1. (a)

Obviously, if a(b) is prime number, c(d) must be a(b) or 1, so GCD(c,d) = 1

If a and b are not prime numbers:

$a = 1 \times P_1 \times P_2 \times \dots \times P_n,\ A = \{\mathrm{P} \mid P_{1\dots n}$ are prime numbers$\}$

$b = 1 \times Q_1 \times Q_2 \times \dots \times Q_n,\ B = \{\mathrm{Q} \mid Q_{1\dots n}$ are prime numbers$\}$

$\because \mathrm{GCD(a,b)} = 1$

$\therefore \{1, P_1, \dots, P_n\} \cap \{1, Q_1, \dots, Q_n\} = 1,\ \ i.e. \mathrm{A} \cap \mathrm{B} = \emptyset$

$\because \mathrm{c|a}$ and $\mathrm{d|b}$

$\therefore \mathrm{c} = 1 \times p_1 \times p_2 \times \dots \times p_n,\quad \mathrm{C} = \{\mathrm{p} \mid p_{1\dots n} \subseteq \mathrm{A}\}$

$\mathrm{d} = 1 \times r_1 \times r_2 \times \dots \times r_n,\quad \mathrm{D} = \{\mathrm{q} \mid q_{1\dots n} \subseteq \mathrm{B}\}$

$\because\ \mathrm{A} \cap \mathrm{B} = \emptyset\ and\ C \subseteq \mathrm{A}$ and $\mathrm{D} \subseteq \mathrm{B}$

$\therefore\ \mathrm{C} \cap \mathrm{D} = \emptyset$

$\therefore \{1, p_1, p_2, \dots p_n\} \cap \{1, r_1, r_2, \dots, r_n\} = 1,\ i.e. \mathrm{GCD(c,d)} = 1$

(b) i.

```
def ExtendedEuclid(a, b):
        remainder = -1
        x1 = 1
        x2 = 0
        y1 = 0
        y2 = 1
        if a > b:
                dividend = a
                divisor = b
        else:
                dividend = b
                divisor = a
        while remainder != 0:
                gcd = remainder
                quotient = dividend // divisor
                remainder = dividend % divisor
                temp1 = x1 - x2 * quotient
                x1 = x2
                x2 = temp1
                temp2 = y1 - y2 * quotient
                y1 = y2
                y2 = temp2
                dividend = divisor
                divisor = remainder
        if a > b:
                return [x1,y1,gcd]
        else:
                return [y1,x1,gcd]
```

ii.

```
def Inverse(a, n):
    remainder = -1
    x1 = 1
    x2 = 0
    y1 = 0
    y2 = 1
    dividend = n
    divisor = a

    while remainder != 0:
        gcd = remainder
        quotient = dividend // divisor
        remainder = dividend % divisor
        temp1 = x1 - x2 * quotient
        x1 = x2
        x2 = temp1
        temp2 = y1 - y2 * quotient
        y1 = y2
        y2 = temp2
        dividend = divisor
        divisor = remainder
    ‘‘‘
    If a and n are coprime, inverse of a mod n must exist and the program will return the
    inverse number. In contrast, if a and n are not coprime, inverse of a mod n doesn’t
    exist, so the program will output a string “a and n are not coprime”.
    ’’’
    if gcd == 1:
        if y1 > 0:
            return y1
        else:
            return y1 % n
    else:
        return 'a and n are not coprime!'
```

c.

https://asecuritysite.com/encryption/random3

This webpage is an online prime number generator, I entered 100 which means it will generate prime number of approximately 2^{100}.

p_1 = 1,039,723,492,994,222,382,182,965,778,357

p_2 = 482,825,924,593,761,590,482,585,731,907

n = 502,005,456,826,790,823,201,330,654,301,662,553,568,927,524,166,346,784,936,799

i.

a = 1,435,736,916,986,898,986,959,698,346,014,060,325

The inverse of a mod n is:

145,164,198,622,093,177,992,608,306,501,597,687,289,238,735,447,622,451,124,775

ii.

a = p_1 ∗ 13468 = 14,002,996,003,646,187,043,240,183,102,912,076

The output is:

a and n are not coprime!

iii.

a = 502,005,456,826,790,823,201,330,654,301,662,553,568,927,524,166,346,784,936,798

The inverse of a mod n is:

502,005,456,826,790,823,201,330,654,301,662,553,568,927,524,166,346,784,936,798

2. (a)

Security risk is the potential for violation of security, i.e. it can destroy security and cause damages and losses under appropriate conditions. It's dangers that may bring for the people when vulnerability is exploited.

