

How to use the generic RSA functionality from the PDL crypto driver

To demonstrate encryption and decryption process you can use attached test project with precompiled **openssl** tool.

To encrypt or decrypt RSA operations you should have pair of the two keys: private and public keys.

Step by step instructions to demonstrate generic RSA functionality:

1. Go to **tools** subdirectory and open command line window
2. Generate and save private key file

```
Cmd>.\.bin\openssl genrsa 2048 > priv_key.txt
```

3. Save keys data to **my-keys.txt** file

```
Cmd>.\.bin\openssl rsa -in priv_key.txt -text > my-keys.txt
```

4. Create public key file

```
Cmd>.\.bin\openssl rsa -in priv_key.txt -pubout -out pub_key.txt
```

5. Open attached project in the PSoC Creator 4.2
6. Open **main_cm4.c** file
7. Open **my-keys.txt** file with keys information in the text viewer
8. Copy **modulus** data without leading byte

```

Lister - [c:\cy-work\temp\Use_RSA\tools\gen_rsa_key\keys.txt]
File Edit Options Encoding Help 25 %
Private-Key: (2048 bit)
modulus:
  00:d5:70:3e:86:fb:2d:fc:48:15:80:bb:ca:26:68:
  48:be:25:e9:eb:85:16:21:69:81:85:e9:f2:1c:f1:
  b4:8a:ab:b3:e6:22:c5:43:23:9b:55:df:8f:8f:a2:
  13:82:0a:c4:1e:c1:11:68:4f:de:37:05:77:a9:49:
  6a:de:09:7e:2e:a5:47:20:58:08:85:49:31:6a:b6:
  0b:d0:1e:27:f9:0f:76:88:b1:48:a5:f1:4c:f0:18:
  bb:ca:86:30:ff:cd:75:07:80:80:23:3b:f1:41:06:
  41:02:80:f5:4e:76:97:2c:d2:11:40:54:ce:59:1c:
  2d:7f:85:08:37:7c:a1:f9:e6:a6:1b:e4:30:ce:ed:
  a0:4b:40:c3:5f:85:14:cf:b6:34:64:bb:cb:f8:1b:
  88:83:4a:92:30:b2:87:7c:3b:da:ee:32:fe:b7:ea:
  12:8a:d3:3c:14:46:9f:02:77:ad:11:cd:a1:b1:7b:
  b4:78:b4:c1:0b:0d:5d:0f:f9:65:d3:83:41:9f:4d:
  01:fb:1c:9a:8d:b0:8e:3f:0e:a8:63:03:03:73:6a:
  55:5d:bd:1c:6a:78:3e:fb:62:d7:78:a1:63:c9:37:
  a4:ec:c8:78:5e:6b:d8:32:4f:a1:ac:fc:43:39:21:
  7f:c6:0f:34:8a:c4:20:0d:bd:f6:1e:ca:8a:49:51:
  7c:73
publicExponent: 65537 (0x10001)
privateExponent:
  00:b6:6b:c9:b5:3a:47:12:61:55:a7:82:59:03:3c:
  8c:37:a0:55:ee:8a:ff:e0:2c:b9:9c:07:d8:7b:ae:
  85:9d:23:a5:8d:63:58:6f:ca:a5:ff:de:24:68:21:
  a1:44:bb:08:e6:34:23:39:a1:51:8e:7b:28:cb:d2:
  48:f9:5e:e9:ae:da:6a:11:15:cc:aa:86:65:2b:0c:
  4e:ca:60:8b:cf:8d:cc:c4:85:a9:4e:d3:0e:ec:02:
  67:b6:6f:bc:b6:55:8d:da:0c:0b:f8:08:ba:60:b5:

