Part A

1.(a)

I used C language.

```
void XGCD(int a, int b, int& d, int& x, int& y)
/* a and b are general numbers, d is divisor, x and y are parameters which
satisfies the equation gcd(a,b)= x*a+y*b */
{
    if(b==0)
    {
        d=a;
        x=1;
        y=0;
    }
    else
    {
        XGCD(b,a % b,d,y,x);
        y=y-x*(a/b);
    }
}
```

In the Main function, just call XGCD(a,b,d,x,y), then printf("%d,%d,%d", d,x,y) is the result of the XGCD.

(b) If gcd (a,n) is 1, we can apply the Extended Euclid's algorithm here and get xa+yn=1. Then move the term yn to the other side of the equation, we have xa= -yn+1. That is, xa=1 mod n.

And when applying the Extended Euclid's algorithm like above, we can easily calculate the x, which is the inverse of a number a mod n.

(c)Suppose we have gcd(c,d)=z. That is, there exists two general numbers x,y which satisfie that c=x*z, d=y*z. And since c|a and d|b, we assume that there are two general numbers m,n making a=m*c and b=n*d. Thus, we have a=m*c=m*xz, b=n*d=n*yz. As the gcd(a,b)=1, so gcd(mxz,nyz)=1. And at least, we get z=1. Hence, we have gcd(c,d)=1.

2.(a) Security risks are more like loopholes of computers or possibilities that the computer may encounters attack. For instance, data which were stored in the computers or servers may be easily stolen or lost.

Security attack includes passive attack and active attack. The aim of passive attack is to utilise the information but not influence on the system resources. The famous examples are wiretap and monitor. By contrast, the active attack tries to affect the operations of system, such as information modification.

In the May of this year, a worm virus named ‘Wanna Decryptor’ (Wanna Cry) began to break out. The virus is based on the ‘Eternal Blue’ tool, using AES-128 and RSA algorithms to maliciously encrypt user files to extort bit coins.

The program will call Windows CryptoAPI after the completion of the load, then a pair of new 2048-bit RSA key will be created and stored to the infected computer, which includes the private key and the public key.

However, when decrypting, before the required private key was stored, it has been encrypted by another RSA public key in the program. Then the program will traverse the device and encrypt files with specific extensions. (en.wikipedia.org, 2017)

(b)i. $p=a^{-1}(c-b) \bmod 29$

ii. Since a is a number of the range {1,2,3…28} and b is a number of the range {0,1,2…28}. Thus, the non-trivial keys are 28*29-1=811.

iii.

The complexity of Cipher Text only Attack is based on two circumstances. One is that if the plaintext is the common words we used, then the complexity is equal to the summary of the frequency of each character in the plaintext and process of comparing with the frequency of characters which we used in the life. Another is that if the plaintext doesn't follow the law above (random plaintext), then we can't measure the complexity.

The complexity of Chosen Plain Attack is based on the length of the plaintext attackers chose. The more length they know, the complexity become less.

3.(a)

26*25*m - 1 =650m - 1

(b) Assuming a Hill cipher is with ‘m’ pairs of plaintext and ciphertext and the length of each is ‘m’. And assuming for each plaintext P_j, ciphertext C_j and secret key matrix in the encipherment K (1<=j<=m), we have $C_j=P_j*K$. In the known plaintext attack, suppose we get the plaintext matrix P and ciphertext matrix C, so we get the equation C=P*K. If P is invertible, we have $K=P^{-1}*C$. If P is not invertible, thus we have to find another pair of plaintext and ciphertext matrix until we find the invertible P. That is why the Hill cipher is easily broken.

(c)

Based on the given plaintext and ciphertext block, we have three plaintext matrixes P1=[15, 7, 8], P2=[11,14,18], P3=[14,15,8] and three ciphertext matrixes C1=[20,9,21], C2=[4,15,22], C3=[17,1,4]. We need to calculate the secret key matrix in the encipherment, which is $K=\begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$.

Based on the theory in question (b), we now have plaintext matrix $P=\begin{bmatrix} 15 & 7 & 8 \\ 11 & 14 & 18 \\ 14 & 15 & 8 \end{bmatrix}$ and ciphertext matrix $C=\begin{bmatrix} 20 & 9 & 21 \\ 4 & 15 & 22 \\ 17 & 1 & 4 \end{bmatrix}$. Then calculate the inverse matrix of P. That is, $P^{-1}=\begin{bmatrix} 4 & 5 & 16 \\ 5 & 5 & 0 \\ 11 & 9 & 9 \end{bmatrix}$. So the K= $P^{-1}*C=\begin{bmatrix} 372 & 127 & 258 \\ 120 & 120 & 215 \\ 409 & 243 & 465 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 & 23 & 24 \\ 16 & 16 & 7 \\ 19 & 9 & 23 \end{bmatrix}$. To decrypt the ciphertext, we should calculate the inverse matrix of K. That is, $K^{-1}=$

$$\begin{bmatrix} 25 & 11 & 9 \\ 11 & 2 & 6 \\ 18 & 15 & 14 \end{bmatrix}$$. After calculating C*K^{-1} sequentially, we have the plaintext is ‘PHILOSOPHER SASKCAN HUMAN INGENUITY CONCOCT A CIPHER WHICH HUMAN INGENUITY CAN NOT RESOLVE.’.

The decryption code in Java:

```
   public class Main {

   public static void main(String[] args) {
      int i, j;
      String arr =
"UJVEPWRBEWGFKOSDHJGRMWUPQPEEPMCHUUCFLFHCAQWZHXAVVTDGRMWUPQPEEPMCHUNNALZCOMY
GBJ"; //The ciphertext
      char c[] = arr.toCharArray();
      int num[] = new int[78];
      int num2[] = new int[78];
      for (i = 0; i < c.length; i++) { //Convert characters to numbers,
then store in a new number array.
         num[i] = c[i] - 65;
      }

      for (j = 0; j < i; j = j + 3) { //Read number from the number array
num[]
         //And decryption, then store numbers in an new number array
         num2[j] = (num[j] * 25 + num[j + 1] * 11 + num[j + 2] * 18) % 26;
         num2[j + 1] = ( num[j] * 11 + num[j + 1] * 2 + num[j + 2] * 15 ) %
26;

         num2[j + 2] = ( num[j] * 9 + num[j + 1] * 6 + num[j + 2] *
14) %26;
```

```
        }
        for (i = 0; i < c.length; i++) { //Convert numbers to characters.
            c[i] = (char)(num2[i] + 65);
        }
        String arr2 = new String(c);
        System.out.println(arr2); //Print the plaintext
    }

}
```

Reference:

1. En.wikipedia.org. (2017). WannaCry ransomware attack. [online] Available at: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack [Accessed 14 Aug. 2017].