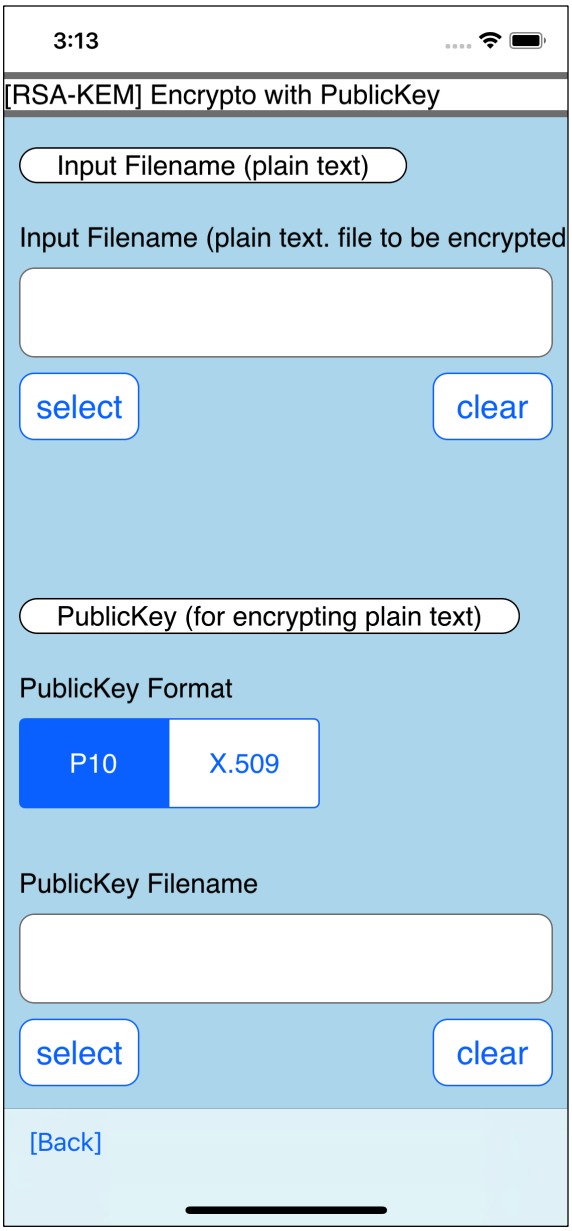
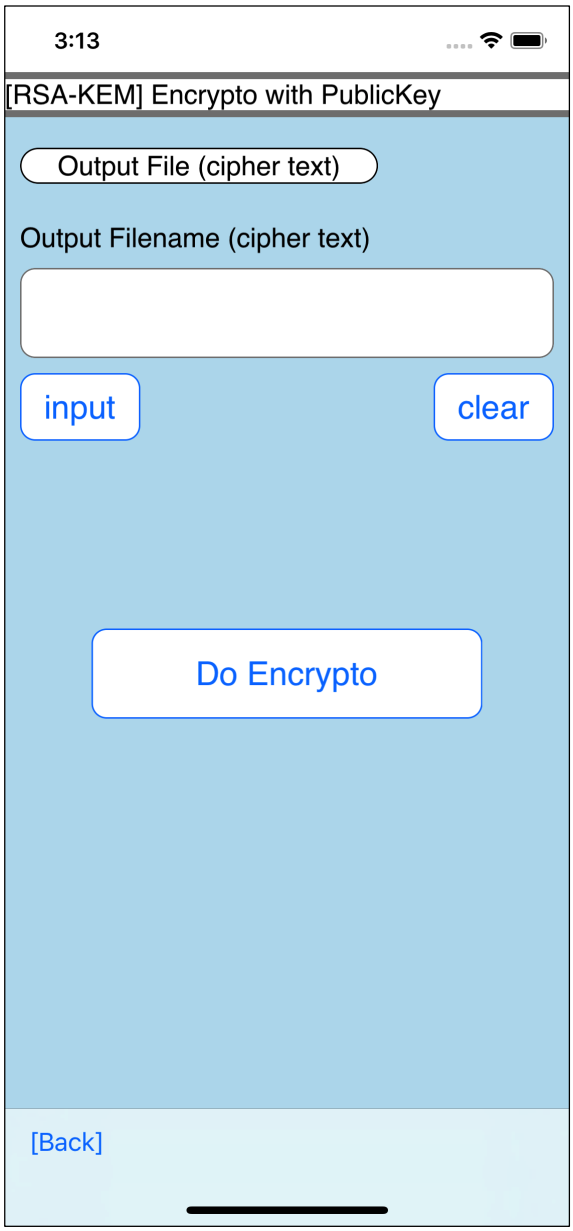
RSA-KEM encryption (using public key)