Security attack is man-made security breach, i.e. it is an intelligent action that attempt to run counter to security rules and violate the system security policy.

Security attacks are classified into passive attacks and active attacks, thereinto, denial of service(DoS) is one of the active attacks. SYN Flood is the most common and the most effective DoS form. SYN Flood exploits the vulnerability of the TCP three-way handshake protocol. Firstly, A mass of SYN requests are sent to the server by attacker. Then the server will send SYN + ACK back to the attacker, however, attacker doesn't respond to these messages which result in a large amount of half-open connections. Finally, the server is overwhelmed owing to these fake TCP connections instead of real requests and this attack strategy is so called denial of service(DoS).

(b) i.

The decryption function is

$$\mathrm{p} = (\mathrm{c} - \mathrm{b})a^{-1} \bmod 28$$

ii.

a should have inverse, so a and 28 are coprime, i.e. GCD(a, 28) = 1.

a should belong to {1,3,5,9,11,13,15,17,19,23,25,27}.

b can take any value from integers modulo 26.

So the total non-trivial keys are 12 * 28 - 1= 335 (except a = 1, b = 0)

iii.

The complexity of Ciphertext only Attack is 336. The complexity of Chosen Plaintext Attack is only 1(Given 2 different plaintext the a and b can be solved directly). Due to the simplicity of encryption function, both of the computational complexity and space complexity are very low, so attacker can get the key easily by using Brute Force method.

3. (a)

From $k_{1,1}\ to\ k_{m,m}$, the amount of k is m^2. The range of k is [0,28], so the number of different possible keys is 29^{m^2}. However, considering the matrix properties, the matrix should be reversible, which means the determinant value cannot be 0. In order to meet this condition, matrix column cannot be all 0 and element value of one column cannot be a multiple of element value of another column. So:

$$\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{pmatrix}$$

The first column has $29^m - 1$ probabilities(except all 0s). The second column has $29^m - 29$ probabilities(except the multiple of the first column). The third column has $29^m - 29 - 29^2$ probabilities(except the multiple of the first column and the second column), and so on. Finally, the answer should be $(29^m - 1)(29^m - 29) * \dots * (29^m - 29^{m-1})$, and that is

$$29^{m^2}\left(1-\frac{1}{29}\right)\left(1-\frac{1}{29^2}\right)\dots(1-\frac{1}{29^m})$$

(b)

For m × m Hill cypher, suppose we have m plaintext – cyphertext pairs and the length of each plaintext is m.

$$\because (c_1, c_2, \dots c_m) = (p_1, p_2, \dots p_m)\begin{pmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mm} \end{pmatrix} mod\ 29$$

$$\therefore \begin{pmatrix} c_{11} & \cdots & c_{1m} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mm} \end{pmatrix} = \begin{pmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mm} \end{pmatrix}\begin{pmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mm} \end{pmatrix} mod\ 29$$

We have matrix C and matrix P, if we want to get the key matrix:

$$\therefore \begin{pmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mm} \end{pmatrix} = \begin{pmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mm} \end{pmatrix}^{-1}\begin{pmatrix} c_{11} & \cdots & c_{1m} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mm} \end{pmatrix} mod\ 29$$

If we want to get the key matrix, matrix P should have an inverse, then we can get the key by the above method. If P is not reversible, P can be modified by additional plaintext – ciphertext pairs until P is invertible.

