Worked Example of Encrypting and then Decrypting a Single Plaintext Item.

(Recapping first of all on the general notes in the separate document called "Vector Factorising".)

Quote:

Let the general vector be $\underline{N} = \alpha.\hat{i} + \beta.\hat{j} + \gamma.\hat{k}$

And let $\varepsilon_x = g.c.d(\beta,\gamma)$, $\varepsilon_y = g.c.d(\alpha,\gamma)$, $\varepsilon_z = g.c.d(\alpha,\beta)$

The primary pair $\underline{V}_0$ and $\underline{V}_1$ are found at each of the intercepts in turn.

There are three possibilities for the three pairs of 'primary' vectors

At the ZY intercept (<= X =0)

$$\underline{V}_0 = \begin{pmatrix} 0 \\ \gamma/\varepsilon_x \\ -\beta/\varepsilon_x \end{pmatrix} \quad \text{and} \quad \underline{V}_1 = \begin{pmatrix} \varepsilon_x \\ y \\ -(\alpha.\varepsilon_x + \beta.y)/\gamma \end{pmatrix} \quad * \text{ y decides z}$$

At the ZX intercept (<= Y = 0)

$$\underline{V}_0 = \begin{pmatrix} -\gamma/\varepsilon_y \\ 0 \\ \alpha/\varepsilon_y \end{pmatrix} \quad \text{and} \quad \underline{V}_1 = \begin{pmatrix} -(\beta.\varepsilon_y + \gamma.z)/\alpha \\ \varepsilon_y \\ z \end{pmatrix} \quad * \text{ z decides x}$$

At the XY intercept (<= Z =0)

$$\underline{V}_0 = \begin{pmatrix} \beta/\varepsilon_z \\ -\alpha/\varepsilon_z \\ 0 \end{pmatrix} \quad \text{and} \quad \underline{V}_1 = \begin{pmatrix} x \\ -(\gamma.\varepsilon_z + \alpha.x)/\beta \\ \varepsilon_z \end{pmatrix} \quad * \text{ x decides y}$$

(The proof of these results is simply to multiply out ($\underline{V}_1$ x $\underline{V}_0$) and see if the result equals $\underline{N}$ - that was done).

Equations of lines that may then be used as 'factor' lines.

$\underline{V}n = \underline{V}_0 + n(\underline{V}_1 - \underline{V}_0)$
$\underline{V}n = \underline{V}_0 + n(\underline{V}_1 + \underline{V}_0)$
$\underline{V}n = \underline{V}_0 + n(\underline{V}_1)$
$\underline{V}n = \underline{V}_1 + n(-\underline{V}_0)$

* In the example being demonstrated next the first of each group i.e. the first primary pair above and the first line will be taken as the model for demonstrating.

The up-and-running cipher to hand (i.e. the one being offered to readers for free downloading called "Skew Line Encryptions") cycles continuously through all 12 combinations of primary factor pairs coupled with a different equation of line in regular practice, this goes on throughout the encryption of any file over its entire length.

Let the Normal vector that is chosen by Alice on this occasion be $\underline{N} = \begin{pmatrix} 8 \\ 6 \\ 15 \end{pmatrix}$

$$\varepsilon_x = \text{GCD } \{6.15\} = 3$$

$$\underline{V}_0 = \begin{pmatrix} 0 \\ \gamma/\varepsilon_x \\ -\beta/\varepsilon_x \end{pmatrix} \Rightarrow \underline{V}_0 = \begin{pmatrix} 0 \\ 15/3 \\ -6/3 \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \\ -2 \end{pmatrix}$$

$$\underline{V}_1 = \begin{pmatrix} \varepsilon_x \\ y \\ -(\alpha\,\varepsilon_x + \beta\, y)/\gamma \end{pmatrix} \Rightarrow \underline{V}_1 = \begin{pmatrix} 3 \\ y \\ -(8\times 3 + 6\cdot y)/15 \end{pmatrix} **$$

** y decides z here

when y = 1 z = $-30/15 = -2$ So,

$$\underline{V}_0 = \begin{pmatrix} 0 \\ 5 \\ -2 \end{pmatrix} \text{ and } \underline{V}_1 = \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix}$$

*always check that $\underline{V}_1 \times \underline{V}_0 = \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix} \times \begin{pmatrix} 0 \\ 5 \\ -2 \end{pmatrix} = \begin{pmatrix} 8 \\ 6 \\ 15 \end{pmatrix} = \underline{N}$ (OK)

Alice chooses a line in the plane that has the equation

$$\underline{V}n = \underline{V}_0 + n\,(\underline{V}_1 - \underline{V}_0)$$

$$\underline{V}_1 - \underline{V}_0 = \begin{pmatrix} 3 \\ -4 \\ 0 \end{pmatrix}$$

Explictly then, the equation of Alice's encryption line is,

$$\underline{V}n = \begin{pmatrix} 0 \\ 5 \\ -2 \end{pmatrix} + n \begin{pmatrix} 3 \\ -4 \\ 0 \end{pmatrix}$$