```

- Place copied **modulus** data into text editor and make hex byte array (by some search/replace commands)

```

*new 13 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 13 new 15 new 14 new 16 Cypress.PDL.pdsc emWin.PDL.pdsc 1.bt Keil.MDK-Middleware.7.4.0.pdsc
1 0xd5, 0x70, 0x3e, 0x86, 0xfb, 0x2d, 0xfc, 0x48, 0x15, 0x80, 0xbb, 0xca, 0x26, 0x68, 0x48, 0xbe,
2 0x25, 0xe9, 0xeb, 0x85, 0x16, 0x21, 0x69, 0x81, 0x85, 0xe9, 0xf2, 0x1c, 0xf1, 0xb4, 0x8a, 0xab,
3 0xb3, 0xe6, 0x22, 0xc5, 0x43, 0x23, 0x9b, 0x55, 0xdf, 0x8f, 0x8f, 0xa2, 0x13, 0x82, 0x0a, 0xc4,
4 0x1e, 0xc1, 0x11, 0x68, 0x4f, 0xde, 0x37, 0x05, 0x77, 0xa9, 0x49, 0x6a, 0xde, 0x09, 0x7e, 0x2e,
5 0xa5, 0x47, 0x20, 0x58, 0x08, 0x85, 0x49, 0x31, 0x6a, 0xb6, 0x0b, 0xd0, 0x1e, 0x27, 0xf9, 0x0f,
6 0x76, 0x88, 0xb1, 0x48, 0xa5, 0xf1, 0x4c, 0xf0, 0x18, 0xbb, 0xca, 0x86, 0x30, 0xff, 0xcd, 0x75,
7 0x07, 0x80, 0x80, 0x23, 0x3b, 0xf1, 0x41, 0x06, 0x41, 0x02, 0x80, 0xf5, 0x4e, 0x76, 0x97, 0x2c,
8 0xd2, 0x11, 0x40, 0x54, 0xce, 0x59, 0x1c, 0x2d, 0x7f, 0x85, 0x08, 0x37, 0x7c, 0xa1, 0xf9, 0xe6,
9 0xa6, 0x1b, 0xe4, 0x30, 0xce, 0xed, 0xa0, 0x4b, 0x40, 0xc3, 0x5f, 0x85, 0x14, 0xcf, 0xb6, 0x34,
10 0x64, 0xbb, 0xcb, 0xf8, 0x1b, 0x88, 0x83, 0x4a, 0x92, 0x30, 0xb2, 0x87, 0x7c, 0x3b, 0xda, 0xee,
11 0x32, 0xfe, 0xb7, 0xea, 0x12, 0x8a, 0xd3, 0x3c, 0x14, 0x46, 0x9f, 0x02, 0x77, 0xad, 0x11, 0xcd,
12 0xa1, 0xb1, 0x7b, 0xb4, 0x78, 0xb4, 0xc1, 0x0b, 0x0d, 0x5d, 0x0f, 0xf9, 0x65, 0xd3, 0x83, 0x41,
13 0x9f, 0x4d, 0x01, 0xfb, 0x1c, 0x9a, 0x8d, 0xb0, 0x8e, 0x3f, 0x0e, 0xa8, 0x63, 0x03, 0x03, 0x73,
14 0x6a, 0x55, 0x5d, 0xbd, 0x1c, 0x6a, 0x78, 0x3e, 0xfb, 0x62, 0xd7, 0x78, 0xa1, 0x63, 0xc9, 0x37,
15 0xa4, 0xec, 0xc8, 0x78, 0x5e, 0x6b, 0xd8, 0x32, 0x4f, 0xa1, 0xac, 0xfc, 0x43, 0x39, 0x21, 0x7f,
16 0xc6, 0x0f, 0x34, 0x8a, 0xc4, 0x20, 0x0d, 0xbd, 0xf6, 0x1e, 0xca, 0x8a, 0x49, 0x51, 0x7c, 0x73
17
Normal text file length: 1567 lines: 17 Ln: 17 Col: 1 Sel: 0|0 Windows (CR LF) UTF-8 INS

```

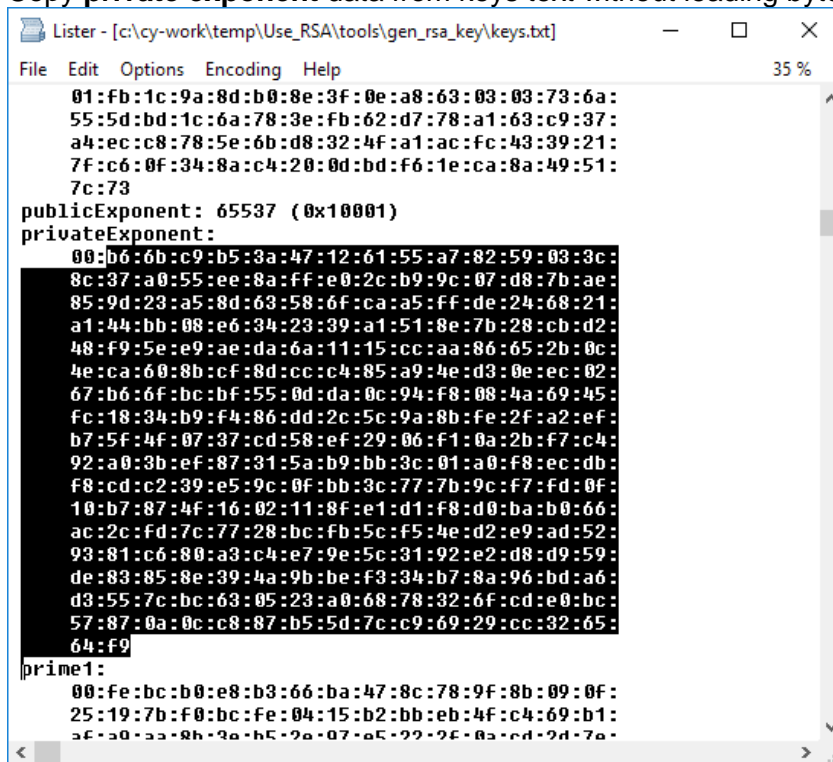
- Place this produced array to the **main_cm4.c** file into the appropriate **modulus** variable

```

30
31 /* --- PLACE KEY'S DATA GIVEN FROM openssl HERE --- */
32 uint8_t modulus[RSA_MODULO_DATA_SIZE] =
33 { /* modulus in Big-Endian for a private and public keys - see my_keys.txt */
34 /* 8< ----- BEGIN ----- >8 */
35 0xd5, 0x70, 0x3e, 0x86, 0xfb, 0x2d, 0xfc, 0x48, 0x15, 0x80, 0xbb, 0xca, 0x26, 0x68, 0x48, 0xbe,
36 0x25, 0xe9, 0xeb, 0x85, 0x16, 0x21, 0x69, 0x81, 0x85, 0xe9, 0xf2, 0x1c, 0xf1, 0xb4, 0x8a, 0xab,
37 0xb3, 0xe6, 0x22, 0xc5, 0x43, 0x23, 0x9b, 0x55, 0xdf, 0x8f, 0x8f, 0xa2, 0x13, 0x82, 0x0a, 0xc4,
38 0x1e, 0xc1, 0x11, 0x68, 0x4f, 0xde, 0x37, 0x05, 0x77, 0xa9, 0x49, 0x6a, 0xde, 0x09, 0x7e, 0x2e,
39 0xa5, 0x47, 0x20, 0x58, 0x08, 0x85, 0x49, 0x31, 0x6a, 0xb6, 0x0b, 0xd0, 0x1e, 0x27, 0xf9, 0x0f,
40 0x76, 0x88, 0xb1, 0x48, 0xa5, 0xf1, 0x4c, 0xf0, 0x18, 0xbb, 0xca, 0x86, 0x30, 0xff, 0xcd, 0x75,
41 0x07, 0x80, 0x80, 0x23, 0x3b, 0xf1, 0x41, 0x06, 0x41, 0x02, 0x80, 0xf5, 0x4e, 0x76, 0x97, 0x2c,
42 0xd2, 0x11, 0x40, 0x54, 0xce, 0x59, 0x1c, 0x2d, 0x7f, 0x85, 0x08, 0x37, 0x7c, 0xa1, 0xf9, 0xe6,
43 0xa6, 0x1b, 0xe4, 0x30, 0xce, 0xed, 0xa0, 0x4b, 0x40, 0xc3, 0x5f, 0x85, 0x14, 0xcf, 0xb6, 0x34,
44 0x64, 0xbb, 0xcb, 0xf8, 0x1b, 0x88, 0x83, 0x4a, 0x92, 0x30, 0xb2, 0x87, 0x7c, 0x3b, 0xda, 0xee,
45 0x32, 0xfe, 0xb7, 0xea, 0x12, 0x8a, 0xd3, 0x3c, 0x14, 0x46, 0x9f, 0x02, 0x77, 0xad, 0x11, 0xcd,
46 0xa1, 0xb1, 0x7b, 0xb4, 0x78, 0xb4, 0xc1, 0xb0, 0xd0, 0x5d, 0x0f, 0xf9, 0x65, 0xd3, 0x83, 0x41,
47 0x9f, 0x4d, 0x01, 0xfb, 0x1c, 0x9a, 0x8d, 0xb0, 0x8e, 0x3f, 0x0e, 0xa8, 0x63, 0x03, 0x03, 0x73,
48 0x6a, 0x55, 0x5d, 0xbd, 0x1c, 0x6a, 0x78, 0x3e, 0xfb, 0x62, 0xd7, 0x78, 0xa1, 0x63, 0xc9, 0x37,
49 0xa4, 0xec, 0xc8, 0x78, 0x5e, 0x6b, 0xd8, 0x32, 0x4f, 0xa1, 0xac, 0xfc, 0x43, 0x39, 0x21, 0x7f,
50 0xc6, 0x0f, 0x34, 0x8a, 0xc4, 0x20, 0xd0, 0xbd, 0xf6, 0x1e, 0xca, 0x8a, 0x49, 0x51, 0x7c, 0x73
51 /* 8< ----- END ----- >8 */
52 };
53

