Cryptography and Network Security

(Final Exam, 2016/1/11)

$a^{p-1} \equiv 1 \pmod p$

$a^{n-1} \equiv 1 \pmod n$

1. (20%) The following is the Miller-Rabin primality testing method. Please write the answers from (a) to (j).

   Miller_Rabin Test (n, a) // n is the number; a is the base

   {

   Find m and k such that __(a)__$=m\times 2^k$

   T $\leftarrow a^m$ mod n

   if (T= ± 1) return "__(b)___" // why? __(c)___

   for ($i \leftarrow$ 1 to __(d)___)

   {

   T $\leftarrow$T^2 mod n

   If (T= -1) return "___(e)__" // why? ___(f)___

   If (T= +1) return "___(g)__" // why? ___(h)___

   }

   return " __(i)___" // why? ___(j)____

   }

   swapped, evil

   $n-1 = m \times 2^k$

   $a^{n-1} = a^{m\times 2^k}$

   $\phi(p^e) = p^e - p^{e-1}$

   square root test: $(\pm 1)^2 \equiv 1 \pmod n$

   $63 \times 15 = 945$

   $77 \times 13 = 1001$

2. (10%) Find the value of $\Phi(29)$, $\Phi(32)$, $\Phi(80)$, $\Phi(100)$, $\Phi(101)$.

   p 2^5 $2^4\times5^1$ $2^2\times5^2$ p

   $(4-2)(25-5) = 2\times 20 = 40$

3. (10%) Find the results of the following.

   (a) 12^{-1} mod 77

   (b) 13^{-1} mod 403

   $\phi(77) = \phi(7\cdot 11) = 6\times 10 = 60$

   $\phi(8) = 4$ 1, 3, 5, 7

   $\phi(403) = \phi(13\times 31) = 12\times 30 = 360$

4. (10%) Find the smallest positive integer satisfying the following sets of congruence:

   (a) $x \equiv 2$ mod 7, $x \equiv 3$ mod 11, $x \equiv 9$ mod 13.

   (b) $x \equiv 2$ mod 7, $x \equiv 3$ mod 9, $x \equiv 9$ mod 15.

5. (10%) Prove that the numbers of prime are infinite. You may give an informal proof by an example.

   $\frac{n}{\ln n} < \pi(n) < \frac{n}{\ln n - 1.08366}$

6. (10%) Show that every prime excluding 2 is either in the form $4k+1$ or $4k+3$, where k is a positive integer.

   $\phi(p) = p-1 = 2j$ $p = 2j+1$ if $j = 2k$ even, if $j = 2k+1$ odd

7. (10%) Let P and Q be two prime numbers and $N=P\cdot Q$. Find the value of $\Phi(N)$.
8. (10%) What is a deterministic algorithm? What is a probabilistic algorithm?
9. (10%) What is the form for Mersenne Primes? What is the form for Fermat Primes.

   2^p-1 $2^{2^n}+1$

10. **(Bonus, 10%)** For RSA, a pair of (private key, public key) of Bob is generated by Bob. First, Bob selected two large prime number, say P and Q. Let $N=P\cdot Q$. Find e and d such that $e\cdot d \equiv 1$ mod $\Phi(N)$. Then e and d is the private key and public key of Bob.

    (a) Show how to encrypt and decrypt a message M.

    (b) Show why (a) can work.