CS211 ALGORITHMS & DATA STRUCTURES II

LAB 5

Dr. Phil Maguire

CRYPTOGRAPHY

Question 1

Calculate 7^{29} mod 11 by hand (see crypto notes).

7^1 mod 11 = 7

7^2 mod 11 = 7 * 7 = 49 mod 11 = 5

7^4 mod 11 = 5 * 5 = 25 mod 11 = 3

7^8 mod 11 = 3 * 3 = 9 mod 11 = 9

7^{16} mod 11 = 9 * 9 = 81 mod 11 = 4

$7^{29} = 7^{16} * 7^8 * 7^4 * 7^1 = 4 * 9 * 3 * 7$ mod 11

= 36 mod 11 * 21 mod 11

= 3 * 10 mod 11

= 30 mod 11

= 8

Question 2

$(c_1, c_2) = (23, 27)$

In order to find the message m we compute $c_2 / c_1^{x} \bmod p$

$1 / c_1^{x} = c_1^{-x} = c_1^{p-1-x} = c_1^{29-1-5} = c_1^{23}$

So we need to compute $27 \times 23^{23} \bmod 29$

$23^{1} \bmod 29 = 23$

$23^{2} \bmod 29 = 7$

$23^{4} \bmod 29 = 20$

$23^{8} \bmod 29 = 23$

$23^{16} \bmod 29 = 7$

$23^{23} \bmod 29 = (23^{16} \times 23^{4} \times 23^{2} \times 23^{1}) \bmod 29 = (7 \times 20 \times 7 \times 23) \bmod 29 = 7$

$27 \times 7 \bmod 29 = 15$

So Bob is sending the message 15