```

11. Copy **private exponent** data from keys text without leading byte



```

Listner - [c:\cy-work\temp\Use_RSA\tools\gen_rsa_key\keys.txt]
File Edit Options Encoding Help 35 %

01:fb:1c:9a:8d:b0:8e:3f:0e:a8:63:03:03:73:6a:
55:5d:bd:1c:6a:78:3e:fb:62:d7:78:a1:63:c9:37:
a4:ec:c8:78:5e:6b:d8:32:4f:a1:ac:fc:43:39:21:
7f:c6:0f:34:8a:c4:20:0d:bd:f6:1e:ca:8a:49:51:
7c:73
publicExponent: 65537 (0x10001)
privateExponent:
00:b6:6b:c9:b5:3a:47:12:61:55:a7:82:59:03:3c:
8c:37:a0:55:ee:8a:ff:e0:2c:b9:9c:07:d8:7b:ae:
85:9d:23:a5:8d:63:58:6f:ca:a5:ff:de:24:68:21:
a1:44:bb:08:e6:34:23:39:a1:51:8e:7b:28:cb:d2:
48:f9:5e:e9:ae:da:6a:11:15:cc:aa:86:65:2b:0c:
4e:ca:60:8b:cf:8d:cc:c4:85:a9:4e:d3:0e:ec:02:
67:b6:6f:bc:bf:55:0d:da:0c:94:f8:08:4a:69:45:
fc:18:34:b9:f4:86:dd:2c:5c:9a:8b:fe:2f:a2:ef:
b7:5f:4f:07:37:cd:58:ef:29:06:f1:0a:2b:f7:c4:
92:a0:3b:ef:87:31:5a:b9:bb:3c:01:a0:f8:ec:db:
f8:cd:c2:39:e5:9c:0f:bb:3c:77:7b:9c:f7:fd:0f:
10:b7:87:4f:16:02:11:8f:e1:d1:f8:d0:ba:b0:66:
ac:2c:fd:7c:77:28:bc:fb:5c:f5:4e:d2:e9:ad:52:
93:81:c6:80:a3:c4:e7:9e:5c:31:92:e2:d8:d9:59:
de:83:85:8e:39:4a:9b:be:f3:34:b7:8a:96:bd:a6:
d3:55:7c:bc:63:05:23:a0:68:78:32:6f:cd:e0:bc:
57:87:0a:0c:c8:87:b5:5d:7c:c9:69:29:cc:32:65:
64:f9
prime1:
00:fe:bc:b0:e8:b3:66:ba:47:8c:78:9f:8b:09:0f:
25:19:7b:f0:bc:fe:04:15:b2:bb:eb:4f:c4:69:b1:
a5:a0:a3:8b:3a:b5:2a:07:a5:22:2f:0a:cd:2d:7a:

