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)

19 = 73 – 27x 2

8 = 27 – 19 x 1

3 = 19 – 8 x 2

2 = 8 – 3 x 2

1 = 3 – 2 x 1 : gcd =1

0 = 2 – 1x 2

1 = (3) – 2 x 1

1 = 3 – (8 – 3 x 2)x1 → 1 = - 8 + 3 x 3

= -8 + (19 – 8 x 2)x3 → 1 = 19 x 3 – 8 (7)

1 = 19 x3 –(27 – 19 x 1)7→ 1 = 19 (3+7) – 27(7) → 1 = 19 (10) – 27(7)

1= (73 – 27x2)10 – 27(7)→ 1= 73x10-27(27) → 73x10 + 27 (-27).

Thus, XGCD(27,73) = 1,-27,10, implying gcd =1 = (-27)x27+ 10x73

3) The following lines 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.

11^{-1}= 20, 12^{-1}= -6 = (73-6) = 67, 13^{-1}= (-28) = 45, 14^{-1} = (-26) = 47, 15^{-1} = -34 = 39; 35^{-1} = -25 = 48;