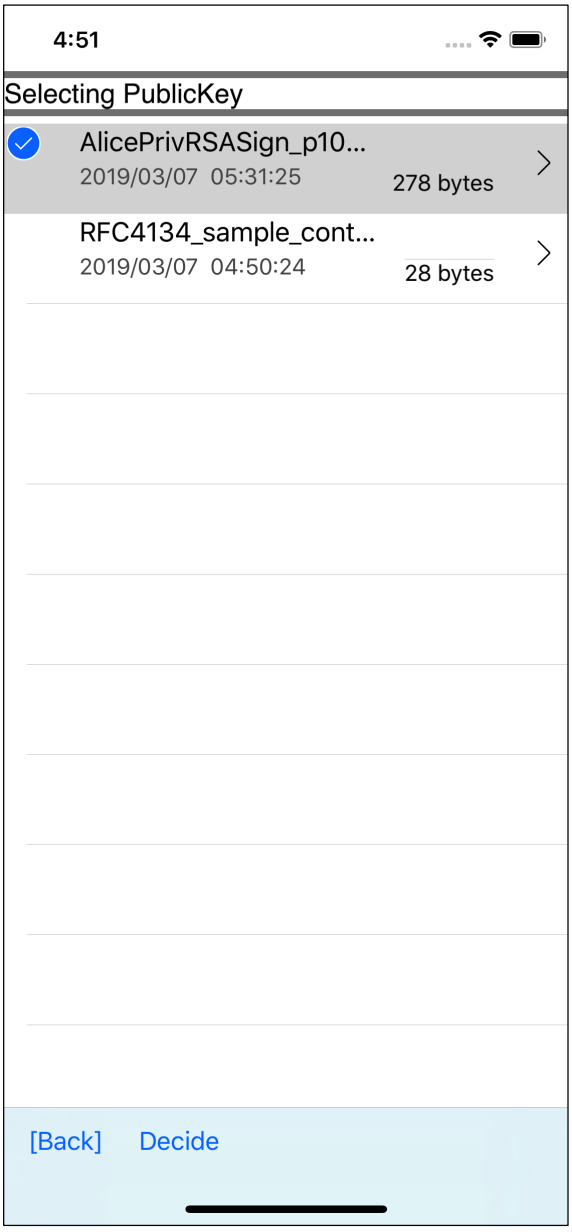
File name of public key

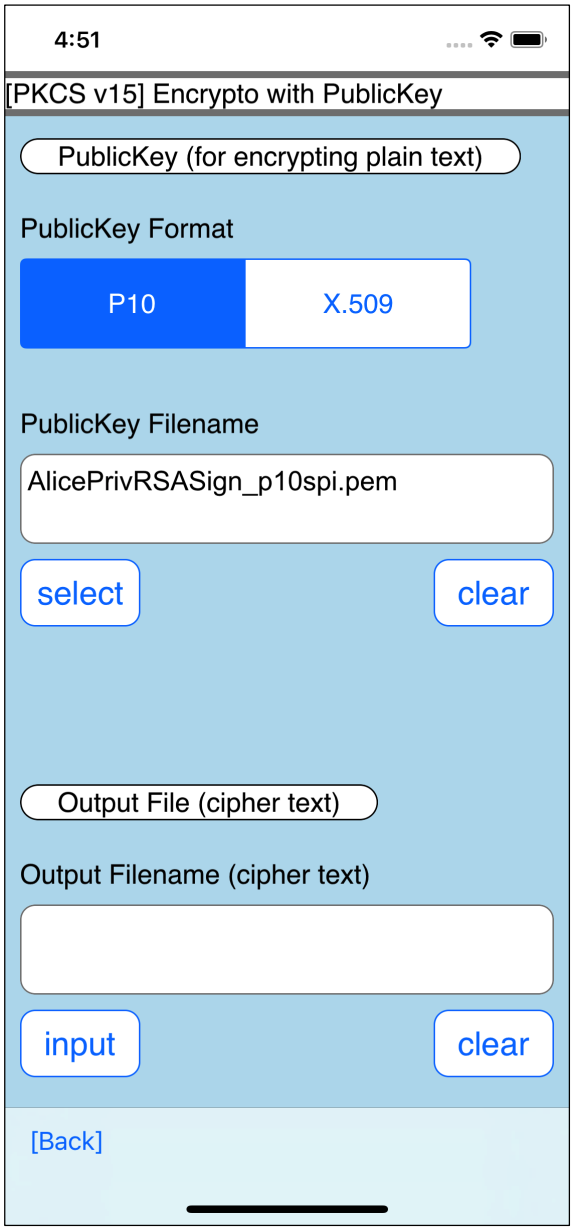
File name of ciphertext output destination

