MCS 425: Codes and Cryptography (Fall 2020)

Homework 3

Due at 12:00pm CDT, Monday, Nov 2

1. In the RSA algorithm, suppose the public key (n, e) is $n = 77$ and $e = 13$. Given the factorization $n = 7 \cdot 11$, find the private key d by hand.

2. Alice receives a ciphertext $c = 3$ encrypted by the RSA algorithm. Alice's public key is $(n, e) = (85, 57)$ and her private key is $d = 9$. Find the plaintext by hand.

3. In the lecture, we proved the correctness of the RSA algorithm under the assumption that $\gcd(m, n) = 1$. Prove the correctness of the RSA algorithm without this assumption, that is, $m^{de} \equiv m \pmod{n}$ for all $1 \leq m < n$. (Hint: use the Chinese remainder theorem.)

4. Suppose we know that $3^{1540} \equiv 1 \pmod{1541}$, $4^{1540} \equiv 967 \pmod{1541}$, $3^{1728} \equiv 1 \pmod{1729}$, and $4^{1728} \equiv 1 \pmod{1729}$. What can we say about the primality of 1541 and 1729 using Fermat's primality test?

5. 401 is a prime and 3 is a primitive root of 401. Given that $3^{246} \equiv 44 \pmod{401}$ and $3^{26} \equiv 2 \pmod{401}$, solve the discrete logarithm $3^x \equiv 11 \pmod{401}$ by hand using index calculus.

6. In Diffie-Hellman key exchange, Alice and Bob agree on a (public) prime $p = 11$ and primitive root $g = 2$. Suppose Alice's secret exponent is $a = 3$ 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?

7. In the ElGamal encryption, Alice and Bob use $p = 19$ and $g = 3$. Alice chooses a secret $a = 6$ and computes $g^a \bmod p = 3^6 \bmod 19 = 7$. Alice publishes $(p, g, g^a \bmod p) = (19, 3, 7)$.

   Suppose Bob sends Alice the ciphertext $(g^b \bmod p, c) = (16, 4)$. That is, he tells Alice that $g^b \equiv 16 \pmod{p}$ and $c = 4 \equiv (g^a)^b \cdot m \pmod{p}$. Find the plaintext m. Show your work.

8. Implement the RSA algorithm and the Diffie-Hellman key exchange.

   Suppose in RSA, Alice chooses $n = 305647189 = 17393 \cdot 17573$ and $e = 254071759$. Use your code to compute Alice's secret key and then decrypt the ciphertext 116142292.

   Suppose in the Diffie-Hellman key exchange, Alice and Bob use $p = 4252019$ and $g = 79$. Suppose Alice's secret exponent is $a = 3141592$ and Bob's secret exponent is 535897. Use your code to compute the number Alice sends to Bob, and then compute (from Bob's perspective) the secret key that they agree on.

   (You only need to answer 4 integers for this question. You may reuse your code from HW2.)