Algorithm implementation

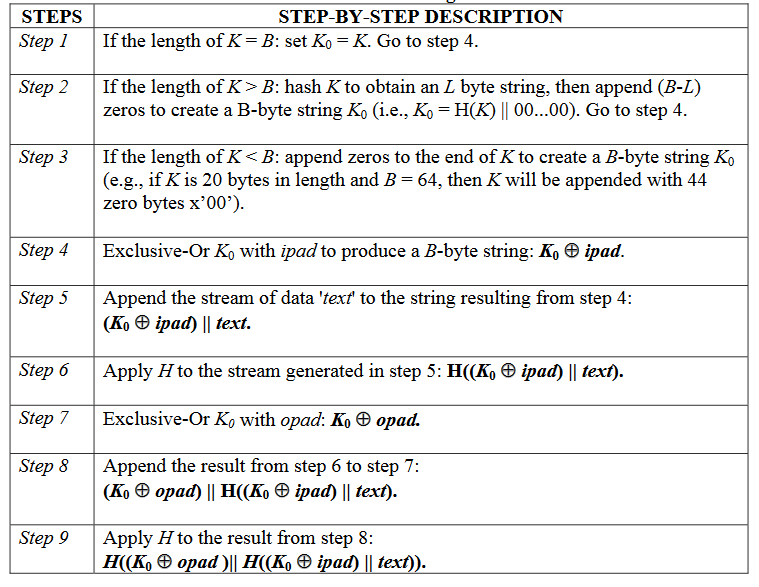
The student needs to implement the algorithm according to the given description, and the scoring shall be based on,

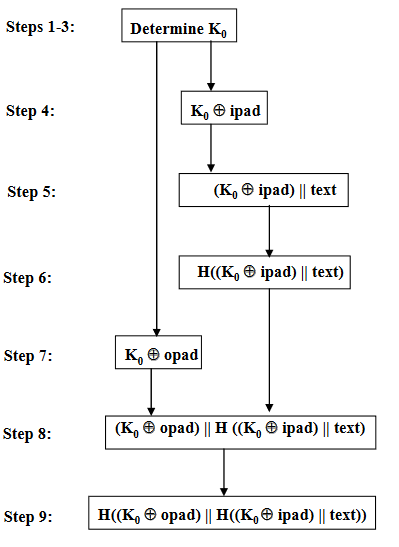
1. Passing test vector
2. Clean Code
3. Code documentation

Note:

1. H: SHA2-256 shall be used.

|  |  |
| --- | --- |
| B | Block size (in bytes) of the input to the Approved hash function. |
| H | Approved hash function. |
| ipad | Inner pad; the byte x'36' repeated B times. |
| K | Secret key shared between the originator and the intended receiver(s). |
| K0 | The key K after any necessary pre-processing to form a B byte key. |
| L | Block size (in bytes) of the output of the Approved hash function. |
| opad | Outer pad; the byte x'5c' repeated B times. |
| text | The data on which the Function shall calculate; text does not include the padded key.  The length of text is n bits, where |
| x’N’ | Hexadecimal notation, where each symbol in the string 'N' represents 4 binary bits |
| || | Concatenation |
|  | Exclusive-Or operation. |





**Test Vectors:**

Key: 0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b (32 bytes)

Data: 4869205468657265

Output from the algorithm: 198a607eb44bfbc69903a0f1cf2bbdc5ba0aa3f3d9ae3c1c7a3b1696a0b68cf7