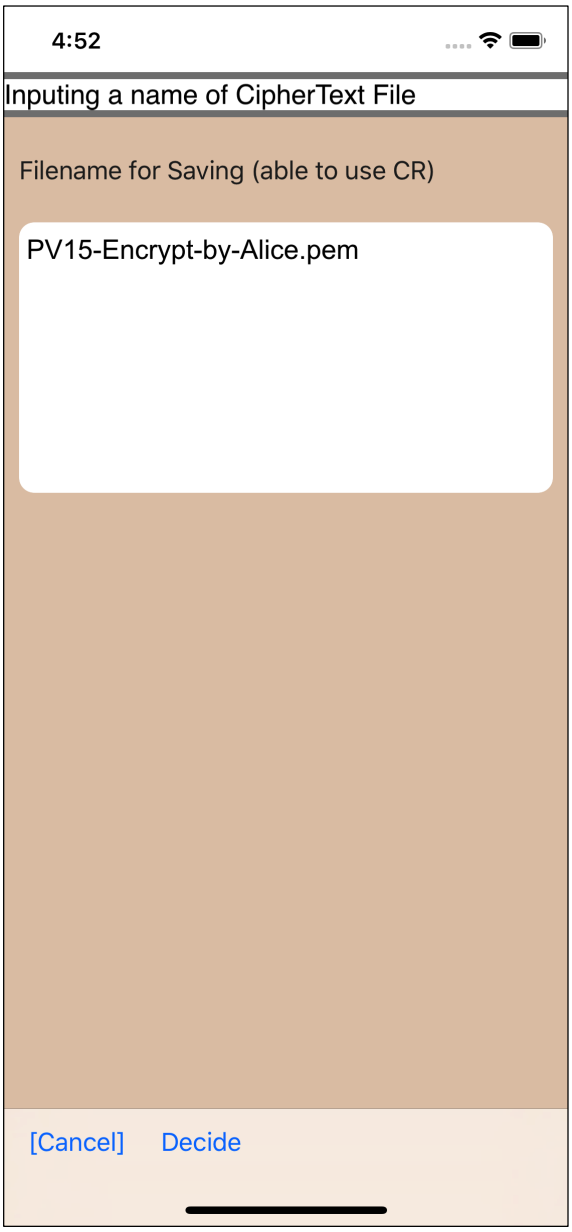
This is the meaning.