```

12. Make byte array to place to the C code

```
*new 15 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 13 new 15 new 14 new 16 Cypress.PDL.pdsc emWin.PDL.pdsc 1.bt Keil.MDK-Middleware.7.4.0.pdsc
1 0xb6, 0x6b, 0xc9, 0xb5, 0x3a, 0x47, 0x12, 0x61, 0x55, 0xa7, 0x82, 0x59, 0x03, 0x3c, 0x8c, 0x37,
2 0xa0, 0x55, 0xee, 0x8a, 0xff, 0xe0, 0x2c, 0xb9, 0x9c, 0x07, 0xd8, 0x7b, 0xae, 0x85, 0x9d, 0x23,
3 0xa5, 0x8d, 0x63, 0x58, 0x6f, 0xca, 0xa5, 0xff, 0xde, 0x24, 0x68, 0x21, 0xa1, 0x44, 0xbb, 0x08,
4 0xe6, 0x34, 0x23, 0x39, 0xa1, 0x51, 0x8e, 0x7b, 0x28, 0xcb, 0xd2, 0x48, 0xf9, 0x5e, 0xe9, 0xae,
5 0xda, 0x6a, 0x11, 0x15, 0xcc, 0xaa, 0x86, 0x65, 0x2b, 0x0c, 0x4e, 0xca, 0x60, 0x8b, 0xcf, 0x8d,
6 0xcc, 0xc4, 0x85, 0xa9, 0x4e, 0xd3, 0x0e, 0xec, 0x02, 0x67, 0xb6, 0x6f, 0xbc, 0xbf, 0x55, 0xd,
7 0xda, 0x0c, 0x94, 0xf8, 0x08, 0x4a, 0x69, 0x45, 0xfc, 0x18, 0x34, 0xb9, 0xf4, 0x86, 0xdd, 0x2c,
8 0x5c, 0x9a, 0x8b, 0xfe, 0x2f, 0xa2, 0xef, 0xb7, 0x5f, 0x4f, 0x07, 0x37, 0xcd, 0x58, 0xef, 0x29,
9 0x06, 0xf1, 0x0a, 0x2b, 0xf7, 0xc4, 0x92, 0xa0, 0x3b, 0xef, 0x87, 0x31, 0x5a, 0xb9, 0xbb, 0x3c,
10 0x01, 0xa0, 0xf8, 0xec, 0xdb, 0xf8, 0xcd, 0xc2, 0x39, 0xe5, 0x9c, 0x0f, 0xbb, 0x3c, 0x77, 0x7b,
11 0x9c, 0xf7, 0xfd, 0x0f, 0x10, 0xb7, 0x87, 0x4f, 0x16, 0x02, 0x11, 0x8f, 0xe1, 0xd1, 0xf8, 0xd0,
12 0xba, 0xb0, 0x66, 0xac, 0x2c, 0xfd, 0x7c, 0x77, 0x28, 0xbc, 0xfb, 0x5c, 0xf5, 0x4e, 0xd2, 0xe9,
13 0xad, 0x52, 0x93, 0x81, 0xc6, 0x80, 0xa3, 0xc4, 0xe7, 0x9e, 0x5c, 0x31, 0x92, 0xe2, 0xd8, 0xd9,
14 0x59, 0xde, 0x83, 0x85, 0x8e, 0x39, 0x4a, 0x9b, 0xbe, 0xf3, 0x34, 0xb7, 0x8a, 0x96, 0xbd, 0xa6,
15 0xd3, 0x55, 0x7c, 0xbc, 0x63, 0x05, 0x23, 0xa0, 0x68, 0x78, 0x32, 0x6f, 0xcd, 0xe0, 0xbc, 0x57,
16 0x87, 0xa0, 0x0c, 0xc8, 0x87, 0xb5, 0x5d, 0x7c, 0xc9, 0x69, 0x29, 0xcc, 0x32, 0x65, 0x64, 0xf9
Normal text file length: 1 582 lines: 16 Ln: 6 Col: 101 Sel: 0 | 0 Windows (CR LF) UTF-8 INS
```