This command encrypts with RSA-KEM using the public key.

With RSA-KEM encryption, there is no limit on the length of a plain text to be encrypted.





The user interface will be something like this.

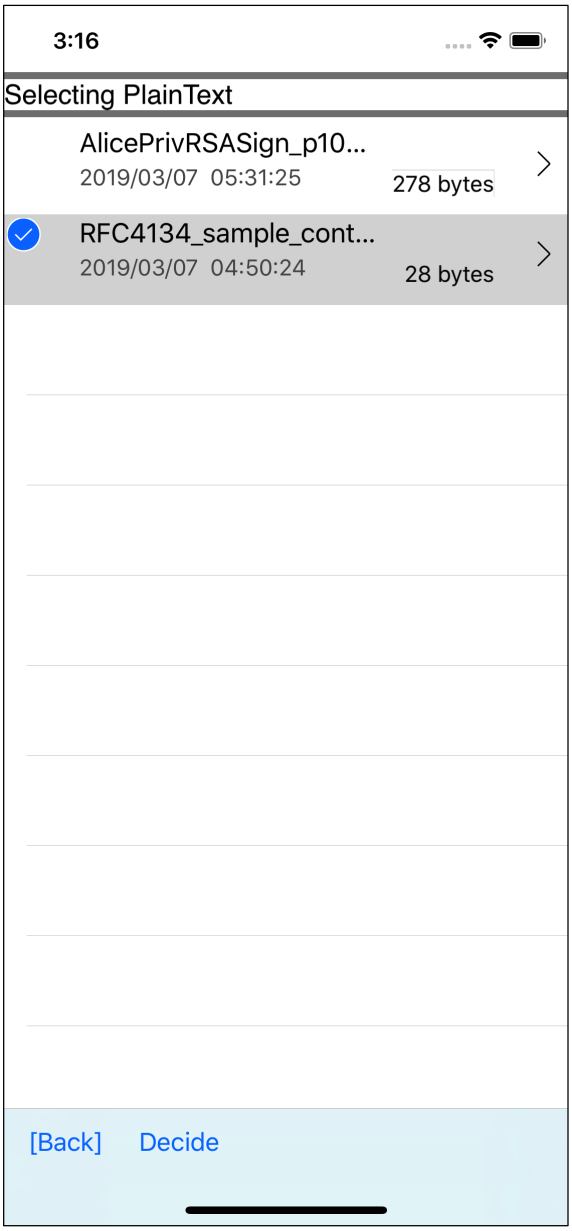
Plain text file name to be encrypted

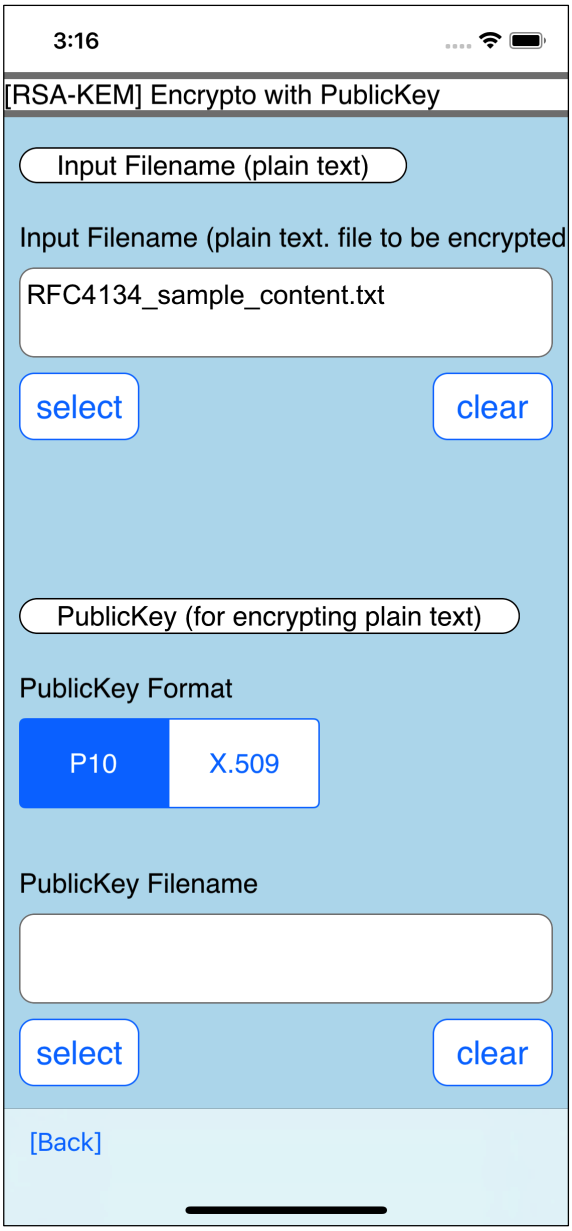
Type of public key

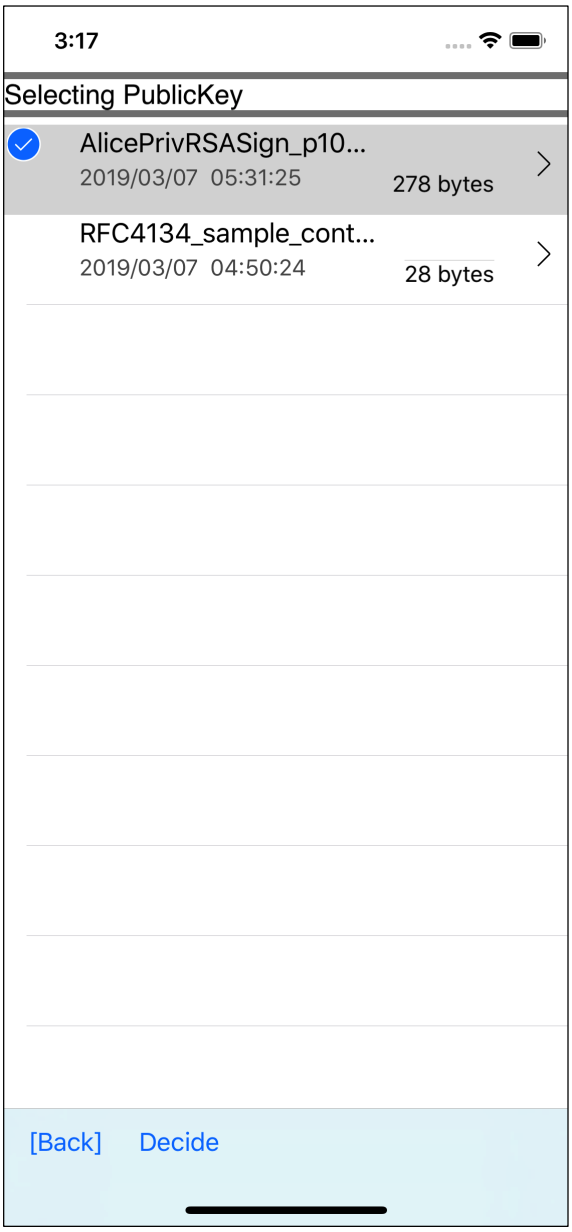
