SEM - VII - 2022-23
CNS Lab
B3 - 2019BTECS 00094 - Sweety Shrawan Gupta

Assignment 9

Chinese Remainder Theorem

Theory:-

Chinese Remainder Theorem

Given pairwise coprime positive integers $n_1, n_2, \ldots, n_k$ and arbitrary integers $a_1, a_2, \ldots, a_k$, the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution, and the solution is unique modulo $N = n_1 n_2 \cdots n_k$.

The CRT is a theorem which gives a unique solution to simultaneous linear congruences with coprime moduli. In its basic form, the CRT will determine a number p that, when divided by some given divisors, leaves given remainders.

Code:

```
def calcMultInv(a: int, b: int):
  r1 = a
  r2 = b
  t1 = 0
  t2 = 1

  while r2 != 0:
    q = r1 // r2
    r = r1 - q * r2
    t = t1 - q * t2
```

```
    r1 = r2
    r2 = r
    t1 = t2
    t2 = t

  if r1 == 1:
    if t1 > 0:
      return t1
    else:
      return a + t1
  else:
    return None

def main():
  n = int(input('Enter no. of equations: '))
  a = list(map(int, input('Enter a0 a1 a2 ... an: ').split()))
  m = list(map(int, input('Enter m0 m1 m2 ... mn: ').split()))

  pM = 1
  for i in range(n):
    pM *= m[i]

  M = []
  for i in range(n):
    M.append(pM // m[i])

  MInv = []
  for i in range(n):
    MInv.append(calcMultInv(m[i], M[i]))

  x = 0
  for i in range(n):
    x = (x + a[i] * M[i] * MInv[i]) % pM

  print('\na =', a)
  print('m =', m)
  print('pM =', pM)
  print('M =', M)
  print('MInv =', MInv)
```

```
  print('\nx =', x)

main()
```

Output:

```
In [21]: runfile('D:/CNS Lab/CRT.py', wdir='D:/CNS Lab')

Enter no. of equations: 3

Enter a0 a1 a2 ... an: 2 3 2

Enter m0 m1 m2 ... mn: 3 5 7

a = [2, 3, 2]
m = [3, 5, 7]
pM = 105
M = [35, 21, 15]
MInv = [2, 1, 1]

x = 23
```

output
point steps
implement

- CRT
- RSA
- SHA
- Cryptanalysis
- Vignese
- Ceaser
- columnar
- Playfair

- euclidean
- Diffie Hellman
  Primitive root
- Railfence
- DES
- AES

python
Theory
modes
virtual lab

wireshark
snort
Digital certificate