13. Place produced array into appropriate **privateExponent** variable in the **main_cm4.c** file

```
53
54 uint8_t privateExponent[RSA_MODULO_DATA_SIZE] =
55 {
56     /* private exponent in Big-Endian for a private key - see my_keys.txt */
57     /* 8< ----- BEGIN ----- >8 */
58     0xb6, 0x6b, 0xc9, 0xb5, 0x3a, 0x47, 0x12, 0x61, 0x55, 0xa7, 0x82, 0x59, 0x03, 0x3c, 0x8c, 0x37,
59     0xa0, 0x55, 0xee, 0x8a, 0xff, 0xe0, 0x2c, 0xb9, 0x9c, 0x07, 0xd8, 0x7b, 0xae, 0x85, 0x9d, 0x23,
60     0xa5, 0x8d, 0x63, 0x58, 0x6f, 0xca, 0xa5, 0xff, 0xde, 0x24, 0x68, 0x21, 0xa1, 0x44, 0xbb, 0x08,
61     0xe6, 0x34, 0x23, 0x39, 0xa1, 0x51, 0x8e, 0x7b, 0x28, 0xcb, 0xd2, 0x48, 0xf9, 0x5e, 0xe9, 0xae,
62     0xda, 0x6a, 0x11, 0x15, 0xcc, 0xaa, 0x86, 0x65, 0x2b, 0x0c, 0x4e, 0xca, 0x60, 0x8b, 0xcf, 0x8d,
63     0xcc, 0xc4, 0x85, 0xa9, 0x4e, 0xd3, 0x0e, 0xec, 0x02, 0x67, 0xb6, 0x6f, 0xbc, 0xbf, 0x55, 0xd,
64     0xda, 0x0c, 0x94, 0xf8, 0x08, 0x4a, 0x69, 0x45, 0xfc, 0x18, 0x34, 0xb9, 0xf4, 0x86, 0xdd, 0x2c,
65     0x5c, 0x9a, 0x8b, 0xfe, 0x2f, 0xa2, 0xef, 0xb7, 0x5f, 0x4f, 0x07, 0x37, 0xcd, 0x58, 0xef, 0x29,
66     0x06, 0xf1, 0x0a, 0x2b, 0xf7, 0xc4, 0x92, 0xa0, 0x3b, 0xef, 0x87, 0x31, 0x5a, 0xb9, 0xbb, 0x3c,
67     0x01, 0xa0, 0xf8, 0xec, 0xdb, 0xf8, 0xcd, 0xc2, 0x39, 0xe5, 0x9c, 0x0f, 0xbb, 0x3c, 0x77, 0x7b,
68     0x9c, 0xf7, 0xfd, 0x0f, 0x10, 0xb7, 0x87, 0x4f, 0x16, 0x02, 0x11, 0x8f, 0xe1, 0xd1, 0xf8, 0xd0,
69     0xba, 0xb0, 0x66, 0xac, 0x2c, 0xfd, 0x7c, 0x77, 0x28, 0xbc, 0xfb, 0x5c, 0xf5, 0x4e, 0xd2, 0xe9,
70     0xad, 0x52, 0x93, 0x81, 0xc6, 0x80, 0xa3, 0xc4, 0xe7, 0x9e, 0x5c, 0x31, 0x92, 0xe2, 0xd8, 0xd9,
71     0x59, 0xde, 0x83, 0x85, 0x8e, 0x39, 0x4a, 0x9b, 0xbe, 0xf3, 0x34, 0xb7, 0x8a, 0x96, 0xbd, 0xa6,
72     0xd3, 0x55, 0x7c, 0xbc, 0x63, 0x05, 0x23, 0xa0, 0x68, 0x78, 0x32, 0x6f, 0xcd, 0xe0, 0xbc, 0x57,
73     0x87, 0xa0, 0x0c, 0xc8, 0x87, 0xb5, 0x5d, 0x7c, 0xc9, 0x69, 0x29, 0xcc, 0x32, 0x65, 0x64, 0xf9
74     /* 8< ----- END ----- >8 */
75 };
76
```

14. Place public exponent value (value 0x10001 is a standard de-facto value for the public exponent) into **publicExponent** variable in the **main_cm4.c** file

```
76
77 /* Little endian exponent for a public key - see my_keys.txt */
78 uint8_t publicExponent[32] = { 0x01, 0x00, 0x01 };
79
```

*** Please note:**

All information produced by openssl tool are in the octet-string format (Big-Endian)!
You must revert it manually or by special revert function **Cy_Crypto_Rsa_InvertEndianness()** to the Big Integer (Little-Endian) format before using!

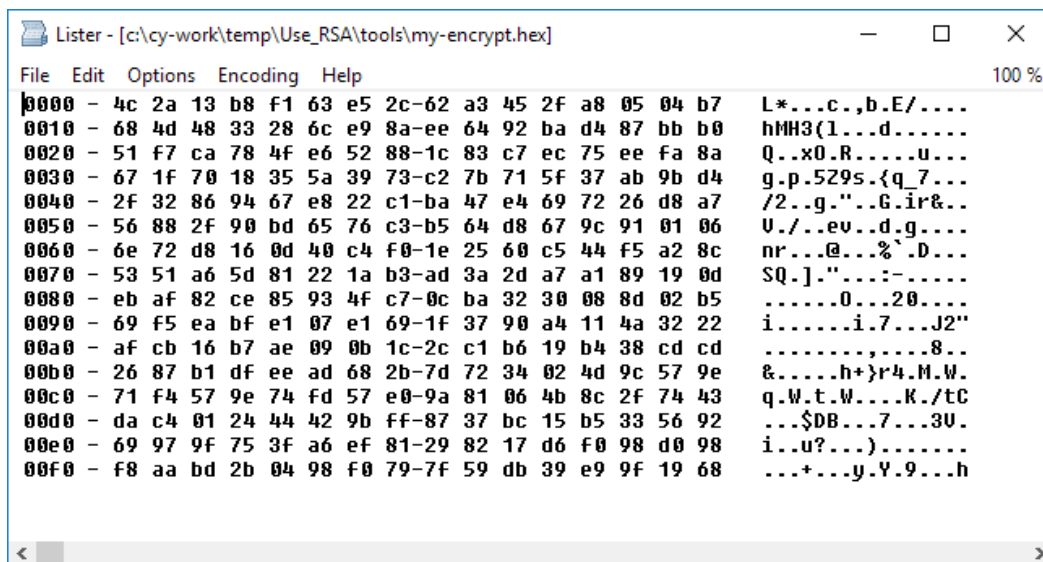
This project performs revert the key data at lines 200-201 and revert the signatures at lines 204-205.