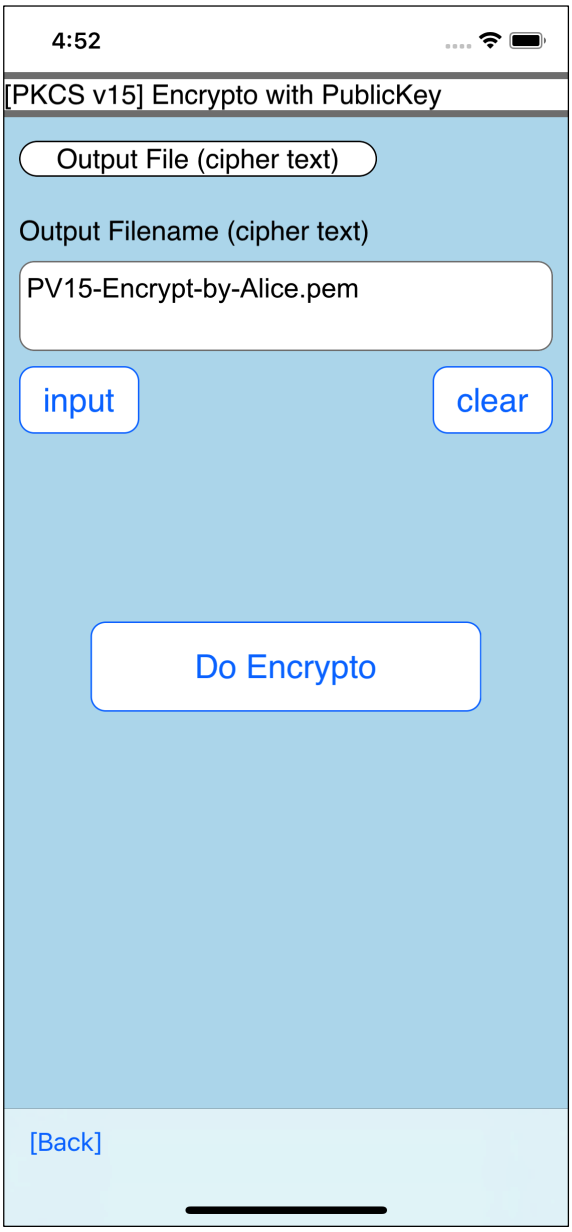

4:50
Selecting PlainText
AlicePrivRSASign_p10...
2019/03/07 05:31:25
278 bytes
RFC4134_sample_cont...
2019/03/07 04:50:24
28 bytes
[Back]
Decide

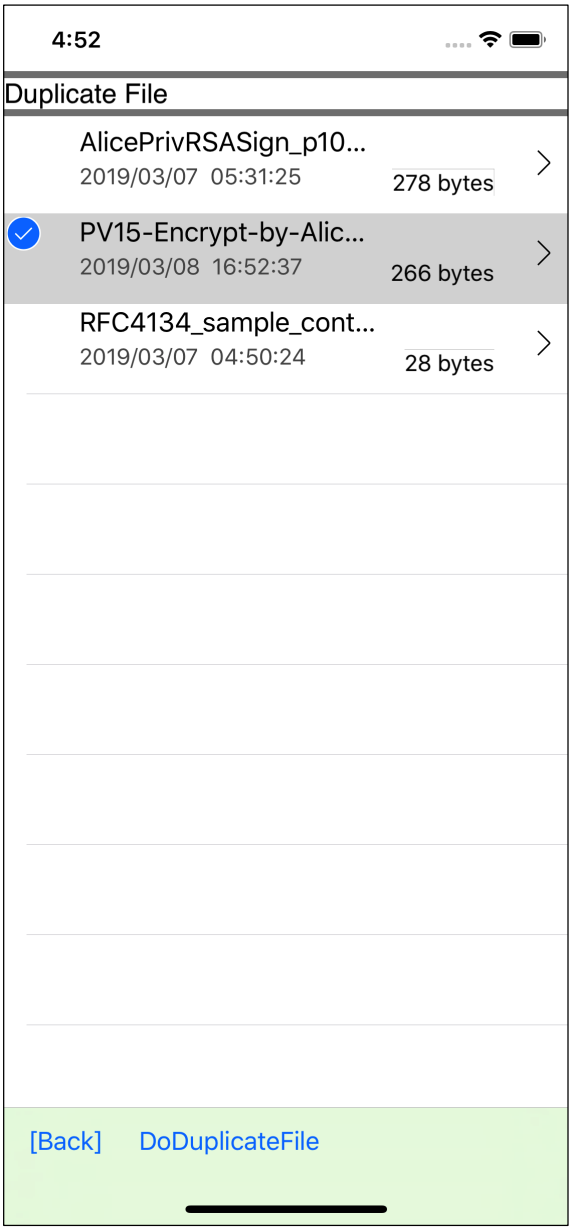

4:50
[PKCS v15] Encrypto with PublicKey
Input File (plain text)
Input Filename (plain text. file to be encrypted
RFC4134_sample_content.txt
select
clear
PublicKey (for encrypting plain text)
PublicKey Format
P10
X.509
PublicKey Filename
select
clear
[Back]

