Cryptography and security

Special Worksheet

1. Extended GCD algorithm

Example: XGCD between 32 and 63

```
32) 63 (q = 1
     32
    ---------
  r=31) 32 ( q=1
          31
         ------------
         r= 1) 31 (q=31
                 31
                 ------------
                r=0        * Algorithm terminates
```

The last but one non zero remainder is gcd = 1
q= quotient and r=remainder
in equation form:

63 = 32 * 1 + 31
32= 31 * 1 + 1
31 = 1 * 31 + 0

Extended Euclidean algorithm
start with last but one equation (the one which gives the gcd)
In this case it is 2nd equation
1 = 32 - 31 *1
Substitute 31 using the first equation
1= 32 - (63 - 32*1)*1
1 = 32 (1 +1) - 63 (1)

1 = 32 * x + 63* y ; where x =2 and y = -1

Thus we are able to express gcd as a linear sum of 32 and 63

The output of XGCD algorithm is 3 tuple [gcd,x,y]

Thus gcd =1= 32 x + 63 y

Taking modulo 63 on both sides, we get

1 = 32 x mod 63.

Hence x is the inverse of 32 mod 63.

2) Find XGCD (27, 73)

3) The following lists certain outputs from XGCD algorithm.

XGCD(11,73) = 1, 20, -3

XGCD(12,73) = 1, -6, 1

XGCD(13,73) = 1, -28, 5

XGCD(14,73)= 1, -26, 5

XGCD(15,73)= 1, -34, 7

XGCD(35,73) = 1, -25, 12

Find the inverses of the following numbers modulo 73.

11, 12, 13, 14, 15, 35.

Also note that, on Magma,

InverseMod(a,n)

function returns inverse of a modulo n.

For example,

InverseMod(7,26) is 15.

Because (7*15) mod 26 is 1.