

Vector Factoring and Vector Cryptography.

This cryptography uses ‘directed number-lines’ being used instead of the universal number-line that may have arbitrary direction and which has been used in cryptography ever since the very beginning centuries ago. This means that the user of vector cryptography has a vast domain of number-lines to draw from whereas traditional cryptographers have had only one line ever that they were bound to use repeatedly for every encryption/decryption of any number of plaintext characters however great. Concealing their transformations of plaintext into ciphertext is extremely difficult and although it gives rise to some very fine algorithms that were elegant and intelligent they did not really do the job of complete obfuscation of the plaintext. The ciphers that they produced could never really shake off the threat of statistical cryptanalysis.

In vector cryptography the entities can use a different number-line for each and every encryption of a single plaintext and discard it immediately for a fresh line for the next plaintext.

In a nutshell, vector cryptography has an infinite number of number-lines that a cryptographer may use whereas traditional (scalar) cryptography has only one. In vector cryptography the number-line in hand each time begins in a fresh plane and is used to track the transformation of a plaintext to a unique point in three-dimensional space i.e. the transformation becomes a ‘displacement’ which is a vector quantity.

The innate perpendicular property of the humble ‘vector cross-product’ is a natural transforming operator that lends itself admirably to enable profoundly strong cryptography.

Because of using directed number-lines this cryptography requires a fairly advanced knowledge of vector methods in plane geometry.

I have created a cipher that is vector-based and it uses my personal invention of “Vector Factoring”. That cipher is called the ‘ASLEC’ cipher. ASLEC is an acronym of “Alternating Skew Line Encryption Cipher.

The general concept of ‘vector factoring’ and ‘vector cryptography’ is described here in this document but not the ASLEC cipher,