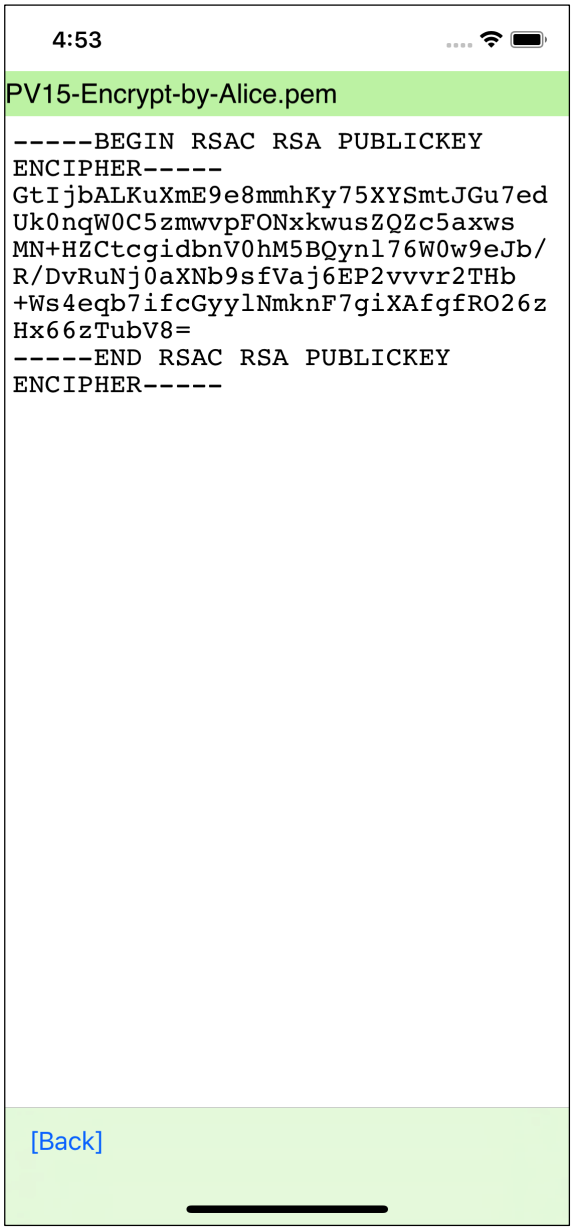

4:51
Selecting PublicKey
AlicePrivRSASign_p10...
2019/03/07 05:31:25
278 bytes
RFC4134_sample_cont...
2019/03/07 04:50:24
28 bytes
[Back]
Decide

