Assignment - feedback

Zdeněk Říha

Assignments

1. Write a program (in any programming language) that will prepare a padded block for RSA signature with PKCS#1 v1.5 padding. Input is a file and RSA key size; output is the padded octet string (print it in hex). Use SHA-256 as the hash function. Do not use crypto library for the padding itself [5 points].

2. Write a program that will generate 2048 bit DH parameters in DER format. Use any cryptolibrary and any programming language. Recommendation: Openssl & C & functions DH_new, DH_generate_parameters_ex, i2d_DHparams_bio. [5 points].

Assignment 1

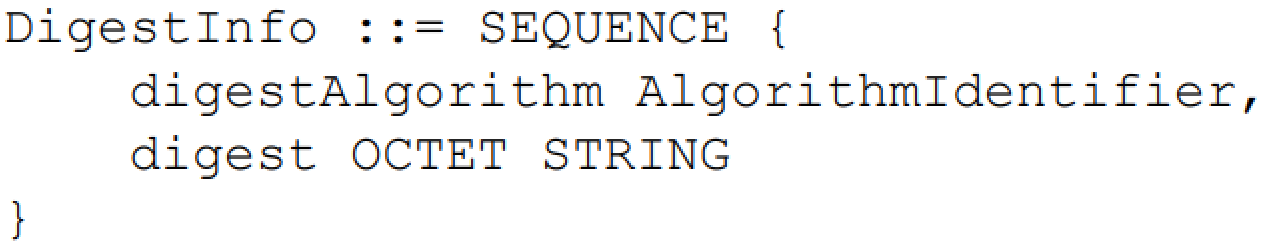
- PKCS#1 v1.5 padding
- We open the PKCS#1 v2.2 document :-)
  - Also available as RFC 8017
- We find the relevant section
  - 9.2 EMSA-PKCS1-v1_5
- EMSA-PKCS1-v1_5-ENCODE (M, emLen)
  - Input: Message + length of padded result (key size)
  - Output: EM (the padded results) to be signed

Assignment 1

- As we can see in step 5 the result is:

$$EM = 0x00 \,||\, 0x01 \,||\, PS \,||\, 0x00 \,||\, T\,.$$

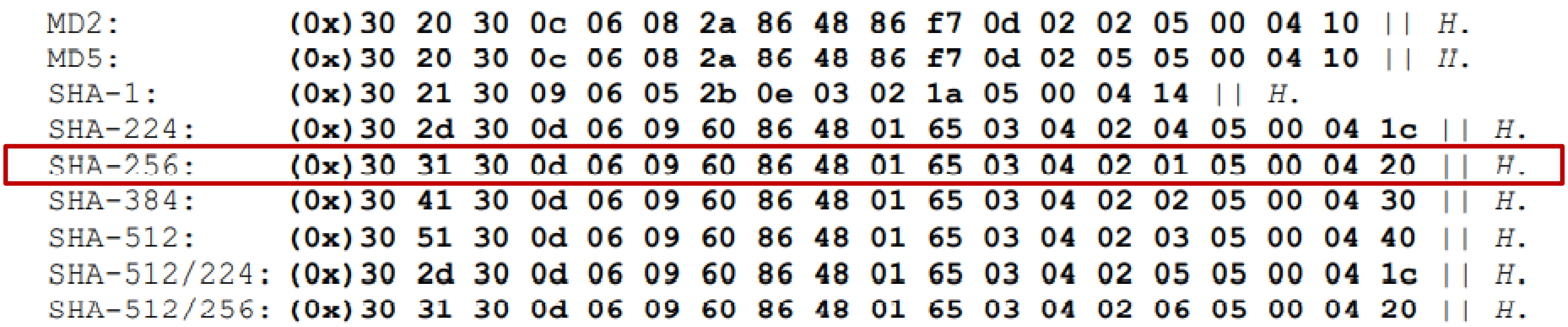
  - where PS is composed of 0xff bytes to fit the size
  - and T is DER encoded structure containing the hash algorithm and hash itself:



```
DigestInfo ::= SEQUENCE {
    digestAlgorithm AlgorithmIdentifier,
    digest OCTET STRING
}
```

