MCS 425: Codes and Cryptography (Spring 2020)
Homework 3

Due in class, Friday, Feb 28

The RSA algorithm:

1) In the RSA algorithm, suppose the public key (n, e) is $n = 55$ and $e = 3$. Given the factorization of $n = 5 \cdot 11$, find the private key d.

2) Write code for the RSA algorithm.

   Assume p, q, and e are given to you. You need to implement the following functions:

   - *generate_key*: Given p, q, and e, compute the decryption exponent d.
   - *encrypt*: Given n, e, and the plaintext m, compute the ciphertext c.
   - *decrypt*: Given n, d, and the ciphertext c, compute the plaintext m.

   You can use the following functions **without** implementing them:

   - *extended_gcd*: Given a and b, return two integers x and y such that $ax + by = \gcd(a, b)$.
   - *modular_exp*: Given a, b, and n, return $a^b \bmod n$.

3) Prove the correctness of the RSA algorithm, that is, $m^{de} \equiv m \pmod{n}$ for all $1 \leq m < n$.

Primality testing and factoring:

4a) Given that $3^{1726} \equiv 1587 \pmod{1727}$ and $3^{1728} \equiv 1 \pmod{1729}$, what do you know about the primality of 1727 and 1729?

4b) Using the fact that $1239^2 \equiv 121100 \pmod{202003}$ and $1318^2 \equiv 121100 \pmod{202003}$, find a non-trivial factor of 202003.

Discrete logarithms, Diffie-Hellman key exchange, and ElGamal encryption:

5) Suppose you know that 137 is a prime and 3 is a primitive root of 137, $3^6 \equiv 44 \pmod{137}$, and $3^{10} \equiv 2 \pmod{137}$. Solve the discrete logarithm problem $3^x \equiv 11 \pmod{137}$.

6a) In Diffie-Hellman key exchange, Alice and Bob agree on a (public) prime $p = 13$ and primitive root $g = 2$. Suppose Alice's secret exponent is $a = 8$ and Bob's secret exponent is $b = 4$. What numbers Alice and Bob send back and forth, and what is the key they agreed on?

6b) In the ElGamal cryptosystem, Alice and Bob use $p = 17$ and $g = 3$. Alice chooses her secret to be $a = 6$, so $g^a \bmod p = 3^6 \bmod 17 = 15$. Alice publishes $(p, g, g^a \bmod p) = (17, 3, 15)$.

Suppose Bob sends Alice the ciphertext $(7, 6)$. That is, he chooses a secret $1 \leq b \leq p - 1$ and tells Alice that $g^b \equiv 7 \pmod{p}$ and $c = 6 \equiv (g^a)^b \cdot m \pmod{p}$. Determine the plaintext m.