Now all keys data and signatures are ready to use!

15. Encrypt plain text file **my-text.txt** by public key and save encrypted data to **my-encrypt.hex** file

Cmd>.\\bin\\openssl rsautl -inkey pub_key.txt -encrypt -raw -in my-text.txt -hexdump -out my-encrypt.hex

16. Open **my-encrypt.hex** file and copy encrypted data into text editor to make source code byte array



```

File Edit Options Encoding Help 100 %
0000 - 4c 2a 13 b8 f1 63 e5 2c-62 a3 45 2f a8 05 04 b7 L*...c.,b.E/....
0010 - 68 4d 48 33 28 6c e9 8a-ee 64 92 ba d4 87 bb b0 hMH3(1...d.....
0020 - 51 f7 ca 78 4f e6 52 88-1c 83 c7 ec 75 ee fa 8a Q..x0.R.....u...
0030 - 67 1f 70 18 35 5a 39 73-c2 7b 71 5f 37 ab 9b d4 g.p.529s.{q_7...
0040 - 2f 32 86 94 67 e8 22 c1-ba 47 e4 69 72 26 d8 a7 /2..g..."G.ir&..
0050 - 56 88 2f 90 bd 65 76 c3-b5 64 d8 67 9c 91 01 06 U./..ev...d.g....
0060 - 6e 72 d8 16 0d 40 c4 f0-1e 25 60 c5 44 f5 a2 8c nr...@...%`.D...
0070 - 53 51 a6 5d 81 22 1a b3-ad 3a 2d a7 a1 89 19 0d SQ.J."...:-.....
0080 - eb af 82 ce e5 93 4f c7-0c ba 32 30 08 8d 02 b5 .....0...20....
0090 - 69 f5 ea bf e1 07 e1 69-1f 37 90 a4 11 4a 32 22 i.....i.7...J2"
00a0 - af cb 16 b7 ae 09 0b 1c-2c c1 b6 19 b4 38 cd cd .....8..
00b0 - 26 87 b1 df ee ad 68 2b-7d 72 34 02 4d 9c 57 9e &.....h+}r4.M.W.
00c0 - 71 f4 57 9e 74 fd 57 e0-9a 81 06 4b 8c 2f 74 43 q.W.t.W....K./tC
00d0 - da c4 01 24 44 42 9b ff-87 37 bc 15 b5 33 56 92 ...$.DB...7...3U.
00e0 - 69 97 9f 75 3f a6 ef 81-29 82 17 d6 f0 98 d0 98 i..u?...).
00f0 - f8 aa bd 2b 04 98 f0 79-7f 59 db 39 e9 9f 19 68 ...+...y.V.9...h
  
```

17. Place produced array into the **rsaEncrypted** variable

```

79
80 /* Encrypted data from my-cipher.txt file */
81 CY_ALIGN(4) uint8_t rsaEncrypted[RSA_MODULO_DATA_SIZE] =
82 {
83     /* 8< ----- BEGIN ----- >8 */
84     0x4c, 0x2a, 0x13, 0xb8, 0xf1, 0x63, 0xe5, 0x2c, 0x62, 0xa3, 0x45, 0x2f, 0xa8, 0x05, 0x04, 0xb7,
85     0x68, 0x4d, 0x48, 0x33, 0x28, 0x6c, 0xe9, 0x8a, 0xee, 0x64, 0x92, 0xba, 0xd4, 0x87, 0xbb, 0xb0,
86     0x51, 0xf7, 0xca, 0x78, 0x4f, 0xe6, 0x52, 0x88, 0x1c, 0x83, 0xc7, 0xec, 0x75, 0xee, 0xfa, 0x8a,
87     0x67, 0x1f, 0x70, 0x18, 0x35, 0x5a, 0x39, 0x73, 0xc2, 0x7b, 0x71, 0x5f, 0x37, 0xab, 0x9b, 0xd4,
88     0x2f, 0x32, 0x86, 0x94, 0x67, 0xe8, 0x22, 0xc1, 0xba, 0x47, 0xe4, 0x69, 0x72, 0x26, 0xd8, 0xa7,
89     0x56, 0x88, 0x2f, 0x90, 0xbd, 0x65, 0x76, 0xc3, 0xb5, 0x64, 0xd8, 0x67, 0x9c, 0x91, 0x01, 0x06,
90     0x6e, 0x72, 0xd8, 0x16, 0x0d, 0x40, 0xc4, 0xf0, 0x1e, 0x25, 0x60, 0xc5, 0x44, 0xf5, 0xa2, 0x8c,
91     0x53, 0x51, 0xa6, 0x5d, 0x81, 0x22, 0x1a, 0xb3, 0xad, 0x3a, 0x2d, 0xa7, 0xa1, 0x89, 0x19, 0x0d,
92     0xeb, 0xaf, 0x82, 0xce, 0xe5, 0x93, 0x4f, 0xc7, 0x0c, 0xba, 0x32, 0x30, 0x08, 0x8d, 0x02, 0xb5,
93     0x69, 0xf5, 0xea, 0xbf, 0xe1, 0x07, 0xe1, 0x69, 0x1f, 0x37, 0x90, 0xa4, 0x11, 0x4a, 0x32, 0x22,
94     0xaf, 0xcb, 0x16, 0xb7, 0xae, 0x09, 0x0b, 0x1c, 0x2c, 0xc1, 0xb6, 0x19, 0xb4, 0x38, 0xcd, 0xcd,
95     0x26, 0x87, 0xb1, 0xdf, 0xee, 0xad, 0x68, 0x2b, 0x7d, 0x72, 0x34, 0x02, 0x4d, 0x9c, 0x57, 0x9e,
96     0x71, 0xf4, 0x57, 0x9e, 0x74, 0xfd, 0x57, 0xe0, 0x9a, 0x81, 0x06, 0x4b, 0x8c, 0x2f, 0x74, 0x43,
97     0xda, 0xc4, 0x01, 0x24, 0x44, 0x42, 0x9b, 0xff, 0x87, 0x37, 0xbc, 0x15, 0xb5, 0x33, 0x56, 0x92,
98     0x69, 0x97, 0x9f, 0x75, 0x3f, 0xa6, 0xef, 0x81, 0x29, 0x82, 0x17, 0xd6, 0xf0, 0x98, 0xd0, 0x98,
99     0xf8, 0xaa, 0xbd, 0x2b, 0x04, 0x98, 0xf0, 0x79, 0x7f, 0x59, 0xdb, 0x39, 0xe9, 0x9f, 0x19, 0x68,
100 /* 8< ----- END ----- >8 */
101 };
102 /* === PLACE KEY'S DATA GIVEN FROM openssl HERE === */
  
