Name:

Math 424: Practice exam

This practice exam is not meant to be comprehensive. Rather, it is meant to complement the prior exams and the textbook problems.

1. Compute $\varphi(667)$.
2. Solve $25x \equiv 1 \pmod{667}$ for x. Find the smallest nonnegative solution.
3. Suppose p_1, p_2, p_3, p_4, p_5 are 5 distinct odd primes. Consider the 5-bit hash h whose domain is $\{n \in \mathbb{Z} : p_i \nmid n \forall i\}$, given by
$$h(n) = \left(\frac{1}{2}\left(\frac{n}{p_1}\right) + 1, \ldots, \frac{1}{2}\left(\frac{n}{p_5}\right) + 1\right),$$
where $\left(\frac{n}{p_i}\right)$ denotes the Legendre symbol.
   (a) Show that h is not strongly collision resistant.
   (b) Suppose each p_i is $\equiv 5 \pmod 8$. Construct an algorithm which, given $y \in \{0,1\}^5$, finds n such that $h(n) = y$. You can write it in Python, or just describe each step in words. Make sure each step is a calculation we know how to do. Explain why it works.
4. The hash function H outputs 3-bit hashes as follows:
   1. Given a bit string, append zeroes to the bit string until the length of the string is a multiple of 3. (If the length was a multiple of 3 to begin with, do nothing.)
   2. Break the bit string into groups of length 3.
   3. Take the XOR sum of all of the groups.
   4. The sum is the value of the hash function.

   (a) Show that H is not collision-resistant.
   (b) Show that H is not preimage resistant.
5. The hash function h produces 128-bit hashes.
   (a) Eve has a file X and knows the hash $h(X)$. She wishes to find a *different* file Y with the same hash value. How many different files does she have to try before finding one with the same hash as X, with probability $\geq 50\%$?
   (b) Suppose instead Eve wants to find *any* two files Y and Z which are different, but have the same hash value. How many files does she need to check to succeed with probability $\geq 50\%$? You may give an approximate value.
6. Alice is using RSA signatures. The verification key is $(551, 101)$.
   (a) Find a message whose signature is 550.
   (b) Compute the signature of $m = 4$.
7. In a $(3, 5)$ Shamir secret sharing scheme, we have $p = 11$, and 3 of the shares are
$$(1, 1), (2, 10), (3, 0).$$
What is the secret?