Homework 1

- Honor Code: You must work completely independently on this assignment. Do not discuss the questions or answers with each other before the assignment is due. Any breach of the honor code will be handled per the University's policy on academic honesty.
- You may need to write a program to answer some questions. If so, you must use the Java program in the appendix as a reference. Do not external Java libraries.
- Follow the instructions very careful. Answers that do not conform to the instructions will not be given credit.
- Submit your answers through Blackboard as a PDF only.

1. Find a collision in each of the hash functions below:
    a. H(x) = x mod 7^{12}, where x can be any integer
    b. H(x) = number of 1-bits in x, where x can be any bit string
    c. H(x) = the three least significant bits of x, where x can be any bit string
2. Prove the statement: In a class of 500 students, there must be two students with the same birthday.
3. Find an x such that H (x ◦ id) ∈ Y where
    a. H = SHA-256
    b. id = 0xED00AF5F774E4135E7746419FEB65DE8AE17D6950C95CEC3891070FBB5B03C77
    c. Y is the set of all 256 bit values that have some byte with the value 0x1D.

    Assume SHA-256 is puzzle-friendly. Your answer for x must be in hexadecimal. You may provide your code for partial credit, if your x value is incorrect. You may use the accompanying CryptoReference1.java file to help you with this question. Submit both your code and your value of x.

    Notes:
    - The notation "x ◦ id" means the byte array x concatenated with the byte array id. For example, "11110000 ◦ 10101010" is the byte array "1111000010101010".
    - The following two code segments are **not** equivalent:

Segment 1	**Segment 2**

`String val = "0x4E4135E7746419FEB0";`
 	
`if (val.contains("1D")) return true;`
	`String val = "0x4E4135E7746419FEB0";`
	
	`byte[] arr = val.getBytes();`
	`for (byte b : arr)`
	`  if (b == 0x1D) return true;`

    The second code segment above is the correct way to check whether 0x1D is a byte in 0x4E4135E7746419FEB0. Remember that hex format is only a way to represent a byte sequence in a human readable format. You should not be performing operations directly on hex-string representations. Instead, you should first convert hex-strings into byte arrays, then perform operations on the byte arrays directly, and then convert the final byte array into a hex format when giving your answer. Performing operations directly on the hex strings is incorrect.

4. Alice and Bob want to play a game over SMS text where Alice chooses a number between 1 and 10 in her head, and then Bob tries to guess that number. If Bob guesses correctly, he wins. Otherwise, Alice wins. However, Bob complains that the game isn't fair, because even if Bob guessed correctly, Alice could lie and claim that she chose a different number than what she initially chose. What can Alice do to prove that she didn't change the number she initially chose? Devise a mechanism to address Bob's concern. Provide a detailed explanation of the mechanism and why it works. An answer with insufficient detail will not receive credit.