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 2: SYMMETRIC KEY CRYPTOGRAPHY

Topic : Euclid's algorithm

Euclid's Algorithm

Greatest Common Divisor (gcd)

gcd : A common problem in number theory.

gcd(a, b) : (greatest common divisor of a and b) is the largest number that divides evenly into both a and b

gcd(a, b) = max{ k ; such that k|a and k|b }

gcd(60, 24) = 12

If gcd(a, b) = 1, i.e. if a and b have no common factors

(except 1) and hence a and b are relatively prime

gcd(8,15) = 1 implies 8 and 15 are relatively prime

Algorithm

```
Euclid(A,B)
If B=0 then return A
                else return Euclid(B, A mod B)
```

To find gcd(1970, 1066)

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

Therefore, gcd(1970, 1066) = 2