File name of public key

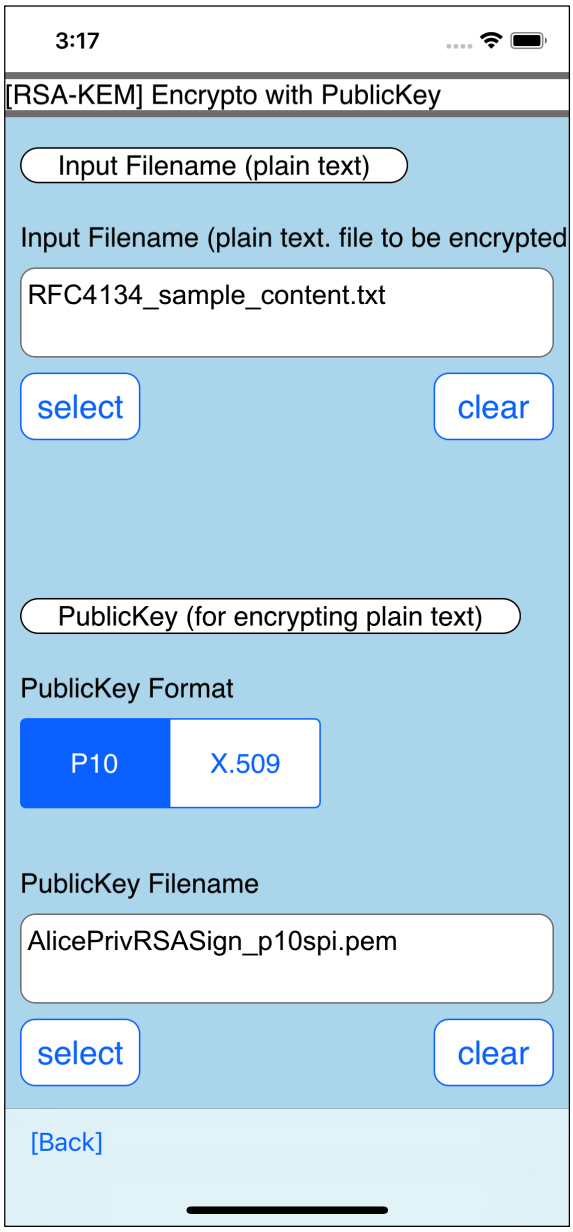
Name of output destination of ciphertext

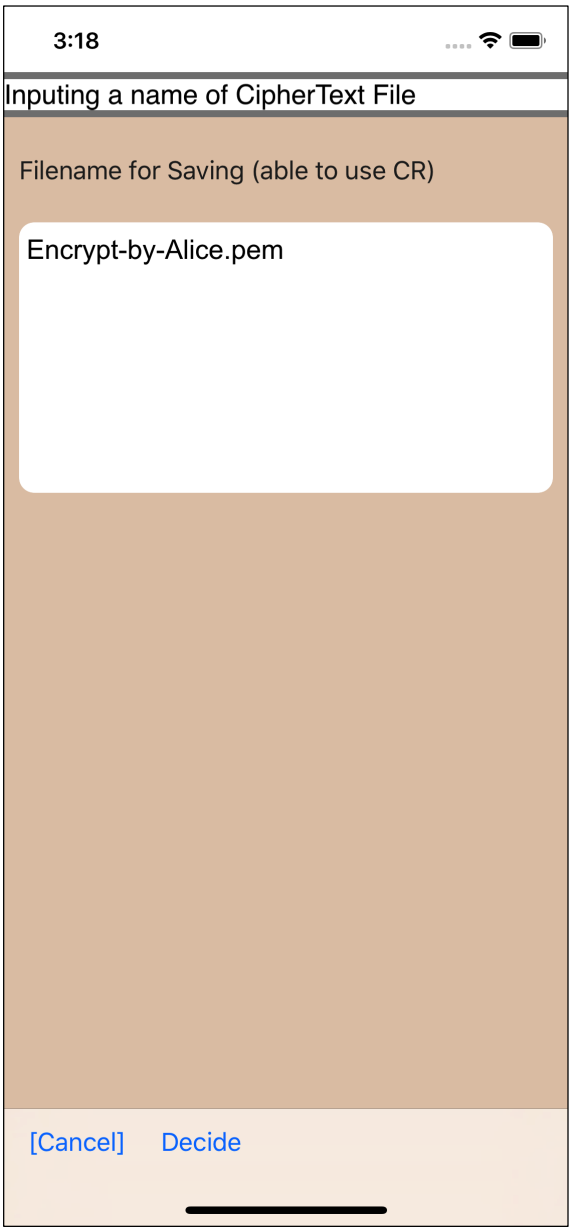
This is the meaning.

