PMAT 4282 – Cryptography   Assignment #9
Winter 2001

1. On Page 137 of Stinson's book is the Miller-Rabin Primality Test:

   1 Given n, write $n - 1 = 2^t m$, where m is odd.

   2 Choose a random integer a such that $1 \leq a \leq n - 1$.

   3 Set $b \leftarrow a^m \pmod{n}$.

   4 If $b \equiv 1 \pmod{n}$ then output "n is likely prime" and stop.

   5 For $i = 0, 1, \ldots, (t - 1)$, do the following:

   5.1 If $b \equiv -1 \pmod{n}$ then output "n is likely prime" and stop.
   Otherwise set $b \leftarrow b^2 \pmod{n}$.

   6 Output "n is composite"

   The intent is to perform this algorithm k times (say $k = 100$), and if each time the output was "likely prime", to then conclude n is very likely to be prime.

   Stinson's book proves that if n is prime, then this algorithm will never output "n is composite". However, if n is composite, then it is possible that the algorithm will incorrectly state that "n is likely prime."

   Find an odd composite number $n \geq 50$ and a value for a $(1 < a < n - 1)$ for which the algorithm outputs "n is likely prime."

2. Let p be an odd prime and let $a \geq 1$. Prove that the number of solutions in $\mathbb{Z}_p$ to the equation $x^a \equiv 1 \pmod{p}$ is $\text{GCD}(a, p - 1)$.

3. Let $n = pq$ where p and q are distinct odd primes. Prove that the number of integers m, $0 \leq m < n$, such that $m^e \equiv m \pmod{n}$ is $(d_1 + 1)(d_2 + 1)$ where $d_1 = \text{GCD}(p - 1, e - 1)$ and $d_2 = \text{GCD}(q - 1, e - 1)$.

4. Bob has published $(30314385727, 683)$ as his public-key for RSA. Eve intercepts the ciphertext 13490063419 sent from Alice to Bob. What was the plaintext message?

5. Use Pollard's $p - 1$ algorithm to factor $n = 3129476997089035646236920257$. What is the smallest B value that will yield a factorisation?

6. Use the Pollard ρ algorithm to factor $n = 1002468832301$.

7. Using the Quadratic Sieve Method, factor at least two of the following integers.

   (a) $n = 39961$

   (b) $n = 49981$

   (c) $n = 99067$