كلية الرشيد الجامعة
قسم هندسة تقنيات الحاسوب

المرحلة الرابعة

أمنية الحاسوب و شبكاتها

المحاضرة رقم (13)

مدرس المادة : م.م تميم محمد

SECURITY OF COMPUTER AND NETWORKS

REFERENCE

CRYPTOGRAPHY AND NETWORK SECURITY

PRINCIPLES AND PRACTICE 5TH EDITION

EUCLID'S ALGORITHM

Let a and b be integers, not both zero. Recall that gcd (a, b) is the greatest common divisor of a and b. The best general algorithm for computing gcd (a, b) (and the only practical algorithm, unless the prime factorizations of a and b are known) is due to Euclid. This algorithm (known as Euclid's Algorithm or the Euclidean Algorithm) involves repeated application of the Division Algorithm.

WHY DOES THE EUCLIDEAN ALGORITHM WORK?

We describe the algorithm in words (if necessary) as follows:

1. To find gcd(a, b), divide a by b, obtaining a quotient and a remainder. Repeatedly divide, at each step taking the previous divisor and remainder as the new dividend and divisor, respectively.

2. At each iteration, the remainder is smaller than at the previous iteration, until at least the remainder becomes zero.

3. Backing up to the previous step, we obtain gcd (a, b) as the last nonzero remainder.

EUCLID'S ALGORITHM LOW

$$A = d * B + r$$

A= the greater number

B = the smaller number

d = the division number

r = the reminder

EXAMPLE: 1 COMPUTE THE GREATEST COMMON DIVISOR (GCD) BETWEEN THE NUMBERS (831, 366).

Solution: $A = d * B + r$

831	=	2 × 366	+ 99
366	=	3 x 99	+ 69
99	=	1 x 69	+ 30
69	=	2 x 30	+ 9
30	=	3 x 9	+ 3
9	=	3 x 3	+ 0

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

EXAMPLE: 1 COMPUTE THE GREATEST COMMON DIVISOR (GCD) BETWEEN THE NUMBERS (A=321805575, B=198645)

Solution: $A = d * B + r$

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

CLASSWORK

Now you try some: Answers		
(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