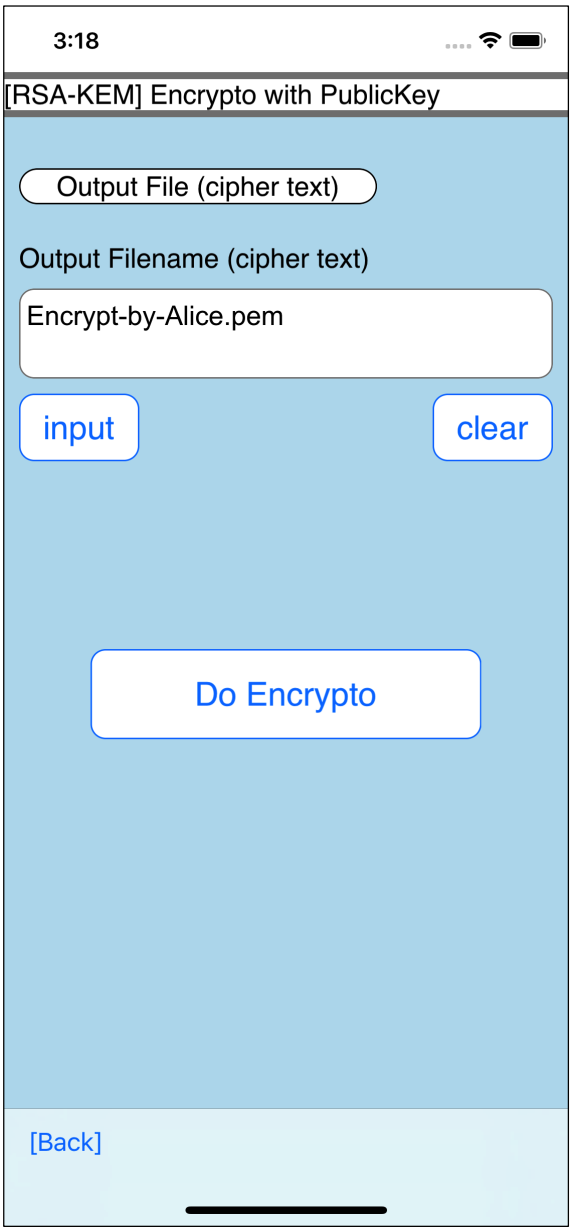

3:16
Selecting PlainText
AlicePrivRSASign_p10...
2019/03/07 05:31:25
278 bytes
RFC4134_sample_cont...
2019/03/07 04:50:24
28 bytes
[Back]
Decide