Assignment 1

- The authors of PKCS#1 are very nice and provide a help for common hash algorithms



```
MD2:         (0x)30 20 30 0c 06 08 2a 86 48 86 f7 0d 02 02 05 00 04 10 || H.
MD5:         (0x)30 20 30 0c 06 08 2a 86 48 86 f7 0d 02 05 05 00 04 10 || H.
SHA-1:       (0x)30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 || H.
SHA-224:     (0x)30 2d 30 0d 06 09 60 86 48 01 65 03 04 02 04 05 00 04 1c || H.
SHA-256:     (0x)30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20 || H.
SHA-384:     (0x)30 41 30 0d 06 09 60 86 48 01 65 03 04 02 02 05 00 04 30 || H.
SHA-512:     (0x)30 51 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 04 40 || H.
SHA-512/224: (0x)30 2d 30 0d 06 09 60 86 48 01 65 03 04 02 05 05 00 04 1c || H.
SHA-512/256: (0x)30 31 30 0d 06 09 60 86 48 01 65 03 04 02 06 05 00 04 20 || H.
```

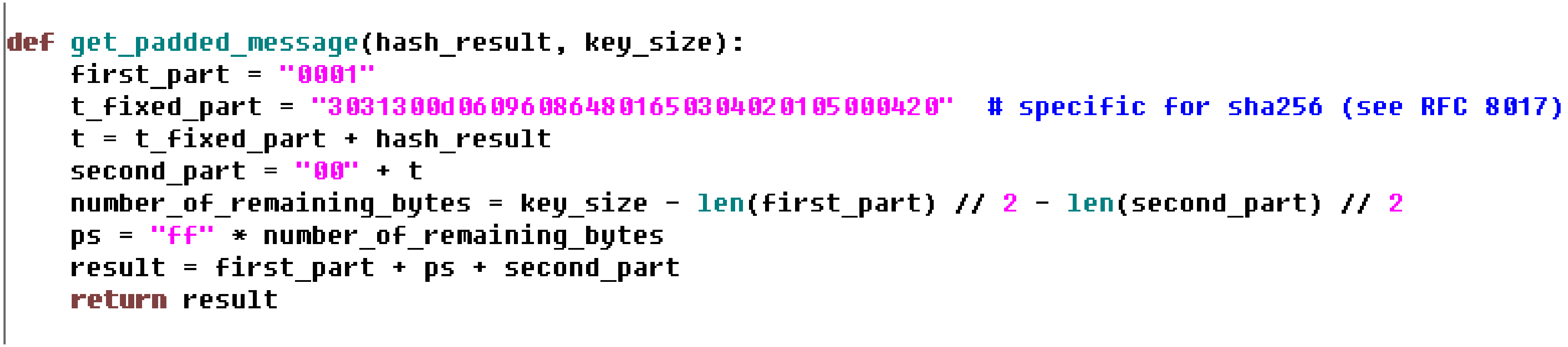
  - where H is the hash (32 bytes for SHA-256)

- Print the EM in hex

Example - result

- 0001
  fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
  fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
  fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
  fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
  ffffffffffffffffffffffffffffffffffffffff
  00
  3031300d060960864801650304020105000420
  7f5effba4da0fc825aa799e9bb3e4c50aec930e34f26e37f
  75a58fd3e26b0a38