Let us say that Alice wants to encrypt
the letter 'P' - Alice's code-point number for 'P' in ASCII is 80 , so,

$$\begin{pmatrix} 0 \\ 5 \\ -2 \end{pmatrix} + 80 \begin{pmatrix} 3 \\ -4 \\ 0 \end{pmatrix} = \begin{pmatrix} 240 \\ -315 \\ -2 \end{pmatrix}$$

Alice's transformation for P is the position vector $\underline{P}n$ which is

$\underline{P}n = \begin{pmatrix} 240 \\ -315 \\ -2 \end{pmatrix}$ - this is her computed ***apparent*** ciphertext

Alice now claps a large and deliberately confusing ***change-of-origin*** vector of say

$\begin{pmatrix} 720 \\ -367 \\ 1100 \end{pmatrix}$ onto this computed vector $\underline{P}n$

So the eventual ciphertext becomes

$$\begin{pmatrix} 240 \\ -315 \\ -2 \end{pmatrix} + \begin{pmatrix} 720 \\ -367 \\ 1100 \end{pmatrix} = \begin{pmatrix} 960 \\ -682 \\ 1098 \end{pmatrix}$$

Bob receives this as the **de facto** ciphertext.

Consulting his mutual database Bob identifies the agreed change-of-origin and removes it from the ciphertext.

$$\begin{pmatrix} 960 \\ -682 \\ 1098 \end{pmatrix} - \begin{pmatrix} 720 \\ -367 \\ 1100 \end{pmatrix} = \begin{pmatrix} 240 \\ -315 \\ -2 \end{pmatrix}$$

Then Bob performs a counter transforming operation of $\underline{P}n \times \underline{V}_0$.

$$\begin{pmatrix} 240 \\ -315 \\ -2 \end{pmatrix} \text{ x } \begin{pmatrix} 0 \\ 5 \\ -2 \end{pmatrix} = \begin{pmatrix} 640 \\ 480 \\ 1200 \end{pmatrix} \text{ (this is Pn cross } \underline{V_0})$$

Then , dividing by the corresponding coefficients of $\underline{N}$

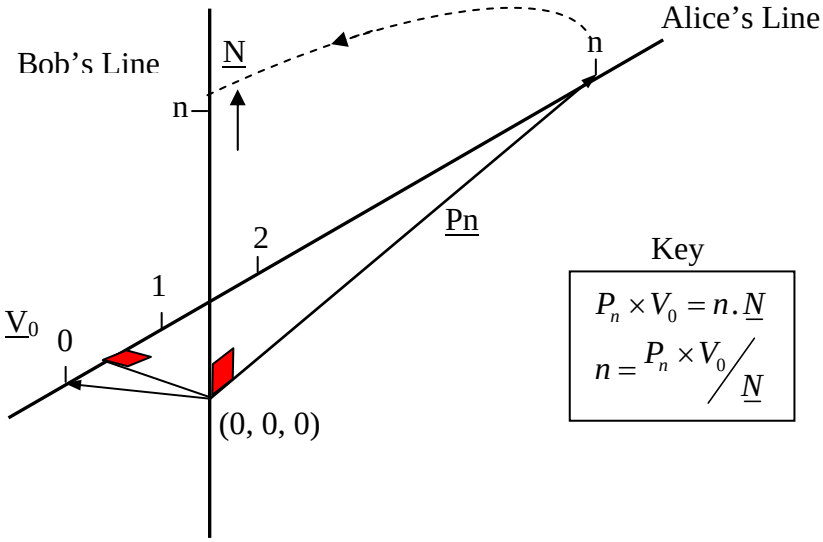
$$\frac{640}{8} = \frac{480}{6} = \frac{1200}{15} = \mathbf{80}$$

80 is decoded back into its ASCII equivalent to get the 'character 'P' as you would expect

---

Appendix - A.

The graphical transformation model shown here of Bob's analytical working is a pair of ***orthogonal skew lines*** that are related to each other in the amount of skew by means of the factoring of vectors methodology already described elsewhere - hence the cipher title "Skew Line Encryptions".



Any number that Alice puts or her line at encryption time, Bob is able to transfer and 'read' by rotating it on to his own line. The mathematical transforming operator that enables this to happen is the simple everyday cross-product. This is thought to be a rather elegant use of the vector cross product

---

Appendix - B

A personal stylised rule for doing the vector cross product is (again) $\Rightarrow$,

$\begin{pmatrix} a \\ b \\ c \end{pmatrix} cross \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} bf - ce \\ af - cd \\ ae - bd \end{pmatrix}$ - but don't forget, the reader must apply the sign matrix

$\begin{pmatrix} + \\ - \\ + \end{pmatrix}$ also - as is usual in the longer determinant method.

The 'rule' is,

To get the coefficient on the right, cover the corresponding row on the left and solve the determinant formed by the remaining two (uncovered) rows - very often this can be done in situ by inspection.

*The reader may want to experiment with encrypting other characters of ASCII also here rather than just 'P' in this demonstration.