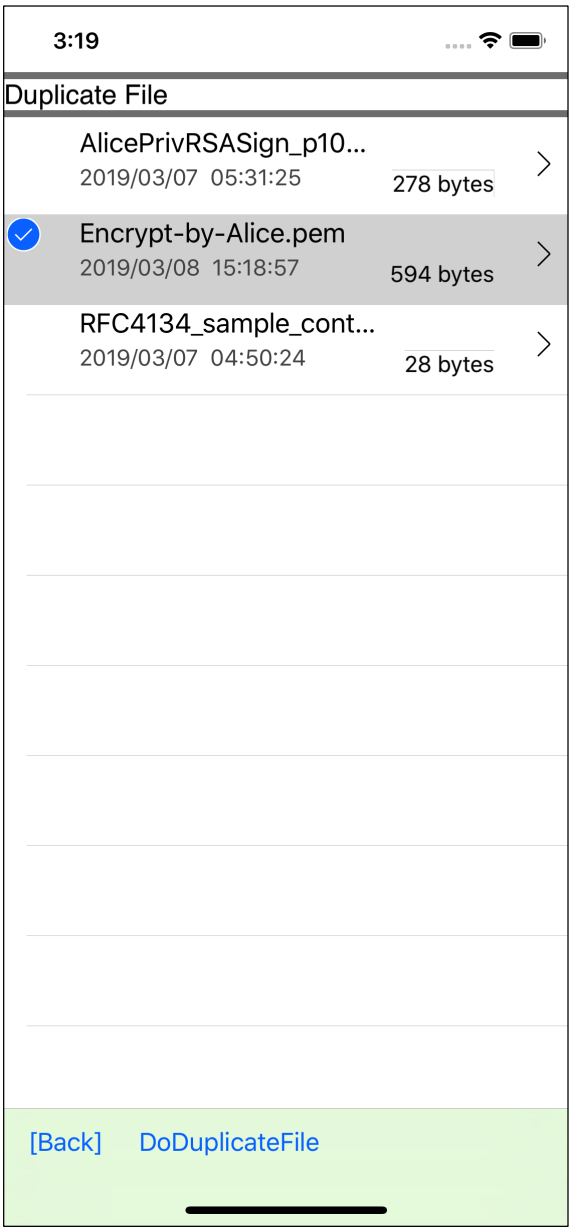

3:16
[RSA-KEM] Encrypto with PublicKey
Input Filename (plain text)
Input Filename (plain text. file to be encrypted
RFC4134_sample_content.txt
select
clear
PublicKey (for encrypting plain text)
PublicKey Format
P10
X.509
PublicKey Filename
select
clear
[Back]


