5. homework assignment; JAVA, Academic year 2011/2012; FER

As usual, please see the last page. I mean it! You are back? OK. Here we have two problems for you to solve.

Problem 1.

You are to write a program that will allow user to encrypt/decrypt given file using AES crypto-algorithm and 128-bit encryption key or calculate and check SHA-1 file digest. Since this kind of cryptography works with binary data, use octet-stream Java based API for reading and writing of files. What needs to be programmed is illustrated by following use cases:

```
java hr.fer.zemris.java.tecaj.hw5.crypto.Crypto checksha file1.pdf
Please provide expected sha signature for file1.pdf:
> fa50c8f37ee0f77ef20149061b7414768291cb13
Digesting completed. Digest of file1.pdf matches expected digest.

java hr.fer.zemris.java.tecaj.hw5.crypto.Crypto checksha file1.pdf
Please provide expected sha signature for file1.pdf:
> da50c8f37ee0f77ef20149061b7414768291cb13
Digesting completed. Digest of file1.pdf does not match the expected digest. Digest
was: fa50c8f37ee0f77ef20149061b7414768291cb13

java hr.fer.zemris.java.tecaj.hw5.crypto.Crypto crypt file1.pdf file1.crypted.pdf
Please provide password as hex-encoded text:
> a52217e3ee213ef1ffdee3a192e2ac7e
Please provide initialization vector as hex-encoded text:
> 000102030405060708090a0b0c0d0e0f
Encryption completed. Generated file file1.crypted.pdf based on file file1.pdf.

java hr.fer.zemris.java.tecaj.hw5.crypto.Crypto decrypt file1.crypted.pdf file1.pdf
Please provide password as hex-encoded text:
> a52217e3ee213ef1ffdee3a192e2ac7e
Please provide initialization vector as hex-encoded text:
> 000102030405060708090a0b0c0d0e0f
Decryption completed. Generated file file1.pdf based on file file.crypted.pdf.
```

Please consult the following references:

http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html#MessageDigest
http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html#Cipher
http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html#MDEx
http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html#SimpleEncrEx

Encryption keys and initialization vectors are byte-arrays each having 16 bytes. In the above examples it is expected from the user to provide these as hex-encoded texts.

Implement these methods. To obtain properly initialized Cipher object, use following code snippet:

```
SecretKeySpec keySpec = new SecretKeySpec(hextobyte(keyText), "AES");
AlgorithmParameterSpec paramSpec = new IvParameterSpec(hextobyte(ivText));
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
cipher.init(encrypt ? Cipher.ENCRYPT_MODE : Cipher.DECRYPT_MODE, keySpec, paramSpec);
```

Method `hextobyte(keyText)` should take hex-encoded String and return appropriate `byte[]`. You are, of course, expected to write this method as well.

Please note, you are not allowed to use `CipherInputStream` or `CipherOutputStream` (or any of its subclasses); you are required to implement encryption/decryption directly using `Cipher` object. Also, you are not allowed to read a complete file into memory, then encrypt/decrypt it and then write the result back to disk since files can be huge. You are only allowed to read a reasonable amount of file into memory at each single time (for example, 4k). The same goes for constructing the resulting file.

Problem 2.

Download from repository file `hw05.bin` and save it in you current directory. Now run your program:

```
java hr.fer.zemris.java.tecaj.hw5.crypto.Crypto checksha hw05.bin
Please provide expected sha signature for hw05.bin:
> 4b310ed8a51c6b25e3ea178fb2a355e9a40f27c1
Digesting completed. Digest of hw05.bin matches expected digest.
```

If you obtain different result, there is something wrong; either the file `hw05.bin` is corrupted (redownload it again) or you have bug in your program (fix it). When you do obtain result as expected, run following command:

```
java hr.fer.zemris.java.tecaj.hw5.crypto.Crypto decrypt hw05.bin hw05-2.pdf
Please provide password as hex-encoded text:
> a52217e3ee213ef1ffdee3a192e2ac7e
Please provide initialization vector as hex-encoded text:
> 000102030405060708090a0b0c0d0e0f
Decryption completed. Generated file hw05-2.pdf based on file hw05.bin.
```

Open the file you just generated, read it and proceed as instructed by the text in that file.

Please note. You can consult with your peers and exchange ideas about this homework *before* you start actual coding. Once you open you IDE and start coding, consultations with others (except with me) will be regarded as cheating. You can not use any of preexisting code or libraries for this homework (whether it is yours old code or someones else). Document your code!

In order to solve this homework, create a blank Eclipse Java Project and write your code inside. Once you are done, export project as a ZIP archive and upload this archive on Ferko before the deadline. Do not forget to lock your upload or upload will not be accepted.