古谷康平　43M22403

岡山大学のロゴマークの暗号化において行った処理を下記に示す。

なお、実行環境はWindowsのコマンドプロンプトである。

コマンド説明文章は、青色で示す。

1. **RSA暗号の鍵生成**

C:\Users\Owner>openssl genrsa > secret.key

Generating RSA private key, 2048 bit long modulus (2 primes)

........................................................................+++++

..+++++

e is 65537 (0x010001)

-RSA暗号秘密鍵の生成の第一行目。eは公開鍵を示している。nは2048ビット。

C:\Users\Owner>openssl rsa -pubout < secret.key > public.key

writing RSA key

-公開鍵の情報から秘密鍵dを計算している。

C:\Users\Owner>openssl rsa -text < secret.key

RSA Private-Key: (2048 bit, 2 primes)

modulus:

00:d0:c1:45:40:1e:12:52:ca:48:ed:f0:a8:b2:22:

5d:62:57:82:35:5a:71:99:ed:90:ac:46:b3:eb:21:

ea:bb:f4:23:85:ca:4a:43:82:27:1e:28:de:87:c1:

6b:9e:c7:c8:5e:d5:4d:b9:f1:d6:da:4a:2b:88:54:

04:82:cd:ba:70:d0:a3:72:16:23:da:d4:0d:64:36:

d8:43:29:5f:3d:d9:3f:02:ba:1c:dd:24:f7:8d:47:

44:d3:09:f1:68:32:1a:ec:3d:70:e8:7a:45:2f:e4:

0e:b4:e5:70:15:55:62:4b:7c:9c:12:60:ac:e0:1a:

8d:7d:8a:bd:c5:86:32:32:04:c8:4e:67:fb:26:c1:

4b:05:6d:ce:fd:6b:ad:00:3a:e8:1e:16:1c:fd:9a:

26:2a:52:53:63:67:73:cb:95:a2:26:9e:30:41:82:

3c:5b:f9:a7:24:b5:7d:fe:f8:94:c9:fd:c0:c2:f7:

39:a8:99:76:62:18:9e:80:a0:10:fe:a2:b5:81:e5:

cf:ab:00:55:22:ee:2d:86:dc:72:5b:7e:46:0c:e9:

1d:d9:3a:19:81:39:3a:7b:3d:7a:ea:fa:83:21:dc:

3c:ad:1c:9d:a9:2a:e5:a4:ba:b0:60:6a:33:96:3f:

af:36:8b:86:77:2e:29:07:92:82:1d:52:1a:09:2d:

e6:11

publicExponent: 65537 (0x10001)

privateExponent:

00:ac:d8:da:76:14:70:27:8c:c6:85:fd:56:30:e8:

b3:59:d2:0b:46:11:f5:2d:f6:be:6b:66:bf:62:59:

5a:fa:f5:52:d4:5c:82:d1:12:db:40:e5:a6:1b:d1:

d3:42:4d:39:63:0c:4a:a7:43:cf:1a:3f:7f:7c:09:

d5:12:59:35:9e:63:a2:71:bc:53:43:c5:80:b1:11:

98:4f:43:da:50:63:a9:00:a1:09:75:32:3e:a7:03:

f3:c0:a9:e2:f0:db:4b:df:7f:a0:15:5d:e8:1b:97:

41:76:16:e3:8f:46:7b:74:f5:60:64:f7:17:2d:17:

cf:3f:bb:b9:15:eb:df:73:f9:72:86:6a:79:45:fc:

4b:90:01:a0:e7:98:e1:18:df:7b:e0:e4:05:3b:5b:

78:34:c6:5b:fb:1e:3c:74:1d:f5:1b:f4:60:9b:76:

f0:75:76:75:c2:f6:25:b2:35:b3:ae:e7:4c:4b:9a:

af:aa:dc:a5:d6:66:7a:28:29:28:51:34:55:c0:60:

f0:11:0e:12:f3:7b:13:f2:e1:7e:f9:a9:fd:9b:32:

e1:25:1a:d4:40:f7:0f:79:07:58:10:45:df:80:ba:

