Problem Set 1

Submit your answers in a simple text file or as a link to a google doc with public access.

1. Find a collision in each of the hash functions below:
    a. $H(x) = x^2 \bmod 9$, where x can be any integer
    b. H(x) = number of 0-bits in x, where x can be any bit string
        i. Note: a "bit string" is simply a sequence of 0s and 1s
        ii. For example, 01011011 is a bit-string
    c. H(x) = the three least significant bits of x, where x is a 32-bit integer.

2. Implement a program to find an x such that $H(x \circ id) \in Y$ where
    a. H = SHA-256
    b. id = 0xED00AF5F774E4135E7746419FEB65DE8AE17D6950C95CEC3891070FBB5B03C78
    c. Y is the set of all 256 bit values that have some byte with the value 0x2F.
    d. Assume SHA-256 is puzzle-friendly. Your answer for x must be in hexadecimal.
    e. Use must use the Rust programming language, as it is a critical language in blockchain:
        i. Use the following Rust crates:
            1. https://crates.io/crates/hex
            2. https://crates.io/crates/sha2
            3. https://crates.io/crates/rand
    f. **Caution**:
        i. The notation "x ◦ id" means the byte array x concatenated with the byte array id. For example, 11110000 ◦ 10101010 is the byte array 1111000010101010.
        ii. The following two code segments are not equivalent:

INCORRECT	**CORRECT**

`let id_hex = "1D253A2F";`
 	
`if id_hex.contains("1D") {`
`  return;`
`}`
	`let id_hex = "1D253A2F";`
	
	`let decoded = hex::decode(id_hex).expect("Decoding failed");`
	`let u = u8::from(29); //29 in decimal is 0x1d in hex`
	`if decoded.contains(&u) {`
	`  return;`
	`}`

The second code segment above is the correct way to check whether 0x1D is a byte in 0x1D253A2F. Remember that hex format is only a way to represent a byte sequence in a human readable format. You should never perform 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.

3. Alice and Bob want to play the game called "rocks-paper-scissors" over SMS text. Their game play is asynchronous in the sense that they can't expect the other person to be available at a certain time or within a certain time window. Design a protocol that enables Alice and Bob to play the game fairly and prevents the possibility of cheating. Provide a detailed explanation of the mechanism and why it works. An answer with insufficient detail will not receive credit. You should only need to use cryptographic hash functions to solve this problem. Keep the solution simple.