```

18. Open my-text.txt file in the hex viewer and copy all data

```

Lister - [c:\cy-work\temp\Use_RSA\tools\my-text.txt]
File Edit Options Encoding Help 100 %
00000000: 53 6F 6D 65 20 70 65 6F 70 6C 65 20 61 63 63 65 | Some people acce
00000010: 70 74 20 74 68 65 20 77 6F 72 6C 64 20 61 73 20 | pt the world as
00000020: 69 74 20 69 73 2E 20 54 68 65 6E 20 74 68 65 72 | it is. Then ther
00000030: 65 92 73 20 74 68 65 20 72 65 73 74 20 6F 66 20 | e's the rest of
00000040: 75 73 96 74 68 65 20 70 65 6F 70 6C 65 20 77 68 | us the people wh
00000050: 6F 20 73 65 65 20 72 6F 6D 20 66 6F 72 20 69 | o see room for i
00000060: 6D 70 72 6F 76 65 6D 65 6E 74 20 61 6E 64 20 74 | mprovement and t
00000070: 69 6E 68 65 72 20 77 69 74 68 20 77 68 61 74 20 | inker with what
00000080: 6D 6F 73 74 20 74 61 68 65 20 66 6F 72 20 67 72 | most take for gr
00000090: 61 6E 74 65 64 2E 0D 0A 0D 0A 57 65 20 73 65 65 | anted.....We see
000000A0: 20 61 20 77 6F 72 6C 64 20 6F 66 20 70 72 6F 62 | a world of prob
000000B0: 6C 65 6D 73 20 41 4E 44 20 49 54 20 49 53 20 41 | lems AND IT IS A
000000C0: 57 45 53 4F 4D 45 2E 20 50 72 6F 62 6C 65 6D 73 | WESOME. Problems
000000D0: 20 67 65 74 20 75 73 20 74 68 69 6E 68 69 6E 67 | get us thinking
000000E0: 2E 20 50 72 6F 62 6C 65 6D 73 20 70 75 73 68 20 | . Problems push
000000F0: 62 6F 75 6E 64 61 72 69 65 73 2E 2E 2E 20 0D 0A | boundaries... ..
  
