MATHS FOR CRYPTOGRAPHY

Number Theory

Number Theory

- Modular Arithmetic
- Prime and relatively prime
- Euclid's algorithm
- Multiplicative inverses
- Chinese Remainder Theorem
- Euler's Totient Function
- Euler's Theorem

Modular Arithmetic

- For integers m and n (n>0) remainder of m/n is smallest integer > 0 that differs from m by a multiple of n
- a mod n = b mod n if a – b = kn
- Z_n is set of all integers mod n
- Z_n= { 0,1,2,…..n-1} a total of n integers
- additive inverse of a is b such that a+b=0
- Multiplicative inverse axb=1, b=a^{-1}

Primes

- Integer p is prime iff evenly divisible by itself and 1
- Infinite number of primes
- 25 primes < 100
- Probability n is prime is 1/ln n
- !0 digit (mod 10) is 1 in 23
- 100 digit (mod 10) is 1 in 230

Relatively Prime

- m and n are relatively prime if gcd(m,n)=1
- For any integer x, gcd(0,x) = x, and 1 is relatively prime to x since gcd(1,x) = 1
- Find gcd from Euclid's algorithm

Euclid's algorithm (I)

- (x,y) and (x-y,y) have same gcd
- replace x by remainder when divided by y
- switch and repeat process
- final remainder is zero
- penultimate remainder is gcd

Euclid's Algorithm (II)

Example (399, 247)

n	division	quotient	remainder
1	399/247	1	152
2	247/152	1	95
3	152/95	1	57
4	95/57	1	38
5	57/38	1	19
6	38/19	2	0

gcd(399,247) = 19

Euclid's Algorithm (III)

$r_{n-2}/r_{n-1} = q_n + r_n/r_{n-1}$

$r_n = r_{n-2} - q_n r_{n-1}$

$r_n = u_n x + v_n y$ consistent if
$u_n = u_{n-2} - q_n u_{n-1}$ and
$v_n = v_{n-2} - q_n v_{n-1}$

if integers u,v can be found such that ux + vy = 1
(x,y) are relatively prime

Multiplicative Inverses

To find inverse of m mod n find u such that

um = 1 mod n or
um + vn = 1 mod n but
ux + vy = 1 iff (x,y) are relatively prime

Inverse of m may be found from Euclid's algorithm
if and only if m is relatively prime to n

Chinese Remainder Theorem

Standard Representation x mod $z_1 z_2 z_3 \ldots\ldots z_k$

Decomposed Representation x_1 mod z_1, x_2 mod z_2, ...x_k mod z_k

if $z_1, z_2, z_3, \ldots z_k$ are relatively prime

From Standard to Decomposed divide x by z_i to give remainder x_i

From Decomposed to Standard take x_1 mod p and x_2 mod q
Since p and q are relatively prime there exists integers a and b
such that ap + bq = 1 (ap = 1 mod q and bq = 1 mod p

$$x = xap + xbq$$
$$x = x_2 ap + x_1 bq \bmod pq$$

Euler's Totient Function

- Z_n set of all integers mod n
- Z_n^* set of all integers relatively prime to n
- Z_n^* is closed under multiplication mod n
- $\Phi(n)$, Euler's Totient Function is number of all elements in Z_n^*

Euler's Totient Function (II)

If n is prime $\Phi(n) = n-1$

$n = p^\alpha$, p prime, $\alpha > 0$ then excluding multiples of p

$$\Phi(n) = p^\alpha - p^{\alpha-1} = (p-1)\,p^{\alpha-1}$$

n = pq, p and q prime, then excluding multiples of p
and multiples of q gives

$$\begin{aligned}\Phi(n) &= pq - 1 - (p-1) - (q-1)\\ &= pq - p - q - 1 = (p-1)(q-1)\\ &= \Phi(p)\Phi(q)\end{aligned}$$

Euler's Theorem

For all a in Z_n^*, $a^{\Phi(n)} = 1$

and for all a in Z_n^* and non-negative integers k

$a^{k\Phi(n)+1} = a \bmod n$