4b:c6:2a:04:e1:81:03:47:2d:8e:de:f3:cf:f5:1c:

df:f6:0e:b0:5f:d9:c5:27:1c:59:54:e4:c8:e5:2c:

9e:61

prime1:

00:f2:0d:1a:77:da:6c:9e:25:3e:ae:8f:66:98:b6:

69:28:82:eb:14:3a:04:74:27:42:6e:64:2f:1c:32:

5e:12:fb:c1:4c:2f:16:3a:ad:4f:a0:6e:8b:f3:6e:

9f:42:44:d0:34:b5:e8:dd:8c:4a:0b:6c:8f:87:5d:

bd:80:91:14:9d:5f:45:4c:65:1a:1f:42:c4:3f:76:

a3:af:45:7d:9f:b7:f5:d6:3b:60:3b:79:ea:ec:90:

87:32:7d:49:6b:70:a1:1f:c6:8c:1b:56:f5:4b:35:

1b:59:74:8a:06:3c:b9:c6:e8:74:1c:1e:98:44:32:

b4:6c:35:2f:3b:d3:88:50:0b

prime2:

00:dc:c8:f5:a6:ff:d7:23:da:a6:3b:f9:a7:97:2a:

d4:b5:26:65:8a:d2:e7:8a:27:e7:8b:9e:4a:28:7c:

72:5a:c5:f9:19:97:0c:1f:f7:c6:3d:d8:56:69:a6:

d3:a6:f6:ba:4e:b5:1f:97:9a:45:4c:c0:69:b9:81:

99:ae:e9:70:2b:96:6c:80:c5:d0:4d:31:47:85:9a:

d1:fb:c2:36:48:a2:17:6a:60:63:a7:a0:11:46:41:

42:39:11:cd:19:05:15:76:a5:c5:dc:6e:56:30:75:

0d:a1:0f:de:4b:93:82:42:a4:e7:30:75:25:49:a2:

79:c4:4d:d2:09:4d:0e:e7:d3

exponent1:

00:bf:ac:82:ae:30:48:5c:ff:4f:60:b9:eb:db:b8:

6f:13:86:80:93:56:d2:1a:0c:d0:bd:4c:16:46:34:

d8:6c:1d:f2:56:da:de:b6:7e:71:94:b0:95:a0:a2:

93:f8:cd:37:36:d6:6a:5d:ae:6f:20:16:ca:9d:be:

2c:87:37:db:e4:37:02:50:59:ab:52:df:f3:39:f2:

3f:f2:56:8c:01:43:92:a8:20:02:b7:76:77:02:f7:

fc:27:8e:30:ea:a4:98:e2:e9:be:1f:14:40:50:5a:

f0:9a:68:ff:b7:aa:b4:ce:7f:5b:1a:bd:5b:84:7d:

c6:83:fd:a5:b6:b1:6e:bb:3b

exponent2:

38:78:e2:74:8b:be:00:ba:bd:88:5b:ac:25:3b:5c:

5a:d5:6e:65:9a:da:84:78:fe:7d:b4:c8:2d:20:df:

b3:1e:2e:40:00:65:a6:8b:9e:d6:54:ce:8d:89:91:

5b:84:82:54:fd:79:0e:32:f4:84:d4:36:76:af:92:

9a:ad:b4:f6:41:2c:91:a7:87:47:27:52:ae:f6:d1:

bc:fe:89:19:fc:f3:d6:4e:bf:4e:b1:df:99:43:b9:

e7:95:09:0b:dc:44:08:2c:10:b6:f8:35:ed:81:13:

32:5e:37:b2:c7:11:2b:70:b8:7d:a9:89:17:13:8a:

e7:ce:2b:ea:1b:1e:b3:e7

coefficient:

00:e5:0b:b4:5b:f3:1f:66:1e:f9:33:ce:73:74:3a:

a9:d3:04:53:b2:9f:26:df:54:06:09:02:d5:96:f2:

83:ce:25:77:46:e6:a9:45:14:c1:4b:c6:a9:51:78:

c7:29:a6:1e:45:0b:79:b9:b1:9a:ca:3c:d2:db:65:

e5:7f:6a:40:89:12:28:54:fe:f0:b8:0d:4c:18:8d:

8a:98:13:bc:9a:22:79:98:7f:03:a3:96:66:cc:55:

dd:44:6b:82:bd:5d:f4:a9:ae:30:c1:d6:05:d5:a8:

01:ee:59:bf:14:07:c2:a3:ae:f1:b6:d1:7f:1f:71:

2c:30:f5:d8:0b:60:7f:49:8f

writing RSA key

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEA0MFFQB4SUspI7fCosiJdYleCNVpxme2QrEaz6yHqu/QjhcpK

Q4InHijeh8FrnsfIXtVNufHW2koriFQEgs26cNCjchYj2tQNZDbYQylfPdk/Aroc

3ST3jUdE0wnxaDIa7D1w6HpFL+QOtOVwFVViS3ycEmCs4BqNfYq9xYYyMgTITmf7

JsFLBW3O/WutADroHhYc/ZomKlJTY2dzy5WiJp4wQYI8W/mnJLV9/viUyf3Awvc5

qJl2YhiegKAQ/qK1geXPqwBVIu4thtxyW35GDOkd2ToZgTk6ez166vqDIdw8rRyd

qSrlpLqwYGozlj+vNouGdy4pB5KCHVIaCS3mEQIDAQABAoIBAQCs2Np2FHAnjMaF

/VYw6LNZ0gtGEfUt9r5rZr9iWVr69VLUXILREttA5aYb0dNCTTljDEqnQ88aP398

CdUSWTWeY6JxvFNDxYCxEZhPQ9pQY6kAoQl1Mj6nA/PAqeLw20vff6AVXegbl0F2

FuOPRnt09WBk9xctF88/u7kV699z+XKGanlF/EuQAaDnmOEY33vg5AU7W3g0xlv7

Hjx0HfUb9GCbdvB1dnXC9iWyNbOu50xLmq+q3KXWZnooKShRNFXAYPARDhLzexPy

4X75qf2bMuElGtRA9w95B1gQRd+AukvGKgThgQNHLY7e88/1HN/2DrBf2cUnHFlU

5MjlLJ5hAoGBAPINGnfabJ4lPq6PZpi2aSiC6xQ6BHQnQm5kLxwyXhL7wUwvFjqt

T6Bui/Nun0JE0DS16N2MSgtsj4ddvYCRFJ1fRUxlGh9CxD92o69FfZ+39dY7YDt5

6uyQhzJ9SWtwoR/GjBtW9Us1G1l0igY8ucbodBwemEQytGw1LzvTiFALAoGBANzI

9ab/1yPapjv5p5cq1LUmZYrS54on54ueSih8clrF+RmXDB/3xj3YVmmm06b2uk61

H5eaRUzAabmBma7pcCuWbIDF0E0xR4Wa0fvCNkiiF2pgY6egEUZBQjkRzRkFFXal

xdxuVjB1DaEP3kuTgkKk5zB1JUmiecRN0glNDufTAoGBAL+sgq4wSFz/T2C569u4

bxOGgJNW0hoM0L1MFkY02Gwd8lba3rZ+cZSwlaCik/jNNzbWal2ubyAWyp2+LIc3

2+Q3AlBZq1Lf8znyP/JWjAFDkqggArd2dwL3/CeOMOqkmOLpvh8UQFBa8Jpo/7eq

tM5/Wxq9W4R9xoP9pbaxbrs7AoGAOHjidIu+ALq9iFusJTtcWtVuZZrahHj+fbTI

LSDfsx4uQABlpoue1lTOjYmRW4SCVP15DjL0hNQ2dq+Smq209kEskaeHRydSrvbR

vP6JGfzz1k6/TrHfmUO555UJC9xECCwQtvg17YETMl43sscRK3C4famJFxOK584r

6hses+cCgYEA5Qu0W/MfZh75M85zdDqp0wRTsp8m31QGCQLVlvKDziV3RuapRRTB

S8apUXjHKaYeRQt5ubGayjzS22Xlf2pAiRIoVP7wuA1MGI2KmBO8miJ5mH8Do5Zm