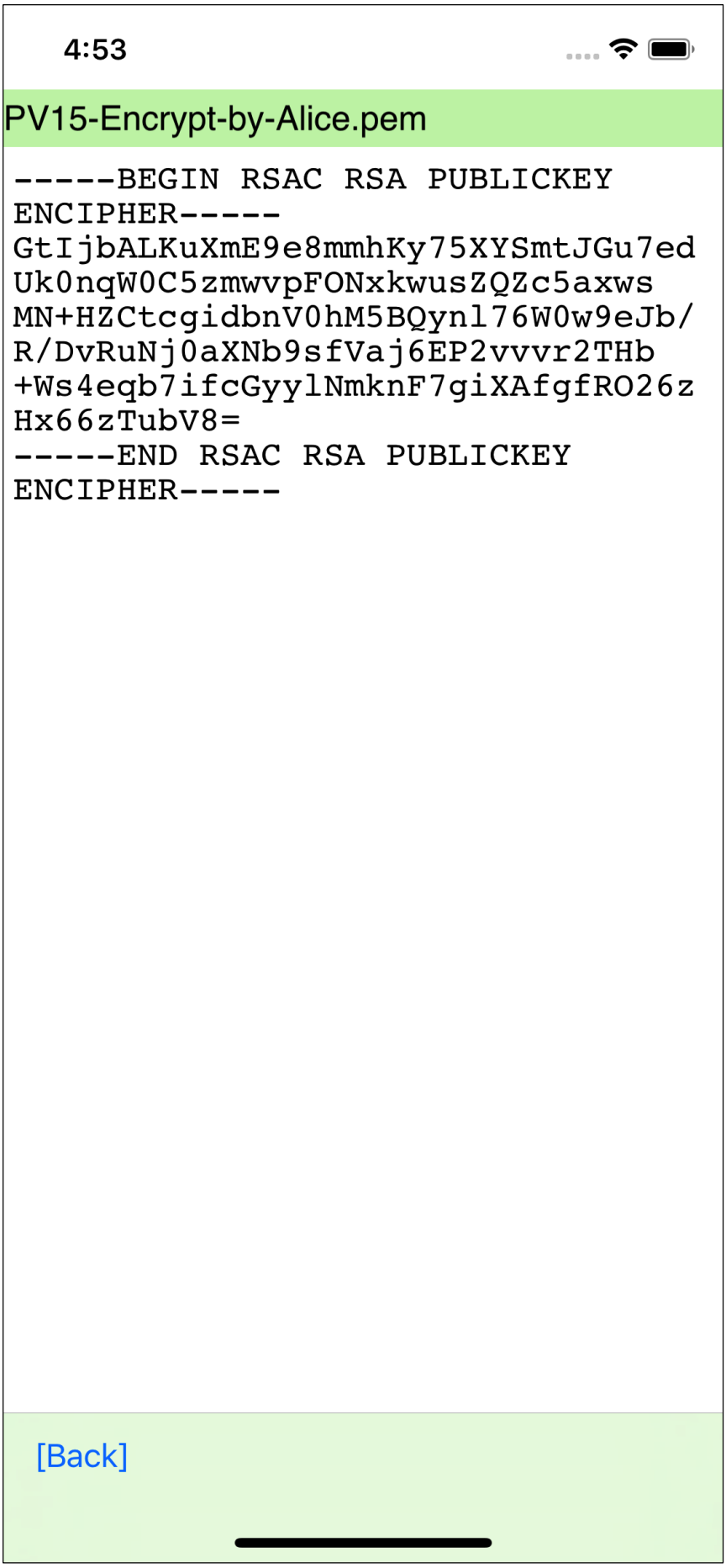

4:51
[PKCS v15] Encrypto with PublicKey
PublicKey (for encrypting plain text)
PublicKey Format
P10
X.509
PublicKey Filename
AlicePrivRSASign_p10spi.pem
select
clear
Output File (cipher text)
Output Filename (cipher text)
input
clear
[Back]


4:52
Inputing a name of CipherText File
Filename for Saving (able to use CR)
PV15-Encrypt-by-Alice.pem
[Cancel]
Decide


4:52
[PKCS v15] Encrypto with PublicKey
Output File (cipher text)
Output Filename (cipher text)
PV15-Encrypt-by-Alice.pem
input
clear
Do Encrypto
[Back]


4:52
Duplicate File
AlicePrivRSASign_p10...
2019/03/07 05:31:25
278 bytes
PV15-Encrypt-by-Alic...
2019/03/08 16:52:37
266 bytes
RFC4134_sample_cont...
2019/03/07 04:50:24
28 bytes
[Back]
DoDuplicateFile


4:53
PV15-Encrypt-by-Alice.pem
-----BEGIN RSAC RSA PUBLICKEY ENCIPHER-----
GtIjbALKuXmE9e8mmhKy75XYSmtJGu7ed
Uk0nqW0C5zmwvpFONxkwusZQZc5axws
MN+HZCtcgidbnV0hM5BQynl76W0w9eJb/
R/DvRuNj0aXNb9sfVaj6EP2vvvr2THb
+Ws4eqb7ifcGyylNmknF7giXAfgfRO26z
Hx66zTubV8=
-----END RSAC RSA PUBLICKEY ENCIPHER-----
[Back]


4:53
PV15-Encrypt-by-Alice.pem
-----BEGIN RSAC RSA PUBLICKEY
ENCIPHER-----
GtIjbALKuXmE9e8mmhKy75XYSmtJGu7ed
Uk0nqW0C5zmwvpFONxkwusZQZc5axws
MN+HZCtcgidbnV0hM5BQynl76W0w9eJb/
R/DvRuNj0aXNb9sfVaj6EP2vvvr2THb
+Ws4eqb7ifcGyylNmknF7giXAfgfRO26z
Hx66zTubV8=
-----END RSAC RSA PUBLICKEY
ENCIPHER-----
[Back]

This ciphertext is not stored in the type of ASN.1 syntax.

One of RSA public key cipher in padding in PKCS#1 v.1.5 format is converted into text by Base 64 encoding and it is just surrounded by boundary character string.

Therefore, if you do removing boundary character string and reverting to ciphertext of RSA public key cipher in binary format by Base 64 decording, it becomes ciphertext of RSA public key cipher in padding in PKCS#1 v.1.5 format of binary format.

Ciphertext of RSA public key cipher in padding in PKCS#1 v.1.5 format of binary format should be able to decrypt with most cryptographic software that supports RSA public key cipher.