Math 4981 Spring 2021
Cryptography HW 7 Solutions
Due Thursday, March 4

1. Let m be an integer, and let x be an integer with $\gcd(x, m) = 1$. Prove that $x^{\phi(m)-a}$ is an inverse of x^a mod m.

   Solution: We see that $x^{\phi(m)-a}x^a = x^{\phi(m)-a+a} = x^{\phi(m)} \equiv 1 \mod m$, so by definition $x^{\phi(m)-a}$ is an inverse of x^a mod m.

2. (a) What is $\phi(3^2)$? What is $\phi(3^3)$?

   (b) What is $\phi(5^2)$? What is $\phi(5^3)$?

   (c) Let p be a prime number. Find and prove a formula for $\phi(p^n)$.

   Solution:

   i. $\phi(3^2) = 6$ and $\phi(3^3) = 18$.

   ii. $\phi(5^2) = 20$ and $\phi(5^3) = 100$.

   iii. We want to know which numbers are relatively prime to p^n. The only way to have a common factor with p^n is to be divisible by p, so $1/p$ of the possible numbers have a common factor. Thus $p^n/p = p^{n-1}$ numbers have a common factor with p, so $(p-1)p^{n-1}$ numbers will be relatively prime to p^n. Thus $\phi(p^n) = (p-1)p^{n-1}$.

3. Compute:

   (a) $\text{ord}_{13} 5$

   (b) $\text{ord}_{13} 7$

   (c) $\text{ord}_{13} 2$

   (d) $\text{ord}_{127} 2$

   Solution:

   (a) $5, 12, 8, 1$ so $\text{ord}_{13} 5 = 4$.

   (b) $7, 10, 5, 9, 11, 12, 6 \ldots$ so $\text{ord}_{13} 7 = 12$.

   (c) $2, 4, 8, 3, 6, 12, 11 \ldots$ so $\text{ord}_{13} 2 = 12$.

   (d) $2, 4, 8, 16, 32, 64, 1$ so $\text{ord}_{127} 2 = 7$.

4. (a) What is the inverse of 19 mod 96?

(b) Use your answer in part (a) to solve the congruence $x^{19} \equiv 36 \mod 97$.

Solution:

(a) $19 \cdot 5 = 95 \equiv -1 \mod 96$ so $-5 \equiv 91$ is the inverse of 19 mod 96.

(b)

$$\begin{aligned} x^{19} &\equiv 36 \mod 97 \\ (x^{19})^{91} &\equiv 36^{91} \mod 97 \\ x &\equiv 36 \mod 97. \end{aligned}$$

5. Supppose Alice and Bob are using the prime $p = 1373$ and the base $g = 2$ for an ElGamal cryptosystem.

   (a) Alice chooses $a = 947$ as her private key. What is the value of her public key A?

   (b) Now suppose Bob chooses $b = 716$ as his private key, and thus his public key is $469 \mod 1373$. Alice encrypts the message $m = 583$ using the ephemeral key $k = 877$. What is the ciphertext Alice sends to Bob?

   (c) Alice chooses a new private key $a = 299$ with associated public key $A \equiv 34 \mod 1373$. Bob encrypts a message and sends the ciphertext $(c_1, c_2) = (661, 1325)$. What is the message?

Solution:

(a) $2^{947} \equiv 177 \mod 1373$.

(b) We have $c_1 \equiv g^k \equiv 2^{877} \equiv 719 \mod 1373$ and $c_2 \equiv mA^k \equiv 583 \cdot 469^{877} \equiv 623 \mod 1373$. So the ciphertext is $(719, 623)$.

(c) We compute $x \equiv c_1^a \equiv 661^{299} \equiv 645$, and then compute $x^{-1} \equiv 661^{1372-299} \equiv 794 \mod 1393$. Finally we compute $c_2 x^{-1} = 1325 \cdot 794 \equiv 332 \mod 1373$ so this is the message.

6. Alice publishes an RSA public key with modulus $N = 2038667$ and exponent $e = 103$.

   (a) Bob wans to send Alice the message $m = 892383$. What ciphertext does he send her?

   (b) Alice knows that N factors into two primes, one of which is 1301. What is her decryption exponent d?

   (c) Some time later, Alice receives the ciphertext $c = 317730$ from Bob. What is the message?

Solution:

(a) Bob computes $c \equiv m^e \equiv 45293 \mod N$.

(b) $N = pq = (1301)(1567)$. Thus $M = (1300)(1566) = 2035800$. We want to compute d the inverse of e modulo M, so $d \equiv 810367 \mod M$.

(c) Alice computes $c^d \equiv 317730^{810367} \equiv 514407 \mod N$.

7. Suppose Eve knows that $N = pq = 352717$, and also intercepts the fact that $(p-1)(q-1) = 351520$. Can you determine $p+q$ from this? Can you determine p and q (without directly factoring N)?

   Solution: We have $pq = 352717$ and $(p-1)(q-1) = pq - p - q + 1 = 351520$. Subtracting the second from the first gives us $p + q - 1 = 1197$ so $p + q = 1198$.

   From here it's not too tough to find p and q by trial multiplication, and we see that $p = 521, q = 677$ (or vice versa).

   Alternatively, we can observe that $pq = p(1198-p) = 352717$, which gives the quadratic $p^2 - 1198p + 352717 = 0$. Solving this gives the two roots 521 and 677.