The RSA Algorithm is described as follows:

Alice: Key Generation:

1. Choose two large primes p and q.
2. Compute $n = pq$.
3. Compute $\phi(n) = (p-1)(q-1)$.
4. Select a public exponent e, where $1 \leq e \leq \phi(n) - 1$ and $\gcd(e, \phi(n)) = 1$.
5. Compute private exponent d such that $ed \equiv 1 \pmod{\phi(n)}$.
6. Alice's public key is (n, e) and her private key is d.

Bob: RSA Encryption

1. Convert message to an integer m, where $1 \leq m \leq n$.
2. Compute $c = m^e \pmod{n}$.
3. The encrypted message is c. Bob sends c to Alice.

Alice: RSA Decryption

1. Compute $m' = c^d \pmod{n}$.
2. The decrypted message is $m' = m$.

Exercises

(1) Using $p = 79$, $q = 101$, $e = 17$, $m = 129$. Execute the RSA key generation, encryption, and decryption algorithm.

(2) Similar to the previous problem, now use $p = 194767$, $q = 235439$, $e = 63953$, $m = 31234632$.

(3) Let $p = 89$ and $q = 101$. Is $e = 15$ a valid RSA public exponent? Explain.

(4) Work in pairs, each team member take turns being Alice and Bob.

(5) Now assume you are an attacker on an RSA scheme. You obtain the ciphertext $c = 24626$ through eavesdropping. The public key is known to be $(n, e) = (30551, 41)$. Can you find the original message?

(6) Similarly as in the previous problem, now use

$$
\begin{aligned}
n &= 22803\ 52281\ 54095\ 46543\ 55619\ 44751\ 38110\ 92893\ 89054\ 58640\ 64408\\
&\quad\ 67470\ 33782\ 15846\ 74118\ 16282\ 10797\ 92085\ 41\\
e &= 19\\
c &= 70001
\end{aligned}
$$

(a) What makes it so difficult to reveal the message m?

(b) What is needed to evaluate the private key d? Use the examples in the previous questions to investigate.

(c) Comment on the security of this encryption system.