Example - python

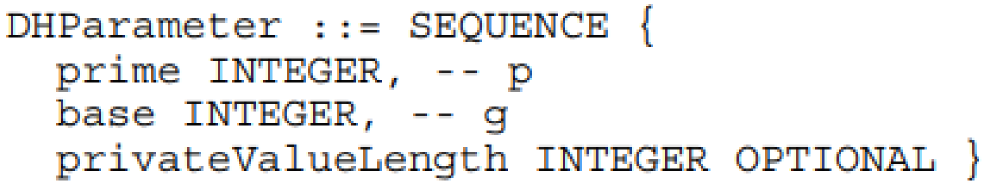


```python
def get_padded_message(hash_result, key_size):
    first_part = "0001"
    t_fixed_part = "3031300d060960864801650304020105000420"  # specific for sha256 (see RFC 8017)
    t = t_fixed_part + hash_result
    second_part = "00" + t
    number_of_remaining_bytes = key_size - len(first_part) // 2 - len(second_part) // 2
    ps = "ff" * number_of_remaining_bytes
    result = first_part + ps + second_part
    return result
```

Submitted by Oldrich Florian

Assignment 2

- Read all PKCS#3 standard
- 8 pages including introduction, history, …
- Assignment:
  - Write a program that will generate 2048 bit DH parameters in DER format.

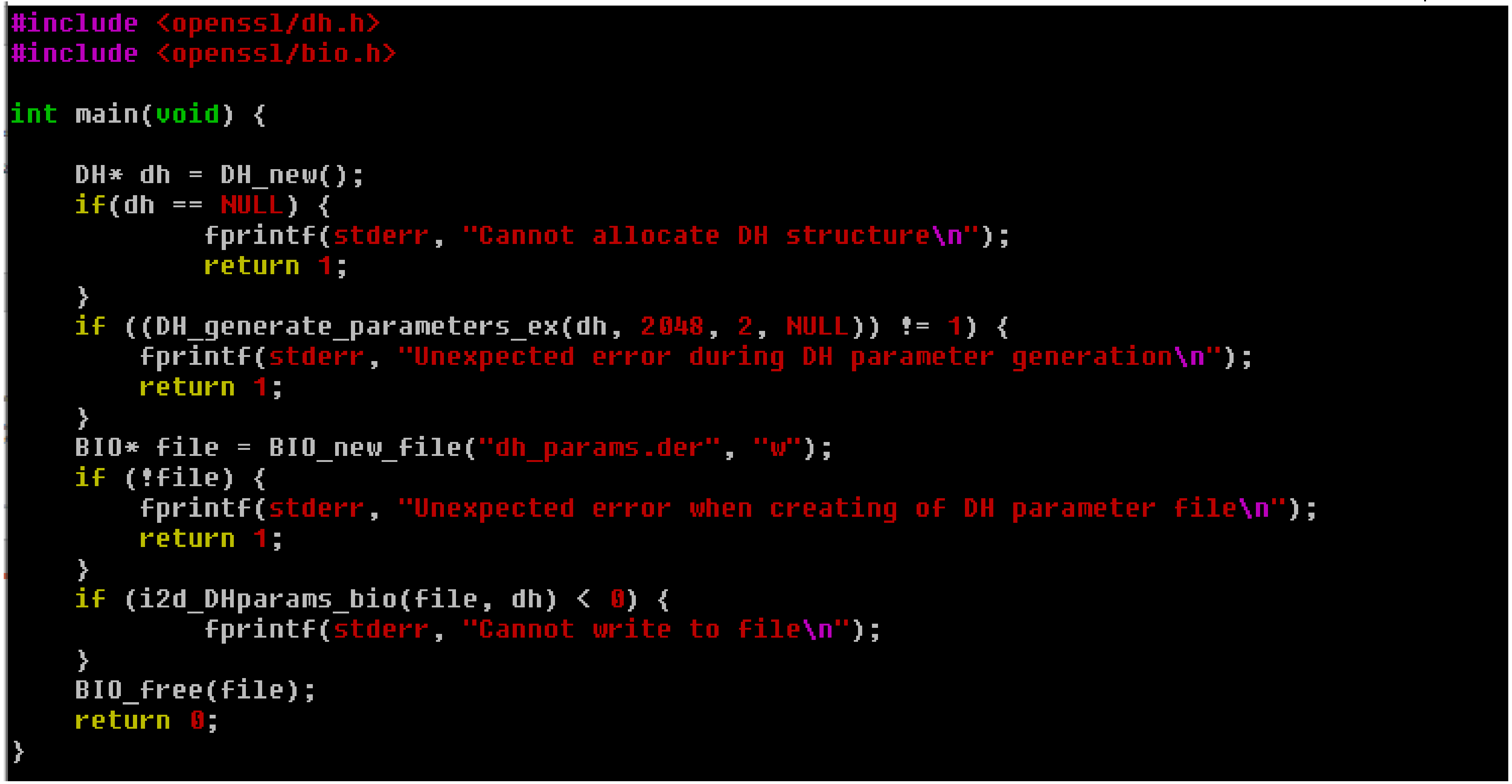


```
DHParameter ::= SEQUENCE {
  prime INTEGER, -- p
  base INTEGER, -- g
  privateValueLength INTEGER OPTIONAL }
```

