**Assignment02**

**60847013S 資工碩一 蘇冠中**

1. **Modular Multiplicative Inverse**
   1. **135 61 = 47**

gcd(135,61)=gcd(61,13)=gcd(13,9)=gcd(9,4)=gcd(4,1)=

gcd(1,0)=1 有一解 從ax + by = 1代回去求x,y

gcd(1,0) ; x=1;y=0

gcd(4,1) ; x=0; y=1

gcd(9,4) ; x=1,y=-2

gcd(13,9) ; x=-2,y=3

gcd(61,13) ; x=3,y=-14

gcd(135,61) ; x=-14,y=31

最後x = -14為其中一個模反元素，而可能的模反元素為

-14 + (61\*n)，n為整數，我們要求最小的正整數解，則為-14+61=47

* 1. **7465 2464 = 2329**

gcd(7465,2464)=gcd(2464,73)=gcd(73,55)=gcd(55,18)=

gcd(18,1)=gcd(1,0)=1，有一解

從ax +by =1 代回去求x,y

gcd(1,0) ; x=1,y=0

gcd(18,1) ; x=0,y=1

gcd(55,18) ; x=1,y=-3

gcd(73,55) ; x=-3,y=4

gcd(2464,73) ; x=4,y=-135

gcd(7465,2464) ; x=-135,y=409

最後x=-135為其中一個模反元素，而可能的模反元素為

-135 + (2464\*n)，n為整數，我們要求最小的正整數解，則為-135+2464=2329

* 1. **42828 6407 = no**

gcd(42828,6407)=gcd(6407,4386)=gcd(4386,2021)=

gcd(2021,344)=gcd(344,301)=gcd(301,43)=gcd(43,0)=43

因此沒有解

1. **Fermat＇s Theorem**

**2.1 =**

**2.2 =**

1. **Chinese Remainder Theorem**

**3.1**

(1) 設P = p1\*p2\*p3\*…\*pk， ,，也就是說是除了pi以外的-1個整數的乘積

(2) 設ti = 為模pi的數論倒數:ti,

(3) n的通解為 n = n1t1P1+n2t2P2+n3t3P3+… =

(4) 從p1~pk都互質上可知，當i、j，j時，gcd()=1，所以gcd() =1，說明存在整數，因此

,且

(5) 所以n = 滿足:

n = + = (mod )，可說明n就是此方程組的一個解。

**3.2**

當p1~pk之間不互質的時候，從上面(4)可知，gcd()就不會=1，且 ，範例:

假設n1,n2兩個方程組，

n 3 (mod 5) 和 n 4 (mod 10)

M = 5\*10=50, M1=10,t1=0,當t=0時，n1方程組算出來的會是0，也就找不出n來。

1. **Complement**

從Fiestel network可知，所以可以得到。

因為排列不會影響到bit的值，加上E⊕= ⊕，所以。

所以S-BOX的輸出保持不變、加密結果也保持不變。

**4.2**

假設有個明文攻擊，若選擇的明文為M和，攻擊者得到，並不會對暴力破解造成太多的影響。

1. **Polynomial Ring**