

Math 400 Fall 2018  
Cryptology HW 6  
Due Thursday, October 11

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  $x^a \pmod{m}$ .
2. Compute:
  - (a)  $\text{ord}_{13} 5$
  - (b)  $\text{ord}_{13} 7$
  - (c)  $\text{ord}_{13} 2$
  - (d)  $\text{ord}_{127} 2$
3.
  - (a) What is the inverse of 19 mod 96?
  - (b) Use your answer in part (a) to solve the congruence  $x^{19} \equiv 36 \pmod{97}$ .
4. Suppose 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  $469 \pmod{1373}$ . 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  $A \equiv 34 \pmod{1373}$ . Bob encrypts a message and sends the ciphertext  $(c_1, c_2) = (661, 1325)$ . What is the message?
5. Alice publishes an RSA public key with modulus  $N = 2038667$  and exponent  $e = 103$ .
  - (a) Bob wants 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?
6. 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  $q$ ?