zFXdRGuCvV30qa4wwdYF1agB7lm/FAfCo67xttF/H3EsMPXYC2B/SY8=

-----END RSA PRIVATE KEY-----

-生成されたRSA暗号秘密鍵の情報を示している。

上記より、RSA暗号の公開鍵と秘密鍵のペアは、

公開鍵: 65537 (0x10001)

秘密鍵:

00:ac:d8:da:76:14:70:27:8c:c6:85:fd:56:30:e8:

b3:59:d2:0b:46:11:f5:2d:f6:be:6b:66:bf:62:59:

5a:fa:f5:52:d4:5c:82:d1:12:db:40:e5:a6:1b:d1:

d3:42:4d:39:63:0c:4a:a7:43:cf:1a:3f:7f:7c:09:

d5:12:59:35:9e:63:a2:71:bc:53:43:c5:80:b1:11:

98:4f:43:da:50:63:a9:00:a1:09:75:32:3e:a7:03:

f3:c0:a9:e2:f0:db:4b:df:7f:a0:15:5d:e8:1b:97:

41:76:16:e3:8f:46:7b:74:f5:60:64:f7:17:2d:17:

cf:3f:bb:b9:15:eb:df:73:f9:72:86:6a:79:45:fc:

4b:90:01:a0:e7:98:e1:18:df:7b:e0:e4:05:3b:5b:

78:34:c6:5b:fb:1e:3c:74:1d:f5:1b:f4:60:9b:76:

f0:75:76:75:c2:f6:25:b2:35:b3:ae:e7:4c:4b:9a:

af:aa:dc:a5:d6:66:7a:28:29:28:51:34:55:c0:60:

f0:11:0e:12:f3:7b:13:f2:e1:7e:f9:a9:fd:9b:32:

e1:25:1a:d4:40:f7:0f:79:07:58:10:45:df:80:ba:

4b:c6:2a:04:e1:81:03:47:2d:8e:de:f3:cf:f5:1c:

df:f6:0e:b0:5f:d9:c5:27:1c:59:54:e4:c8:e5:2c:

9e:61

である。

1. **AES-CBCモードで岡大ロゴマークを暗号化（秘密鍵：43M22403）**

C:\Users\Owner>echo "Okayama University" | openssl rsautl -encrypt -pubin -inkey public.key > ciphertext0.txt

C:\Users\Owner>openssl aes-128-cbc -e -pbkdf2 -iter 100000 -in okayama-u.png -out ciphertext0.txt

enter aes-128-cbc encryption password:

Verifying - enter aes-128-cbc encryption password:

-公開鍵と秘密鍵を暗号化し、ciphertext0.txtに暗号文として書き出している。

非推奨の鍵導出方式を使用しているという旨の警告が出たため、ここでは-pbkdf2と-iterを用いている。-pbkdf2は、[PBKDF2](https://en.wikipedia.org/wiki/PBKDF2)というパスワードベースのキー派生関数2アルゴリズムを使用していて、-iter 100000は、パスワードの元の繰り返し回数を上書きしマニュアルページを引用している。

警告内容は以下。

\*\*\* WARNING : deprecated key derivation used.

Using -iter or -pbkdf2 would be better.

1. **上記の秘密鍵を暗号化（秘密鍵：saku33grand）**

C:\Users\Owner>openssl aes-128-cbc -e -pbkdf2 -iter 100000 -in secret.key -out ciphertext1.txt

enter aes-128-cbc encryption password:

Verifying - enter aes-128-cbc encryption password:

-秘密鍵をさらに暗号化パスワードで暗号化。Ciphertext1.txtに暗号文として書き出している。