CSE 467/567 Computer and Network Security
Department of Computer Science and Engineering, Miami University

Homework-2

John Doll

1. (4 points) Suppose the attacker intercepts the following message, without the knowledge of the encryption key. Please try to decrypt this ciphertext using **frequency analysis**.

   KWJJAJWXJUTJRXFWJYMJQJFXYIJKNSJI

   FREEVERSEPOEMSARETHELEASTDEFINED

2. (10 points) Perform encryption and decryption using the RSA algorithm. Determine the value of ciphertext and the private key to decrypt the ciphertext.

   a) p=3;q=11,e=7;M=5
      C=14, D = 3 KR = {3, 33}
   b) p=5;q=11,e=3;M=9
      C=14, D = 27 KR = {27, 55}
   c) p=7;q=11,e=17;M=8
      C = 57, D = 53 KR = {53, 77}
   d) p=11;q=13,e=11;M=7
      C =106, D = 11 KR = {11, 143}
   e) p=17;q=31,e=7;M=2
      C=128, d=343 KR = {343, 527}

3. (3 points) In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?
   a. 16

4. (3 points) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root alpha = 2. Show all the works
   a) If user A has public key YA = 9, what is A's private key XA?
      a. 9 = 2 ^ XA % 11
      b. 2 ^ 1 % 11 = 2
      c. 2 ^ 2 % 11 = 4
      d. 2 ^ 3 % 11 = 9
      e. XA = 3
   b) If user B has public key YB = 3, what is the shared secret key K?
      a. K = 3 ^ 3 % 11 = 5

Submission Instructions: Upload PDF file to canvas.