ECS253 Notes on April 9, 97

Modular Arithmetic:

- solve ax mod n = 1 by the Extended Euclidean algorithm

  e.g. to solve: g=gcd(5,7)

g	x	y	q
7	0	1	
5	1	0	1
2	-1	1	2
1	3	-2	2
0			

  gcd(5,7)=3*5+(-2)*7=1
- solve x in: ax mod n = b
  - if we can find x_0 s.t. $ax_0 \bmod n = 1$, then we have
    $a(x_0 b \bmod n) = b$
  - thus $x = x_0 b$ is the solution
- Chinese method: solve x in $x \bmod d_i = x_i \quad \forall i \in [1,t]$
  - solution: $x = \sum_{i=1}^{t} (\frac{n}{d_i}) y_i x_i \bmod n$ where
  - $(\frac{n}{d_i}) y_i \bmod d_i = 1$
  - y_i can be solved by the above methods

Cipher:

- transposition cipher:
  - diffusion effect (suggested by Shannon)
  - can be attacked by frequency count (digram, trigram etc.)
- substitution cipher:
  - confusion effect (suggested by Shannon)
  - simple substitution:
    - one mapping applied to all components
    - e.g. Caesar cipher
    - f(m)=(m+k) mod 26 where k is the key length
    - is affine transformation:
      f(m)=(km + k') mod n where gcd(k,n) =1
    - can be attacked by comparing the shift with frequency distribution of normal English text
    - example to attack Caesar cipher is run through
  - homophonic substitution

- ≥1 mapping for the components