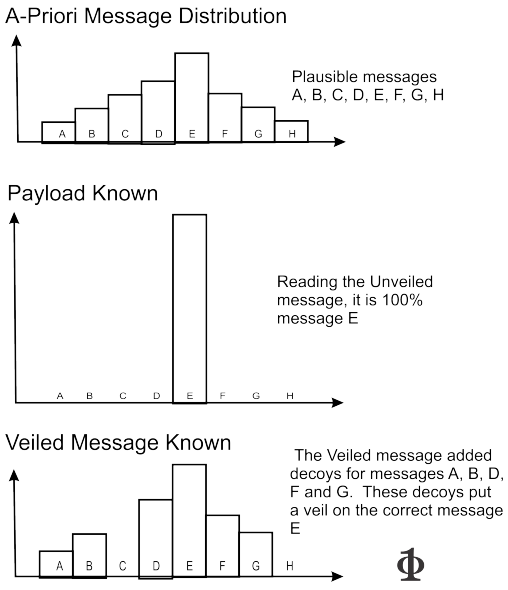
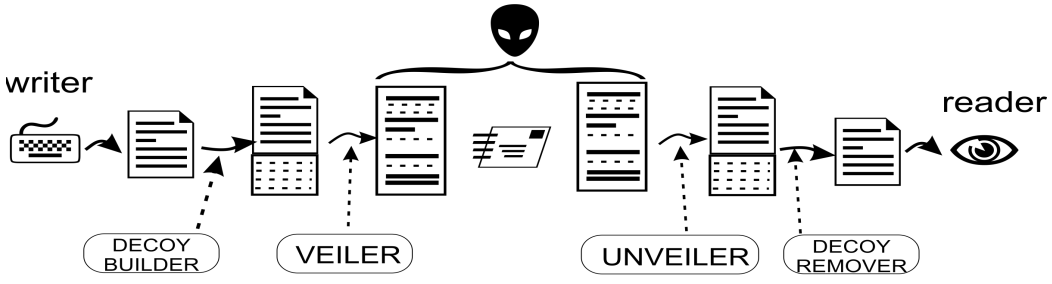
BitMint VEIL™

Protecting Your Unencrypted Files with AI-Built Decoys

Your Google traffic, your emails, your stored documents are all routinely scanned by content-inferring algorithms whether for good or for nefarious purposes -- assailing your privacy all the same. Encrypting a text document is an effective way to conceal its content, but the resultant ciphertext cannot be analyzed, categorized, nor sorted. Also cryptograms serve as hiding places for malware. There is a great advantage to keeping your content in the clear and with textual integrity. Which is what BitMint Veil does. Your text gets mixed with decoys: textual words and phrases that obfuscate the original meaning and message in the pre-mixed text. The intended reader will discard the 'chaff', and focus on the 'grain'. The electronic spy (or human spy) will either concede confusion, or worse, will draw a false conclusion, and ill-interpret the analyzed document. The BitMint Veil output is effective against quantum-computing and advanced math attack (It is based on the Equivoe-T™ technology that guarantees terminal equivocation). The protected clear text is subject to various scanning, sorting and aggregation. The Veil is fitted into the user's document handling system, and operates in the background. The document generating user is writing it normally. The document stores in a Veiled format, in which it is also transported, and stored on the reader's computer. The intended reader machine is loaded with the unveiling key, so that when the text is sent to the screen or to the printer, it comes forth "clean" just the original text, without the decoys. As more and more uninvited players take a peek at our online text, the need for the Veil is becoming more pronounced.

The Veil Hides Content without Encryption





Dolores Perillan, Dolores@BitMint.com