The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 11

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following objective:

- **Euclidean Algorithm.**

Euclid's or Euclidean Algorithm

One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. First, we need a simple definition : Two integers are relatively prime if their only common positive integer factor is 1.

Greatest Common Divisor (GCD)

We will use the notation **gcd(a ,b)** to mean the greatest common divisor of a and b, where a, b are integers. The greatest common divisor a of b and is the largest integer that divides both **a** and **b**.

If have two numbers c,q that c=q*d+r, then GCD(c,q)=GCD(d,r)

<u>Ex1:</u> find the Greatest Common Divisor (GCD) between 132 and 55 by using Euclid's Algorithm.

132 = 55 * 2 + 22
55 = 22 * 2 + 11
22 = 11 * 2 + 0

Stopping when getting zero 0 then GCD is 11:

GCD(132,55) = GCD(55,22) = GCD(22,11) = GCD(11,0) = 11

Ex2: find the GCD (252 , 198) by using Euclid's Algorithm.

$252 = 198 * 1 + 54$

$198 = 54 * 3 + 36$

$54 = 36 * 1 + 18$

$36 = 18 * 2 + 0$

GCD(252,198) = (198,54) = (54,36) = (36,18) = (18,0) = 18.

Example: Compute the greatest common divisor (GCD) between the numbers (831, 366).

Solution:

$$
\begin{aligned}
831 &= 2 \times 366 + 99 \\
366 &= 3 \times 99 + 69 \\
99 &= 1 \times 69 + 30 \\
69 &= 2 \times 30 + 9 \\
30 &= 3 \times 9 + 3 \\
9 &= 3 \times 3 + 0
\end{aligned}
$$

The answer is revealed as the last nonzero remainder: gcd (831, 366) = 3

Note: Because we require that the greatest common divisor be positive GCD (a, b) = GCD (a, -b) = GCD (-a, b) = GCD(-a,-b). In general, GCD(a, b) = GCD(/ a / , / b/).

Example: Find the the greatest common divisor (GCD) of a=321805575, b=198645

Solution:

321805575	=	1620 * ***198645***	+ 675
198645	=	294 * ***675***	+ 195
675	=	3 * ***195***	+ 90
195	=	2 * ***90***	+ 15
90	=	6 * ***15***	+ 0

The answer is revealed as the last nonzero remainder: GCD (321805575, 198645) = 15

Homework

(a) gcd(24, 54) = 6 (b) gcd(18, 42) = 6	(c) gcd(244, 354) = 2 (d) gcd(128, 423) = 1	(e) gcd(2415, 3289) = 23 (f) gcd(4278, 8602) = 46 (g) gcd(406, 555) = 1