Programming Problems

Write a computer program that defines functions for 3 of the following 4 problems. You may use the language of your choice. Submit your source code as well as a text file of sample runs on a variety of inputs, including at least the examples given below. Use the CS200 submit script to submit both files. You will need to use the submit script twice for the two files. Indicate the same amount of time for both submissions.

If you search online for extra help, be sure you are searching for language features (e.g., how to delete from a list in Python) rather than code that answers the problem you are solving. Acknowledge (e.g., in comments) any sources that you do use. If you worked with someone else, including the TAs or the professor, please list their names for each problem as appropriate as well.

1. Given integers \( n \) and \( b \), each greater than 1, find the base \( b \) expansion of \( n \). You can assume \( 1 < b \leq 10 \).

Examples:

```python
>>> expand(0,2)
''
>>> expand(1,2)
'1'
>>> expand(2,2)
'10'
>>> expand(10,2)
'1010'
>>> expand(100,2)
'1100100'
>>> expand(10,3)
'101'
>>> expand(100,3)
'10201'
>>> expand(100,10)
'100'
```

2. Implement the Sieve of Eratosthenes to return all prime numbers less than or equal to a given value \( n \). Examples:

```python
>>> sieve(1)
[]
>>> sieve(59)
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59]
```

3. Given a positive integer \( m \), find the prime factorization of \( m \).

Examples:
>>> factor(1)
[]
>>> factor(30)
[2, 3, 5]
>>> factor(97)
[97]
>>> factor(2016)
[2, 2, 2, 2, 3, 3, 7]

4. Given a message $M$, an integer $n = pq$ where $p$ and $q$ are odd primes, and an integer $e > 1$ relatively prime to $(p - 1)(q - 1)$, encrypt message $M$ using the RSA cryptosystem with key $(n, e)$. Use the RSA Encryption algorithm described in class and in Section 4.6 of the Rosen text. Example with message $M = 'STOP'$ and encryption key $(n, e) = (2537, 13)$:

```python
>>> encrypt('STOP', 2537, 13)
[2081, 2182]
```

5. **Optional:** Given a message $C$ encrypted using the RSA cryptosystem with key $(n, e)$ and associated decryption key $(n, d)$, decrypt $C$ to reveal the original message. Example with encrypted message $C = \{981, 461\}$ and decryption key $(n, d) = (2537, 937)$:

```python
>>> decrypt([981, 461], 2537, 937)
'HELP'
```

Try encrypted message $C = \{649, 2640, 519, 1542, 439\}$ and decryption key $(n, d) = (3233, 2753)$.

6. Approximately how many hours did you spend on this assignment, including reading?