



# **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



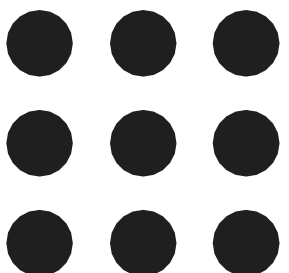
## **DEPARTMENT OF INFORMATION TECHNOLOGY**

**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

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

$$\text{gcd}(60, 24) = 12$$

If  $\text{gcd}(a, b) = 1$ , i.e. if a and b have no common factors

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

$\text{gcd}(8, 15) = 1$  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)

$$1970 = 1 \times 1066 + 904$$

$$1066 = 1 \times 904 + 162$$

$$904 = 5 \times 162 + 94$$

$$162 = 1 \times 94 + 68$$

$$94 = 1 \times 68 + 26$$

$$68 = 2 \times 26 + 16$$

$$26 = 1 \times 16 + 10$$

$$16 = 1 \times 10 + 6$$

$$10 = 1 \times 6 + 4$$

$$6 = 1 \times 4 + 2$$

$$4 = 2 \times 2 + 0$$

Therefore, gcd(1970, 1066) = 2

$$\text{gcd}(1066, 904)$$

$$\text{gcd}(904, 162)$$

$$\text{gcd}(162, 94)$$

$$\text{gcd}(94, 68)$$

$$\text{gcd}(68, 26)$$

$$\text{gcd}(26, 16)$$

$$\text{gcd}(16, 10)$$

$$\text{gcd}(10, 6)$$

$$\text{gcd}(6, 4)$$

$$\text{gcd}(4, 2)$$

$$\text{gcd}(2, 0)$$