SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 3: ASYMMETRIC KEY CRYPTOGRAPHY

Topic : Prime numbers-Primality Testing

Recap

EUCLID(a,b)

1. A ← a; B ← b;
2. If B = 0 return A= gcd(a,b)
3. R =A mod B
4. A ← B
5. B ← R
6. Go to 2

To find gcd (1970, 1066) ?

gcd (1970, 1066) =2

Prime Numbers

- prime numbers only have divisors of 1 and self
  - they cannot be written as a product of other numbers
  - note: 1 is priis generally not of interest me, but
- Example : 2,3,5,7 are prime, 4,6,8,9,10 are not prime numbers are central to number theory
- To factor a number n is to write it as a product of other numbers: n=a x b x c
- Prime factorization

$$a = \prod_{p \in \mathrm{P}} p^{a_p}$$

PRIME NUMBERS
BETWEEN 1 AND 1,000

2	79	191	311	439	577	709	857
3	83	193	313	443	587	719	859
5	89	197	317	449	593	727	863
7	97	199	331	457	599	733	877
11	101	211	337	461	601	739	881
13	103	223	347	463	607	743	883
17	107	227	349	467	613	751	887
19	109	229	353	479	617	757	907
23	113	233	359	487	619	761	911
29	127	239	367	491	631	769	919
31	131	241	373	499	641	773	929
37	137	251	379	503	643	787	937
41	139	257	383	509	647	797	941
43	149	263	389	521	653	809	947
47	151	269	397	523	659	811	953
53	157	271	401	541	661	821	967
59	163	277	409	547	673	823	971
61	167	281	419	557	677	827	977
67	173	283	421	563	683	829	983
71	179	293	431	569	691	839	991
73	181	307	433	571	701	853	997

Example

- Factorization
- 91 = 7 * 13
- 3600 = $2^4 * 3^2 * 5^2$
- 11011 = $7 * 11^2 * 13$

Relatively Prime Numbers & GCD

- two numbers a, b are relatively prime if have no common divisors apart from 1
- Example:
- 8 & 15 are relatively prime since factors of
  - 8 are 1,2,4,8 and
  - 15 are 1,3,5,15 and 1 is the only common factor

GCD

$300=2^1x3^1x5^2$

$18=2^1x3^2$

$GCD(18,300)=2^1x3^1x5^0=6$

Fermat's Theorem

- Useful in public key and primality testing
- If P is Prime Number & a is a positive integer not divisible by p then
  - $a^{p-1} = 1 \pmod p$
    - where p is prime and gcd(a,p)=1
- Also known as Fermat's Little Theorem
- Also have: $a^p = a \pmod p$

Euler Totient Function ø(n)

- Euler Totient Function ø(n) = pq
  - ø(n) = pq =ø(p)*ø(q) = (p-1) *(q-1)
- Where p and q are two prime numbers; p≠q

- **Example**
  - ø(21) = (3–1)x(7–1) = 2x6 = 12

Euler Totient Function ø(n):some Values

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Euler's Theorem

- Every a and n that are relatively prime:
  - $a^{\phi(n)} \equiv 1 \pmod{n}$
- **Example**

  a=3;n=10; ø(10)=4;

  hence 34 = 81 = 1 mod 10

  a=2;n=11; ø(11)=10;

  hence 210 = 1024 = 1 mod 11

Testing for Primality

- often need to find large prime numbers
- traditionally sieve using trial division
  - ie. divide by all numbers (primes) in turn less than the square root of the number
  - only works for small numbers
- alternatively can use statistical primality tests based on properties of primes
  - for which all primes numbers satisfy property
  - but some composite numbers, called pseudo-primes, also satisfy the property
- can use a slower deterministic Primality test

Miller Rabin Algorithm

a test based on prime properties that result from Fermat's Theorem algorithm is:

TEST (n) is:

1. Find integers k, q, k > 0, q odd, so that $(n–1)=2^kq$
2. Select a random integer a, $1<a<n–1$
3. if $a^q \bmod n = 1$ then return ("inconclusive");
4. for j = 0 to k – 1 do
    5. if $(a^{2jq} \bmod n = n-1)$
        then return("inconclusive")
6. return ("composite")

Thank You