Homophonic ciphers

• Alphabetic substitution ciphers (both mono- and poly-) are susceptible to cryptanalysis via frequency methods. Because the English language possesses the characteristic that its letters are not uniformly distributed, cryptanalysts can employ this as a wedge to pry open the secret of the cipher.

• During the Renaissance, a number of cryptographers recognized this vulnerability and devised new methods for skirting this problem. One such was the homophonic cipher, in which the ciphertext alphabet is expanded to include many other symbols than the standard plaintext alphabet. This allows the cipher to substitute more than one ciphertext character for those plaintext letters that appear in language more often than others, in such a way that all cipher characters ultimately appear with roughly the same (uniform) frequency, removing frequency analysis as an effective method of cryptanalysis.

• The table below provides a homophonic cipher. It uses 104 ciphertext digraphs as substitutes for the 26 letters in English plaintext. It assigns $n$ digraphs to a letter when that letter has a frequency in English of roughly $n\%$. 
Cipher digraphs DN and BJ are considered **homophones** since they both substitute for the same plaintext letter g.
• The earliest homophonic cipher was the Great Cipher developed by the Rossignol brothers Auguste and Bonaventure in 1626 while in the employ of King Louis XIV of France. Their cipher was called a nomenclator cipher, since it was a mixture of a cipher with a code, and many of the codewords were selected from the list of names and places in the possession of the royal Nomenclator (the man who introduced dignitaries into the King’s presence).

• Another historically significant homophonic cipher was the famous second cipher in *The Beale Papers*, the only one of the three that appear in this document to be decrypted. It made use of the *Declaration of Independence* as the source of its cipher characters: each letter of the plaintext was encrypted as a number which identified the position of a work in the *Declaration* that began with that letter. Other book ciphers work similarly by using some accessible book (like a dictionary or the Bible) as a source of a large number of words; the ordinal numbers of the position of any word beginning with a plaintext letter are used as cipher characters.