```

19. Make byte array from that data and place it into **rsaDecrypted** variable. This data will be used to check correctness of the decryption operation

```

103
104 CY_ALIGN(4) uint8_t rsaDecrypted[RSA_MODULO_DATA_SIZE] =
105 /*
106 "Some people accept the world as it is. Then there's the rest of us-the people who see room"
107 " for improvement and tinker with what most take for granted.\nWe see a world of problems AND"
108 " IT IS AWESOME. Problems get us thinking. Problems push boundaries... \n"
109 */
110 {
111 /* 8< ----- BEGIN ----- >8 */
112 0x53, 0x6F, 0x6D, 0x65, 0x20, 0x70, 0x65, 0x6F, 0x70, 0x6C, 0x65, 0x20, 0x61, 0x63, 0x63, 0x65,
113 0x70, 0x74, 0x20, 0x74, 0x68, 0x65, 0x20, 0x77, 0x6F, 0x72, 0x6C, 0x64, 0x20, 0x61, 0x73, 0x20,
114 0x69, 0x74, 0x20, 0x69, 0x73, 0x2E, 0x20, 0x54, 0x68, 0x65, 0x6E, 0x20, 0x74, 0x68, 0x65, 0x72,
115 0x65, 0x92, 0x73, 0x20, 0x74, 0x68, 0x65, 0x20, 0x72, 0x65, 0x73, 0x74, 0x20, 0x6F, 0x66, 0x20,
116 0x75, 0x73, 0x96, 0x74, 0x68, 0x65, 0x20, 0x70, 0x65, 0x6F, 0x70, 0x6C, 0x65, 0x20, 0x77, 0x68,
117 0x6F, 0x20, 0x73, 0x65, 0x65, 0x20, 0x72, 0x6F, 0x6D, 0x20, 0x66, 0x6F, 0x72, 0x20, 0x69,
118 0x6D, 0x70, 0x72, 0x6F, 0x76, 0x65, 0x6D, 0x65, 0x6E, 0x74, 0x20, 0x61, 0x6E, 0x64, 0x20, 0x74,
119 0x69, 0x6E, 0x68, 0x65, 0x72, 0x20, 0x77, 0x69, 0x74, 0x68, 0x20, 0x77, 0x68, 0x61, 0x74, 0x20,
120 0x6D, 0x6F, 0x73, 0x74, 0x20, 0x74, 0x61, 0x68, 0x65, 0x20, 0x66, 0x6F, 0x72, 0x20, 0x67, 0x72,
121 0x61, 0x6E, 0x74, 0x65, 0x64, 0x2E, 0x0D, 0x0A, 0x0D, 0x0A, 0x57, 0x65, 0x20, 0x73, 0x65, 0x65,
122 0x20, 0x61, 0x20, 0x77, 0x6F, 0x72, 0x6C, 0x64, 0x20, 0x6F, 0x66, 0x20, 0x70, 0x72, 0x6F, 0x62,
123 0x6C, 0x65, 0x6D, 0x73, 0x20, 0x41, 0x4E, 0x44, 0x20, 0x49, 0x54, 0x20, 0x49, 0x53, 0x20, 0x41,
124 0x57, 0x45, 0x53, 0x4F, 0x4D, 0x45, 0x2E, 0x20, 0x50, 0x72, 0x6F, 0x62, 0x6C, 0x65, 0x6D, 0x73,
125 0x20, 0x67, 0x65, 0x74, 0x20, 0x75, 0x73, 0x20, 0x74, 0x68, 0x69, 0x6E, 0x68, 0x69, 0x6E, 0x67,
126 0x2E, 0x20, 0x50, 0x72, 0x6F, 0x62, 0x6C, 0x65, 0x6D, 0x73, 0x20, 0x70, 0x75, 0x73, 0x68, 0x20,
127 0x62, 0x6F, 0x75, 0x6E, 0x64, 0x61, 0x72, 0x69, 0x65, 0x73, 0x2E, 0x2E, 0x2E, 0x20, 0x0D, 0x0A,
128 /* 8< ----- END ----- >8 */
129 };
130
  
```

20. Set breakpoint to line 237 of the **main_cm4.c** file


```

232  /* Decrypt reverted cipher data (as Big Integer) by private key */
233  cryptoStatus = Cy_Crypto_Rsa_Proc(&cy_privateKey.keyStruct, (const uint32_t*)rsaEncrypted, sizeof(rsaEncrypted), (uint32_t *)rsaOutput, &cryptoRsaContext);
234
235  cryptoStatus = Cy_Crypto_Sync(CY_CRYPTO_SYNC_BLOCKING);
236
237  if (cryptoStatus == CY_CRYPTO_SUCCESS)
238  {
239      /* Compare reverted form of the source and result data */
240      Cy_Crypto_Str_MemCmp(rsaOutput, rsaDecrypted, RSA_MODULO_DATA_SIZE, &compareResult, &cryptoMemContextPtr);
241
242      /* Wait crypto become available */
243      Cy_Crypto_Sync(CY_CRYPTO_SYNC_BLOCKING);
244
245      if(0 != compareResult)
246      {
247          /* "Actual Result is NOT EQUAL to Expected Result" */
248          Cy_SysLib_Halt(0);
249      }
250  }
251
252  /* To use result of the RSA operation you should revert it to octet-string (Big-Endian) form */
253  Cy_Crypto_Rsa_InvertEndianness(rsaOutput, RSA_MODULO_DATA_SIZE);
254

```

21. Run project in Debug mode

22. Observe successful comparison of the **rsaDecrypted** and **rsaOutput** variables

23. Call **Cy_Crypto_Rsa_InvertEndianness()** function to revert the **rsaOutput** variable (line 253) and observe that **rsaOutput** contains the same data as plain text.

Watch 1					
Name	Value	Address	Type	Radix	
rsaOutput [256]		0x08025294 (All)	uint8_t [256]	Default	
0	0x53 'S'	0x08025294 (All)	unsigned char	Default	
1	0x6F 'o'	0x08025295 (All)	unsigned char	Default	
2	0x6D 'm'	0x08025296 (All)	unsigned char	Default	
3	0x65 'e'	0x08025297 (All)	unsigned char	Default	
4	0x20 ''	0x08025298 (All)	unsigned char	Default	
5	0x70 'p'	0x08025299 (All)	unsigned char	Default	
6	0x65 'e'	0x0802529A (All)	unsigned char	Default	
7	0x6F 'o'	0x0802529B (All)	unsigned char	Default	
8	0x70 'p'	0x0802529C (All)	unsigned char	Default	
9	0x6C 'l'	0x0802529D (All)	unsigned char	Default	
10	0x65 'e'	0x0802529E (All)	unsigned char	Default	
11	0x20 ''	0x0802529F (All)	unsigned char	Default	
12	0x61 'a'	0x080252A0 (All)	unsigned char	Default	
13	0x63 'c'	0x080252A1 (All)	unsigned char	Default	
14	0x63 'c'	0x080252A2 (All)	unsigned char	Default	
15	0x65 'e'	0x080252A3 (All)	unsigned char	Default	
16	0x70 'p'	0x080252A4 (All)	unsigned char	Default	

Please note:

To use results of the RSA encrypt/decrypt functions you should revert it to octet-string (Big-Endian) form.