Question 1

I believe integrity to be of the highest concern, followed closely by availability, and last confidentiality.

The low rank for confidentiality – which pertains to preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information – is because COVID passports should not need to hold confidential data other than the holder's name and vaccination record pertaining to the COVID vaccine. If it had been a vaccine passport that contained the holder's entire vaccination history, then that may be a cause of concern for confidentiality, but with COVID passports, there is not much dire consequences of someone finding out a person's COVID vaccination history.

On the flip side, with availability which pertains to timely and reliable access to and use of the information, it would be a concern depending on the situation; it may not be necessary for some rules such as the travel exemptions as these activities would likely need to go through an approval process and could therefore include the waiting time to access the holder's vaccination status on the COVID passport into the travel approval wait-time. However, in the case of needing to access and show proof of the holder's vaccination upon entry to a physical venue, the public would want to be as readily available and accessible to gain entry to a venue.

That said, I believe integrity to be of the utmost concern. Integrity refers to the avoidance of improper modification, destruction, or information non-repudiation and authenticity. Authenticity and integrity are extremely important in highly infectious pandemic situations where a case in public could lead to widespread disease. This means we cannot be allowing people to tamper with the vaccination record on their COVID passport, i.e. those not vaccinated cannot say that they are already fully vaccinated. This may arise especially if the difference in vaccination privileges become large. For example, with the mandatory full-vaccination rules on flights or for quarantine-free international travel, some people may lie about their vaccination status to get access to these privileges. In the case that these imposters contract the disease while being in the community, it would lead to drastic consequences. It is also a cause of concern to ensure the integrity and legality of the reason when considering those who cannot get the vaccination for valid reasons. According to the government, they would not want "vulnerable Australians excluded from society" and hence this would mean these holders should be able to enjoy the privileges of those fully vaccinated while not being vaccinated themselves, which is entirely different from just not wanting to be vaccinated. With this, we need to ensure anti-vaxxers who may not follow COVID safety guidelines do not forge the validity of their reasons. Lastly, we also want to protect holders against identity theft and against other people deleting one's vaccination record and impede on their vaccination privileges.

Question 2

a) $P = D_{(a,b)}(c) = (c - b)a^{-1} \bmod 27$

$a \in \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$

$b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$

b) A key can be any combination of a and b's possible values where a decryption algorithm can exist, i.e. a mod 27 must have an inverse, and hence must be relatively prime to 27, which means $\gcd(a, 27) = 1$

$18 \times 27 = 486$ keys (includes 1 trivial key when $a = 1$, $b = 0$)

c) Mono-alphabetic as it uses only one fixed alphabet as the key, which in this case is the characters in the English alphabet and the space character.

d) Knowing the language of the plaintext, the attacker can use statistics based on the frequency of letters in appearing in words in that language to calculate prior and posterior probabilities of a certain cipher character corresponding to a particular plaintext character. The attacker can then work out the probabilities of a and b being a particular number that match those character statistics or use it as heuristics until the attacker finds English words in the decrypted ciphertext.

e) With an oracle, we can perform a Known Plaintext Attack in order to find the key. Here, we can feed two sets of known plaintexts, one of which can be the alphabet $\mathcal{A}$, into the oracle, and with the two encrypted ciphertexts, we can form two pairs of linear equations,

$$P_1 \xrightarrow{Oracle,\ K} C_1$$
$$P_2 \xrightarrow{Oracle,\ K} C_2$$

These two pairs of linear equations can then be solved simultaneously to find the key.

Question 3

a)
```
import sys

def gcd(a, n):
  if a == 0:
    return 0
  if n == 0:
    return a

  quotient = a // n
  remainder = a % n
  return gcd(n, remainder)

a = int(sys.argv[1])
n = int(sys.argv[2])

if n != 0:
  g = gcd(a, n)
  print "gcd({}, {}): {}".format(a, n, g)

else:
  print "n must be > 0"
```