Assignment 2

- Programming language
  - Use any cryptolibrary and any programming language.
  - Recommendation: Openssl & C & functions DH_new, DH_generate_parameters_ex, i2d_DHparams_bio
  - Try “man dh”
- Verify results:
  - “openssl asn1parse -inform DER -in yourfile.der”
  - “openssl dhparam -inform DER -in yourfile.der -noout -text”

Sample code in C



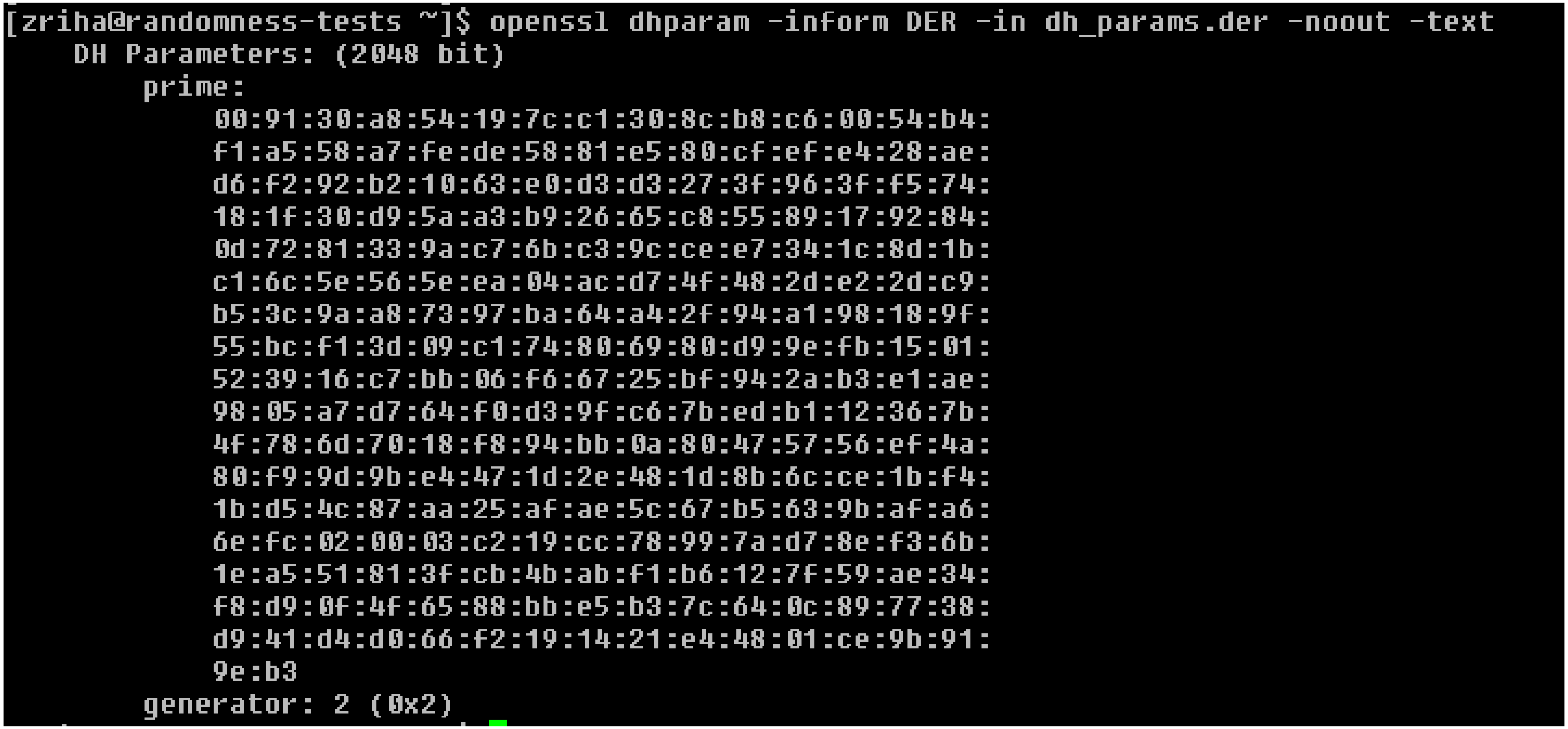
```c
#include <openssl/dh.h>
#include <openssl/bio.h>

int main(void) {

    DH* dh = DH_new();
    if(dh == NULL) {
            fprintf(stderr, "Cannot allocate DH structure\n");
            return 1;
    }
    if ((DH_generate_parameters_ex(dh, 2048, 2, NULL)) != 1) {
        fprintf(stderr, "Unexpected error during DH parameter generation\n");
        return 1;
    }
    BIO* file = BIO_new_file("dh_params.der", "w");
    if (!file) {
        fprintf(stderr, "Unexpected error when creating of DH parameter file\n");
        return 1;
    }
    if (i2d_DHparams_bio(file, dh) < 0) {
            fprintf(stderr, "Cannot write to file\n");
    }
    BIO_free(file);
    return 0;
}
```