(c)

The plaintext: CTRL, CAPS, HOME, PGUP

So, we have $\mathbf{P} = \begin{pmatrix} 2 & 19 & 17 & 11 \\ 2 & 0 & 15 & 18 \\ 7 & 14 & 12 & 4 \\ 15 & 6 & 20 & 15 \end{pmatrix}$

The cyphertext: JYZP, QEPQ, CHZS, GLXF

So, we have $\mathbf{C} = \begin{pmatrix} 9 & 24 & 25 & 15 \\ 16 & 4 & 15 & 16 \\ 2 & 7 & 25 & 18 \\ 6 & 11 & 23 & 5 \end{pmatrix}$

$\det(\mathbf{P}) = 2673 \bmod 29 = 5$

$\therefore (\det \mathbf{P})^{-1} = 6$

$\because [\mathbf{P}^{-1}]_{ij} = (\det \mathbf{P})^{-1}(-1)^{i+j}(\mathrm{D}_{ji})$

$\therefore \mathbf{P}^{-1} = \begin{pmatrix} 11 & 21 & 10 & 24 \\ 7 & 2 & 22 & 4 \\ 9 & 8 & 2 & 20 \\ 9 & 12 & 23 & 0 \end{pmatrix}$

$$\therefore \mathbf{K} = \mathbf{P}^{-1}\mathbf{C} = \begin{pmatrix} 11 & 21 & 10 & 24 \\ 7 & 2 & 22 & 4 \\ 9 & 8 & 2 & 20 \\ 9 & 12 & 23 & 0 \end{pmatrix} \begin{pmatrix} 9 & 24 & 25 & 15 \\ 16 & 4 & 15 & 16 \\ 2 & 7 & 25 & 18 \\ 6 & 11 & 23 & 5 \end{pmatrix} \mathit{mod}\ 29$$

$$= \begin{pmatrix} 599 & 682 & 1392 & 801 \\ 163 & 374 & 847 & 553 \\ 333 & 482 & 855 & 399 \\ 319 & 425 & 980 & 741 \end{pmatrix} \mathit{mod}\ 29 = \begin{pmatrix} 19 & 15 & 0 & 18 \\ 18 & 26 & 6 & 2 \\ 14 & 18 & 14 & 22 \\ 0 & 19 & 23 & 16 \end{pmatrix}$$

Similarly, $\mathbf{K}^{-1} = \begin{pmatrix} 22 & 0 & 22 & 3 \\ 21 & 1 & 22 & 4 \\ 8 & 9 & 19 & 0 \\ 27 & 4 & 10 & 8 \end{pmatrix}$

BGB.D,LYIQJNBGSQLXWRIIBKESOWGEWSXCCAC.ZCPPW.YIAFPDNBUDOBPSFIKBSTRIQQFDOUHBZSRXVULMI,JVSGFUUG

This is the cyphertext:

(1,6,1,27), (3,26,11,24), (8,16,9,13), (1,6,18,16), (11,23,22,17), (8,8,1,10), (4,18,14,22), (6,4,22,18), (23,2,2,0), (2,27,25,2), (15,15,22,27), (24,8,0,5), (15,3,13,1), (20,3,14,1), (15,18,5,8), (10,1,18,19), (17,8,16,16), (5,3,14,20), (7,1,25,18), (17,23,21,20), (11,12,8,26), (9,21,18,6), (5,20,20,6)

This is the plaintext:

(15,7,8,11), (14,18,14,15), (7,4,17,18), (28,0,18,10), (26,28,2,0), (13,28,7,20), (12,0,13,28), (8,13,6,4), (13,20,8,19), (24,28,2,14), (13,2,14,2), (19,28,0,28), (2,8,15,7), (4,17,28,22), (7,8,2,7), (28,7,20,12), (0,13,28,8), (13,6,4,13), (20,8,19,24), (28,2,0,13), (13,14,19,28), (17,4,18,14), (11,21,4,27)

PHILOSOPHERS ASK, CAN HUMAN INGENUITY CONCOCT A CIPHER WHICH HUMAN INGENUITY CANNOT RESOLVE.