b) Assuming that the `gcd` function above is available to us,

```
import sys

def gcdExtended(a, n):

  if a == 0 :
```

```
    return n, 0, 1

  quotient = n // a
  remainder = n % a
  gcd, y, y1 = gcdExtended(remainder, a)

  x = y1 - quotient * y

  return gcd, x, y

a = int(sys.argv[1])
n = int(sys.argv[2])
if n != 0:
  g = gcd(a, n)
  print "gcd({}, {}): {}".format(a, n, g)

  if g != 1:
    print "No inverse"
  else:
  g, x, y = gcdExtended(a, n)
  inverse = x % n
    print "Inverse gcd({}, {}): {}".format(a, n, inverse)

else:
  print "n must be > 0"
```

c) 15 518 756

Question 4

a) Encryption function:
$C = E_K(P) = KP \bmod 41$ such that
$c_1 = (k_{1,1}\, p_1 + k_{1,2}\, p_2 + \cdots + k_{1,m}\, p_m) \bmod 41$
$c_2 = (k_{2,1}\, p_1 + k_{2,2}\, p_2 + \cdots + k_{2,m}\, p_m) \bmod 41$
…
$c_m = (k_{m,1}\, p_1 + k_{m,2}\, p_2 + \cdots + k_{m,m}\, p_m) \bmod 41$

$KP = C \bmod 41$
$K^{-1}KP = K^{-1}C \bmod 41$
$IP = K^{-1}C \bmod 41$, where I is the identity matrix

Hence decryption function:
$P = D_K(C) = K^{-1}C \bmod 41$ such that
$p_1 = (k_{1,1}^{-1}\, c_1 + k_{1,2}^{-1}\, c_2 + \cdots + k_{1,m}^{-1}\, c_m) \bmod 41$
$p_2 = (k_{2,1}^{-1}\, c_1 + k_{2,2}^{-1}\, c_2 + \cdots + k_{2,m}^{-1}\, c_m) \bmod 41$
…
$p_m = (k_{m,1}^{-1}\, c_1 + k_{m,2}^{-1}\, c_2 + \cdots + k_{m,m}^{-1}\, c_m) \bmod 41$

Putting C into column vectors, each with 5 rows (to match the number of columns of the key), then turning it into the corresponding number modulo 41,

$$C = \begin{bmatrix} 0 & S & 7 & \\ A & C & A & \\ N & D & 4 & \dots \\ J & O & R & \\ A & P & 8 & \end{bmatrix} = \begin{bmatrix} 26 & 18 & 33 & \\ 0 & 2 & 0 & \\ 13 & 3 & 30 & \dots \\ 9 & 14 & 17 & \\ 0 & 15 & 34 & \end{bmatrix}$$

Getting the inverse of *K,*

$$K = \begin{bmatrix} 29 & 1 & 5 & 0 & 26 \\ 28 & 17 & 38 & 25 & 8 \\ 37 & 40 & 1 & 26 & 14 \\ 40 & 33 & 31 & 34 & 14 \\ 31 & 23 & 29 & 12 & 23 \end{bmatrix} \bmod 41$$

$$K^{-1} \bmod 41 = \begin{bmatrix} 29 & 1 & 5 & 0 & 26 \\ 28 & 17 & 38 & 25 & 8 \\ 37 & 40 & 1 & 26 & 14 \\ 40 & 33 & 31 & 34 & 14 \\ 31 & 23 & 29 & 12 & 23 \end{bmatrix}^{-1} \bmod 41 = \begin{bmatrix} 27 & 10 & 7 & 32 & 10 \\ 24 & 17 & 37 & 1 & 8 \\ 32 & 21 & 19 & 4 & 37 \\ 19 & 40 & 25 & 15 & 8 \\ 7 & 22 & 36 & 25 & 24 \end{bmatrix}$$

Decrypting *C* to get the plaintext *P*,

$$P = \begin{bmatrix} 27 & 10 & 7 & 32 & 10 \\ 24 & 17 & 37 & 1 & 8 \\ 32 & 21 & 19 & 4 & 37 \\ 19 & 40 & 25 & 15 & 8 \\ 7 & 22 & 36 & 25 & 24 \end{bmatrix} \begin{bmatrix} 26 & 18 & 33 & \\ 0 & 2 & 0 & \\ 13 & 3 & 30 & \dots \\ 9 & 14 & 17 & \\ 0 & 15 & 34 & \end{bmatrix} \bmod 41$$

$$= \begin{bmatrix} 15 & 18 & 17 & \\ 7 & 14 & 18 & \\ 8 & 15 & 0 & \dots \\ 11 & 7 & 18 & \\ 14 & 4 & 10 & \end{bmatrix}$$

$$= \begin{bmatrix} P & S & R & \\ H & O & S & \\ I & P & A & \dots \\ L & H & S & \\ O & E & K & \end{bmatrix}$$

