Team Project #2 – HMAC-SHA1

Max Score: 100 pts, Due: Thurs 12/06/18

Again, this is a team project. It is to create HMAC-SHA1 message authentication tags with various input formats.

The C source code for the hash function SHA1is given on Blackboard [Proj02_sha1.c.zip], which is a slightly modified version from https://www.di-mgt.com.au/src/sha1.c.txt We need you to implement a HMAC-SHA1 message authentication tag generating function based on the formula given in the lecture:

$$t = \text{HMACSHA1}(k, x) = \text{SHA1}[\ (k^{+} \oplus \text{opad})\ \|\ \text{SHA1}(\ (k^{+} \oplus \text{ipad})\ \|\ x\ )\ ]$$

where t is the generated tag, k is the secret key, and x is the message.

You will be making two functions as specified below, one for generating a tag for a string, the other for generating a tag for a given file (in any format, say, pdf, docx, exe, txt, jpeg, etc.).

```
/**
  * \brief   HMAC-SHA1 message authentication code for a string / file
  * \param msg     input string
  * \param key    input key
  * \param inFile   input file name
  * \param mode    control input parameter types
  * \return    generated tag
  */
 unsigned char* Hmacsha1_str( unsigned char* key, unsigned char* msg, int mode );

 unsigned char* Hmacsha1_file( unsigned char* key, char* inFile, int mode );
```

When mode = 0, the type for msg and key is string; mode = 1, the type for msg and key is hex; mode = 2, the type for msg and key is base-64. Returned tag always uses hex format.

Make sure your project gives the correct results with various test vectors. For example, if both secret key and msg are strings, the call to Hmacsha1_str( ) and the generated tag are:

```
Hmacsha1_str("key", "The quick brown fox jumps over the lazy dog", 0);
```

```
de7c9b85b8b78aa6bc8a7a36f70a90701c9db4d9
```

You should test other test vectors with your code, and then compare your results with the ones from your favorite online HMAC calculators.

Submission: Each team only needs to have one submission, it includes the following:

1 Source code: put all source code files into one folder and zip it to TeamName_Hmacsha1.zip. Before submission, make sure you code can generate tags correctly.

2. Technical report in pdf as TeamName_Hmacsha1.pdf, which includes

1) title page include team name, team members names;
2) Various test vectors and their results in different modes;
3) Techinical difficulties you've encountered while doing the project and the solutions to these technical difficulties;
4) What you have learned from doing this project.