3:17
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

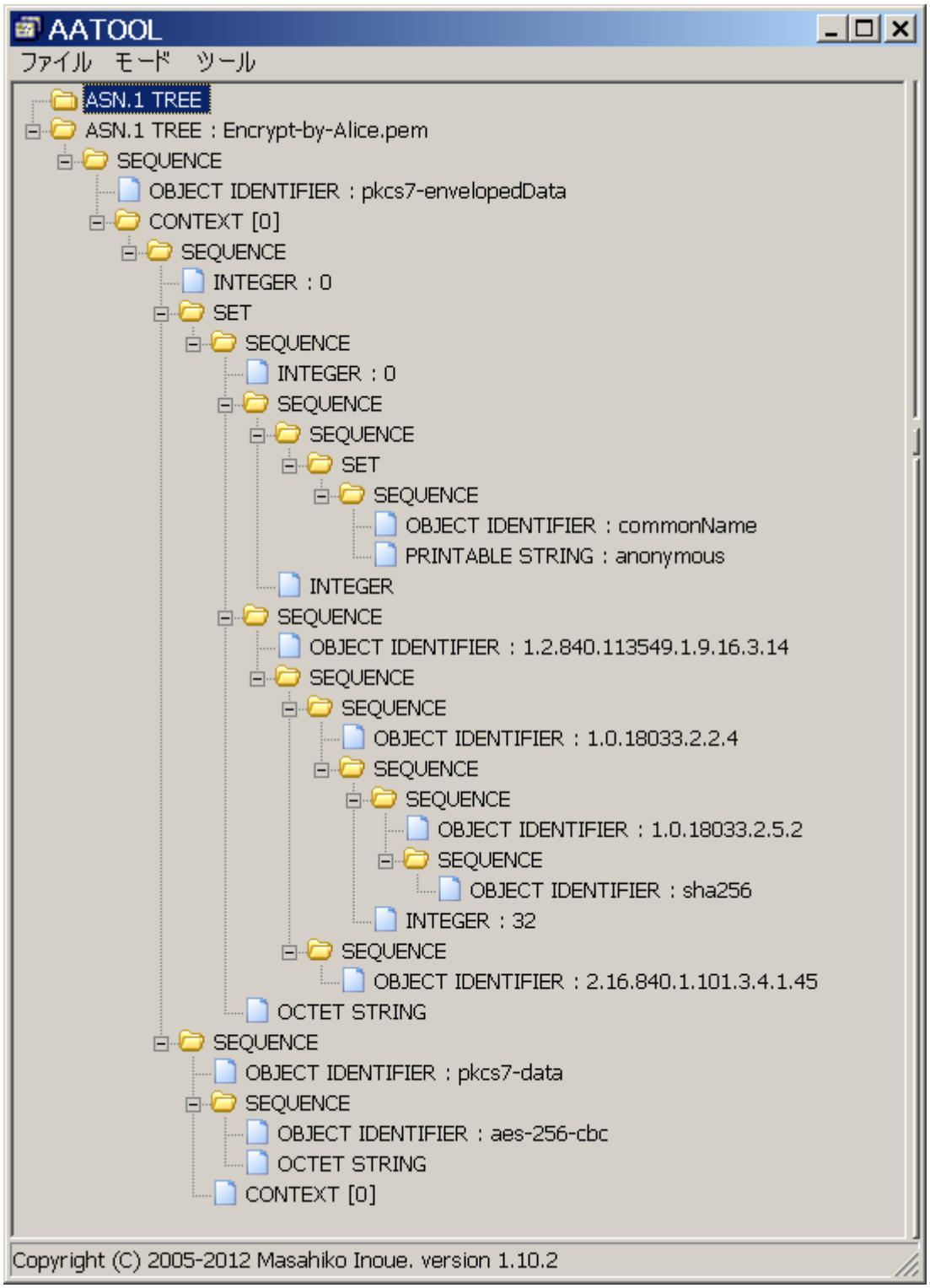

3:17
[RSA-KEM] Encrypto with PublicKey
Input Filename (plain text)
Input Filename (plain text. file to be encrypted
RFC4134_sample_content.txt
select
clear
PublicKey (for encrypting plain text)
PublicKey Format
P10
X.509
PublicKey Filename
AlicePrivRSASign_p10spi.pem
select
clear
[Back]


3:18
Inputing a name of CipherText File
Filename for Saving (able to use CR)
Encrypt-by-Alice.pem
[Cancel]
Decide


3:18
[RSA-KEM] Encrypto with PublicKey
Output File (cipher text)
Output Filename (cipher text)
Encrypt-by-Alice.pem
input
clear
Do Encrypto
[Back]


3:19
Duplicate File
AlicePrivRSASign_p10...
2019/03/07 05:31:25
278 bytes
Encrypt-by-Alice.pem
2019/03/08 15:18:57
594 bytes
RFC4134_sample_cont...
2019/03/07 04:50:24
28 bytes
[Back]
DoDuplicateFile


3:19
Encrypt-by-Alice.pem
-----BEGIN PKCS7-----
MIIBigYJKoZIhvcNAQcDoIIBezCCAXcCA
QAxggEiMIIBHgIBADAoMBQxEjAQBgNV
BAMTCWFub255bW91cwIQYBKFZzdotAVIQ
g1SuqpgRTBEBgsqhkiG9w0BCRADDjA1
MCYGByiBjHECAgQwGzAWBgcogYxxAgUCM
AsGCWCGSAFlAwQCAQIBIDALBglghkgB
ZQMEAS0EgagExmXAoWyhI/
rlcxCxMkcOpVwwwXCbeMGzoro9+9u8fHJ
boRM7ogus
iVBvV0fJol65y1RrQlVxNavKLkhbF1dan
bthIfHSLR74a9bed94AbskHqTtzl0qb
pJQnwaya+jdXwShP2i6fjqG5sXUT4BJGY
HFyYG0eREaGpbiXxjahvpavnh/1fB3J
Lpmafsvl2HlnL4jCCAOTHRvM2OhEb0b8a
PCAtbu/fWIwTAYJKoZIhvcNAQcBMB0G
CWCGSAFlAwQBKgQQuumxGHzdh7SlUq5rH
gjA2IAgQQMG06eiBS3PVp9oSe/oVr3I
I2ph2OIsaxX/t16OUbY=
-----END PKCS7-----
[Back]



Looking at the created ciphertext with the ASN.1 syntax analysis application, it looks something like this.

This ciphertext should be able to be decrypted if you use cryptographic software that can handle PKCS#7 EnvelopedData to store ciphertext of RSA-KEM.

Also, PKCS#7 EnvelopedData has something like a name field.

It is set to anonymous in rsac.