= PHILOSOPHERSASKCANHUMANINGENUITYCONCOCTACIPHERWHICHHUMANING ENUITYCANNOTRESOLVE00

b) To have a decryptable key, the key matrix needs to have an inverse, i.e. the determinant must be 1. The number of invertible matrices in an $n \times n$ matrix can be found using the following formula,

$$(q^n - 1)(q^n - q) \dots (q^n - q^{n-1}), \text{ where } q \text{ is the modulo number}$$

With the given 5×5 matrix with modulo 41, we get

$$\text{Number of Keys} = (41^5 - 1)(41^5 - 41)(41^5 - 41^2)(41^5 - 41^3)(41^5 - 41^4)$$
$$= 2035202662228623762273780093666508800000$$
$$\approx 2.035 \times 10^{40} \text{ keys}$$

If only considering 38 characters, we get

Number of Keys $= (38^5 - 1)(38^5 - 38)(38^5 - 38^2)(38^5 - 38^3)(38^5 - 38^4)$

$= 3038778550344504235129548652600006394880$

$\approx 3.039 \times 10^{39}$ keys

c) Getting the key matrix,

$$P = \begin{bmatrix} X & R & : & Q & 4 \\ Y & 5 & L & R & 8 \\ [& H & M & 6 & S \\ L & I & O & 1 & B \\ E & ; & P & 9 & J \end{bmatrix} = \begin{bmatrix} 23 & 17 & 36 & 16 & 30 \\ 24 & 31 & 11 & 17 & 34 \\ 40 & 7 & 12 & 32 & 18 \\ 11 & 8 & 14 & 27 & 1 \\ 4 & 37 & 15 & 35 & 9 \end{bmatrix}$$

$$C = \begin{bmatrix} [& B & 9 & Q & 1 \\ W & 0 & 4 & < & I \\ Q & A & 8 & A & M \\ : & 6 & C & N & T \\ 9 & 1 & U & Y & D \end{bmatrix} = \begin{bmatrix} 40 & 1 & 35 & 16 & 27 \\ 22 & 26 & 30 & 38 & 8 \\ 16 & 0 & 34 & 0 & 12 \\ 36 & 32 & 2 & 13 & 19 \\ 35 & 27 & 20 & 24 & 3 \end{bmatrix}$$

$KP = C \bmod 41$

$KPP^{-1} = CP^{-1} \bmod 41$

$KI = CP^{-1} \bmod 41$, where I is the identity matrix

$$P^{-1} \bmod 41 = \begin{bmatrix} 23 & 17 & 36 & 16 & 30 \\ 24 & 31 & 11 & 17 & 34 \\ 40 & 7 & 12 & 32 & 18 \\ 11 & 8 & 14 & 27 & 1 \\ 4 & 37 & 15 & 35 & 9 \end{bmatrix}^{-1} \bmod 41 = \begin{bmatrix} 6 & 14 & 11 & 6 & 32 \\ 11 & 31 & 9 & 3 & 1 \\ 37 & 23 & 32 & 31 & 23 \\ 21 & 25 & 30 & 25 & 37 \\ 32 & 36 & 25 & 32 & 0 \end{bmatrix}$$

$$K = \begin{bmatrix} 40 & 1 & 35 & 16 & 27 \\ 22 & 26 & 30 & 38 & 8 \\ 16 & 0 & 34 & 0 & 12 \\ 36 & 32 & 2 & 13 & 19 \\ 35 & 27 & 20 & 24 & 3 \end{bmatrix} \begin{bmatrix} 6 & 14 & 11 & 6 & 32 \\ 11 & 31 & 9 & 3 & 1 \\ 37 & 23 & 32 & 31 & 23 \\ 21 & 25 & 30 & 25 & 37 \\ 32 & 36 & 25 & 32 & 0 \end{bmatrix} \bmod 41$$

