Cryptographic Engineering: Assignment 1 Prelab

1. Compute the residue of $a = 2^{30} - 18 = 1073741806 =$ {`0x3FFFFFEE`} over the following numbers **using the method you learned in class.** Show your work. Then verify your results using SageMath. Show all results in Hexadecimal.
   (a) $p_1 = 2^{17} - 1 =$ {`0x1FFFF`} (Mersenne prime)
   (b) $p_2 = 2^{26} - 5 =$ {`0x3FFFFFB`} (Pseudo-mersenne prime)
   (c) $b = 2^{16} =$ {`0x10000`} (Not a prime number)
2. In class, you learned two methods to compute the multiplicative inverse of an operand over a finite field; Fermat's Little Theorem (FLT) and Extended Euclidean Algorithm (EEA). The finite field is constructed over $p = 2^{17} - 1$ (Mersenne prime from the previous exercise). Compute the multiplicative inverse of $a = 51$ over $\mathbb{F}_p$ using the below methods. Show your work. Then verify your results using SageMath. Show all results in Hexadecimal.
   (a) Fermat's Little Theorem (FLT)
   (b) Extended Euclidean Algorithm (EEA)
3. In Exercise 2, you applied two methods to compute the multiplicative inverse of an operand over a finite field. Answer the following questions related to these 2 methods:
   (a) How many loop iterations does it take to compute the output for each method for $a = 51$ (exercise 2)?
   (b) Which method is faster in general? Why?
   (c) Which method is constant time (aka the number of iterations is the same independent of the input used)? Why?