Homework 2 (100pt)

Rule: Finish all of the following on your own.
Submit your solution in PDF format to eCourseware.

1. Compute the following with detailed steps. (Hints: Use Fermat Theorem, Euler Theorem, properties of totient functions, etc) (40 pts)
   (a) \(1234^{16} \mod 17\)
   (b) \(54^{51} \mod 17\)
   (c) \(\phi(51)\)
   (d) \(\gcd(33, 121)\)
   (e) \(2^{-1} \mod 17\) (i.e., multiplicative inverse of 2 mod 17)
   (f) \(\text{ind}_{2,5}(4)\)
   (g) \(\phi(8000)\)

2. Write a computer program to implement the extended Euclid’s algorithm, use your code to compute the following. Submit your code and results. (20 pts)
   a. \(\gcd(10012012, 2314213)\)
   b. \(\gcd(28176412, 29108188)\)
   c. The multiplicative inverse of 12091 mod 24123123.
   d. The multiplicative inverse of 28173928 mod 129182771.

3. Prove that \(a=n-1\) is always a solution to \(a^2=1 \mod n\). (10 pts)

4. Perform encryption and decryption using RSA for \(p=5; q=11, e=3\) (public key); \(m=9\) (message). Show how you got your results. (10 pts)

5. Explain the reason why an attacker cannot get the private key \(<d,n>\) with the knowledge of public key \(<e,n>\) in RSA. (10 pts)

6. Alice and Bob use a new key establishment protocol to negotiate a symmetric key. Alice selects a random number \(x\) and computes \(x^g\), where \(g\) is a number that is known to the public. Bob selects a random number \(y\) and computes \(y^g\). Alice and Bob send \(x^g\) and \(y^g\) to each other. The shared key is computed as \((xy)^g\). Describe the vulnerability. (10 pts)