$$= \begin{bmatrix} 2746 & 2768 & 2724 & 2592 & 2678 \\ 2582 & 3042 & 2776 & 2346 & 2826 \\ 1738 & 1438 & 1564 & 1534 & 1294 \\ 1523 & 2551 & 1613 & 1307 & 1711 \\ 1847 & 2495 & 2063 & 1607 & 2495 \end{bmatrix} \bmod 41$$

$$= \begin{bmatrix} 40 & 21 & 18 & 9 & 13 \\ 40 & 8 & 29 & 9 & 38 \\ 16 & 3 & 6 & 17 & 23 \\ 6 & 9 & 14 & 36 & 30 \\ 2 & 35 & 13 & 8 & 35 \end{bmatrix}$$

Now let,

$$C = \begin{bmatrix} A & X & N \\ 8 & R & 6 \\ V & D & J \\ S & E & E \\ 3 & O & V \end{bmatrix} \ldots = \begin{bmatrix} 0 & 23 & 13 \\ 34 & 17 & 32 \\ 21 & 3 & 9 \\ 18 & 4 & 4 \\ 29 & 14 & 21 \end{bmatrix} \ldots$$

Following the encryption and decryption functions in 4a:
$C = E_K(P) = KP \bmod 41$
$P = D_K(C) = K^{-1}C \bmod 41$

Getting the inverse of *K,*

$$K^{-1} \bmod 41 = \begin{bmatrix} 40 & 21 & 18 & 9 & 13 \\ 40 & 8 & 29 & 9 & 38 \\ 16 & 3 & 6 & 17 & 23 \\ 6 & 9 & 14 & 36 & 30 \\ 2 & 35 & 13 & 8 & 35 \end{bmatrix}^{-1} \bmod 41 = \begin{bmatrix} 36 & 40 & 25 & 5 & 8 \\ 21 & 8 & 31 & 8 & 9 \\ 10 & 8 & 27 & 35 & 16 \\ 38 & 20 & 13 & 36 & 22 \\ 36 & 22 & 19 & 15 & 37 \end{bmatrix}$$

Decrypting *C* to get the plaintext *P*,

$$P = \begin{bmatrix} 36 & 40 & 25 & 5 & 8 \\ 21 & 8 & 31 & 8 & 9 \\ 10 & 8 & 27 & 35 & 16 \\ 38 & 20 & 13 & 36 & 22 \\ 36 & 22 & 19 & 15 & 37 \end{bmatrix} \begin{bmatrix} 0 & 23 & 13 \\ 34 & 17 & 32 \\ 21 & 3 & 9 \\ 18 & 4 & 4 \\ 29 & 14 & 21 \end{bmatrix} \ldots \bmod 41$$

$$= \begin{bmatrix} 34 & 34 & 29 \\ 16 & 9 & 4 \\ 6 & 32 & 39 \\ 25 & 24 & 12 \\ 30 & 33 & 7 \end{bmatrix} \ldots$$

$$= \begin{bmatrix} 8 & 8 & 3 \\ Q & J & E \\ G & 6 & = \\ Z & Y & M \\ 4 & 7 & H \end{bmatrix} \ldots$$

= 8QGZ48J6Y73E=MHE[34J8N0OU5AWM;KA;S8D4ID9F3:P0MN45N:MZP3

Question 5

a) $\gcd\big(f(x), g(x)\big)$,
$f(x) = (x+1)g(x) + 5x^2 - 27x$

$\gcd(g(x), 5x^2 - 27x)$,
$g(x) = \left(\frac{1}{5}x + \frac{7}{25}\right)(5x^2 - 27x) + \frac{289}{25}x + 6$

$\gcd\left(5x^2 - 27x, \frac{289}{25}x + 6\right)$,
$5x^2 - 27x = \left(\frac{125}{289}x - \frac{213825}{83521}\right)\left(\frac{289}{25}x + 6\right) + \frac{1282950}{83521}$

$\gcd\left(\frac{289}{25}x+6, \frac{1282950}{83521}\right)$,

$\frac{289}{25}x+6=\left(\frac{24137569}{32073750}x-\frac{83521}{213825}\right)\frac{1282950}{83521}+0$

