CSE 280 Challenge Set 06 - Solutions

Instructions: Work on all questions as a group as instructed during class. We will review each answer during class.

Question 1

Use the Eulcid Algorithm to find the gcd for the following pairs of numbers. Use tables as we did in class.

- $gcd(80, 32)$
- $gcd(560, 792)$

Answer:

$x = r'$	$y = x'$	$r = y \bmod x$
80	32	32
32	80	16
16	32	0
0	16	

GCD = 16

$x = r'$	$y = x'$	$r = y \bmod x$
560	792	232
232	560	96
96	232	40
40	96	16
16	40	8
8	16	0
0	8	

GCD = 8

Question 2

Use the Extended Euclid Algorithm to express the answers to question 1 as a linear combination.

Answer:

$x = r'$	$y = x'$	$r = y \bmod x$	$q = y \operatorname{div} x$	$s = t' - qs'$	$t = s'$
80	32	32	0	1	-2
32	80	16	2	-2	1
16	32	0	2	1	0
0	16			0	1

$16 = 80 * 1 - 2 * 32$

$x = r'$	$y = x'$	$r = y \bmod x$	$q = y \operatorname{div} x$	$s = t' - qs'$	$t = s'$
560	792	232	1	-41	29
232	560	96	2	29	-12
96	232	40	2	-12	5
40	96	16	2	5	-2
16	40	8	2	-2	1
8	16	0	2	1	0
0	8			0	1

$8 = -41 * 560 + 29 * 792$

Question 3

Part 1

Create public and private RSA keys. Use the two prime numbers: $p = 163$ and $q = 431$. Calculate N (public) and ϕ. Select the **smallest** value e (public) such than $gcd(e, \phi) = 1$. Use the Extended Eulicd Algorithm to find the multiplicative inverse of $e \bmod \phi$ and call the result d (private).

Determine the equations to encrypt and decrypt. Use the table below to execute the Euclid algorithm.

Answer:

Public: $N = 163 * 431 = 70253$

$\phi = 162 * 430 = 69660$

Public: $e = 7$ NOTE: $gcd(e, \phi) = 1$,

$x = r'$	$y = x'$	$r = y \bmod x$	$q = y \operatorname{div} x$	$s = t' - qs'$	$t = s'$
7	69660	3	9951	19903	-2
3	7	1	2	-2	1
1	2	0	2	1	0
0	1			0	1

Linear Combination: $1 = 7 * 19903 - 69660 * 2$

Private: $d = 19903 \bmod 69660 = 19903$

Encryption Formula: $c = m^7 \bmod 70253$

Decryption Formula: $m = c^{19903} \bmod 70253$

Part 2

Use a python terminal (which is good at working with large numbers) to encrypt and decrypt the word "PIE" using the RSA keys obtained in Part 1 above. To convert the letters to numbers, use the ASCII code provided in the second column. Use the Python terminal to do the math.

Letter	ASCII	Encrypted	Decrypted	Letter
P	80	10569	80	P
I	73	37719	73	I
E	69	46437	69	E