Based on submission of Roman Chrenst

Viewing the result



```
[zriha@randomness-tests ~]$ openssl dhparam -inform DER -in dh_params.der -noout -text
    DH Parameters: (2048 bit)
        prime:
            00:91:30:a8:54:19:7c:c1:30:8c:b8:c6:00:54:b4:
            f1:a5:58:a7:fe:de:58:81:e5:80:cf:ef:e4:28:ae:
            d6:f2:92:b2:10:63:e0:d3:d3:27:3f:96:3f:f5:74:
            18:1f:30:d9:5a:a3:b9:26:65:c8:55:89:17:92:84:
            0d:72:81:33:9a:c7:6b:c3:9c:ce:e7:34:1c:8d:1b:
            c1:6c:5e:56:5e:ea:04:ac:d7:4f:48:2d:e2:2d:c9:
            b5:3c:9a:a8:73:97:ba:64:a4:2f:94:a1:98:18:9f:
            55:bc:f1:3d:09:c1:74:80:69:80:d9:9e:fb:15:01:
            52:39:16:c7:bb:06:f6:67:25:bf:94:2a:b3:e1:ae:
            98:05:a7:d7:64:f0:d3:9f:c6:7b:ed:b1:12:36:7b:
            4f:78:6d:70:18:f8:94:bb:0a:80:47:57:56:ef:4a:
            80:f9:9d:9b:e4:47:1d:2e:48:1d:8b:6c:ce:1b:f4:
            1b:d5:4c:87:aa:25:af:ae:5c:67:b5:63:9b:af:a6:
            6e:fc:02:00:03:c2:19:cc:78:99:7a:d7:8e:f3:6b:
            1e:a5:51:81:3f:cb:4b:ab:f1:b6:12:7f:59:ae:34:
            f8:d9:0f:4f:65:88:bb:e5:b3:7c:64:0c:89:77:38:
            d9:41:d4:d0:66:f2:19:14:21:e4:48:01:ce:9b:91:
            9e:b3
        generator: 2 (0x2)
```