The last non-zero remainder was a constant, which can be multiplied with any polynomial to get a specific polynomial $h(x)$. However, we only consider a polynomial to be divisible by another polynomial only if the last non-zero remainder was a polynomial, not a constant. Hence,

$\gcd\big(f(x), g(x)\big)=1$

b)
```
procedure PolynomialGCD(fx, gx)
  if fx == 0 then
    return 0
  end if

  if gx == 0 then
    return fx
  end if

  if gx == constant then
    return 1
  end if

  quotient, remainder <- polyLongDivision(fx, gx)
  return PolynomialGCD(gx, remainder)
```

c) `PolynomialGCD(f(x), g(x))`

$q=(x+1),\ r=(5x^2-27x)$ `<- polyLongDivision(f(x), g(x))`

`PolynomialGCD(gx,` $5x^2-27x$`)`

$q=\left(\frac{1}{5x}+\frac{7}{25}\right),\ r=\left(\frac{289}{25}x+6\right)$ `<- polyLongDivision(g(x),` $5x^2-27x$`)`

`PolynomialGCD(`$5x^2-27x$`,` $\frac{289}{25}x+6$`)`

$q=\left(\frac{125}{289}x-\frac{213825}{83521}\right),\ r=\left(\frac{1282950}{83521}\right)$ `<- polyLongDivision(g(x), r)`

`PolynomialGCD(`$\frac{289}{25}x+6$`,` $\frac{1282950}{83521}$`)`

$\frac{1282950}{83521}$ `== constant is` **`true`**`, so` **`return`** `1`

d) Using linear substitutions from (a),

$$\begin{aligned}\gcd\big(f(x), g(x)\big) &= 1\\ &= f(x)p(x)+g(x)q(x)\\ &= \left(\frac{289}{51318}x^2-\frac{653}{25659}x+\frac{473}{25659}\right)f(x)+\\ &\quad \left(-\frac{289}{51318}x^3+\frac{113}{5702}x^2-\frac{1085}{51318}x+\frac{7607}{51318}\right)g(x)\end{aligned}$$

Hence,

$$p(x) = \frac{289}{51318}x^2 - \frac{653}{25659}x + \frac{473}{25659}$$

$$q(x) = -\frac{289}{51318}x^3 + \frac{113}{5702}x^2 - \frac{1085}{51318}x + \frac{7607}{51318}$$

e) Let $h(x) = x^4 - 3x^3 - 5x^2 - 17x + 6$

$\gcd\big(g(x), h(x)\big)$,

$g(x) = (0)h(x) + g(x)$

$\gcd\big(h(x), g(x)\big)$,

$h(x) = (x+1)g(x) + (-5x^2 - 27x)$

$\gcd(g(x), -5x^2 - 27x\ )$,

$g(x) = \left(-\frac{1}{5}x + \frac{47}{25}\right)(-5x^2 - 27x) + \frac{1369}{25}x + 6$

$\gcd\left(-5x^2 - 27x, \frac{1369}{25}x + 6\right)$,

$-5x^2 - 27x = \left(-\frac{125}{1369}x - \frac{905325}{1874161}\right)\left(\frac{1369}{25}x + 6\right) + \frac{5431950}{1874161}$

$\gcd\left(\frac{1369}{25}x + 6, \frac{5431950}{1874161}\right)$,

$\frac{1369}{25}x + 6 = \left(\frac{2565726409}{135798750}x - \frac{1874161}{905325}\right)\frac{5431950}{1874161} + 0$

Using linear substitutions from above,

$$\gcd\big(g(x), h(x)\big) = 1$$
$$= \left(-\tfrac{1369}{217278}x^3 + \tfrac{473}{24142}x^2 - \tfrac{5585}{217278}x + \tfrac{29327}{217278}\right)g(x) + \left(\tfrac{1369}{217278}x^2 - \tfrac{2813}{108639}x + \tfrac{3443}{108639}\right)h(x)$$

Hence,

$$g(x)^{-1} \bmod h(x) = -\frac{1369}{217278}x^3 + \frac{473}{24142}x^2 - \frac{5585}{217278}x + \frac{29327}{217278}$$