EE2302 Foundations of Information Engineering

Assignment 7 (Solution)

1.

87	37		
1	0	87	a
0	1	37	b
1	-2	13	$c = a - 2b$
-2	5	11	$d = b - 2c = -2a + 5b$
3	-7	2	$e = c - d = 3a - 7b$
-17	40	1	$f = d - 5e = -17a + 40b$

$x = (3)(87)(-17) + (5)(37)(40) = 2963$.

2.

$M_1 = 12 \times 13 = 156$, $\alpha_1 \equiv 156^{-1} \pmod 7 = 4$ (steps of finding inverses are omitted.)
$M_2 = 7 \times 13 = 91$, $\alpha_2 \equiv 91^{-1} \pmod{12} = 7$
$M_3 = 7 \times 12 = 84$, $\alpha_3 \equiv 84^{-1} \pmod{13} = 11$
$M = 7 \times 12 \times 13 = 1092$
$x = 5(156)(4) + 2(91)(7) + 8(84)(11) \pmod{1092} = 866$

3.

(a) $c = m^e \bmod N = 16^3 \bmod 55$

$16^2 \equiv 36 \bmod 55$

$16^2 \times 16 \bmod 55 = 36 \times 16 \bmod 55 = 26 \; mod \; 55.$

(b) $N = p \times q \quad 55 = 5 \times 11.$

$\phi(N) = (p-1)(q-1) = 4 \times 10 = 40.$

$ed \equiv 1 \bmod 40$

$3d \equiv 1 \bmod 40 \Rightarrow d = -13 = 27.$

$m = c^d \bmod n = 26^{27} \; mod \; 55 = 26^{16} \times 26^8 \times 26^2 \times 26 \; mod \; 55$

$= 26 \times 31 \times 16 \times 26 \; mod \; 55 = 16 \; mod \; 55$

$(\, 26^2 \equiv 16 \; mod \; 55 \,, \; 26^4 \equiv 36 \; mod \; 55, 26^8 \equiv 31 \; mod \; 55 \,, 26^{16} \equiv 26 \; mod \; 55 \,)$

4.

a) a and m are co-primes, so that a^{-1} exists.

b) $\phi(26) = 12$

c) There are 12 possible values for a and 26 possible values for b. Therefore the number of possible keys is $12 \times 26 = 312$.

d) For $a = 9,\ a^{-1} \equiv 3 \mod 26$.

$$9x + 6 = 20 \pmod{26}$$

$$x = 3(20 - 6) \pmod{26}$$

$$= 42 \bmod 26$$

$$= 16$$