Walaupun analisis frekuensi dapat sangat kuat dan menjadi teknik umum melawan banyak sandi, enskripsi masih sangat efektif dalam penerapannya, sebagaimana banyak kriptanalisis masih khawatir akan penerapannya. Memecahkan pesan tanpa menggunakan analisis frekuensi pada dasarnya membutuhkan pengetahuan sandi dan mungkin kunci yang digunakan, sehingga membuat spionase, penyuapan, pencurian, dll. Hal ini secara tegas mengakui kerahasiaan algoritme sandi pada abad 19 sangat tidak peka dan tidak menerapkan praktik keamanan pesan; faktanya, hal ini lebih lanjut disadari bahwa setiap skema kriptografi yang memadai (termasuk sandi) harus tetap aman walaupun musuh benar-benar paham tentang algoritme sandi itu sendiri. Keamanan kunci yang digunakan harus dapat menjamin keamanan pemegang kunci agar tetap rahasia bahkan ketika diserang sekalipun. Prinsip fundamental ini pertama kali dijelaskan pada tahun 1883 oleh *Auguste Kerckhoffs* dan secara umum dikenal dengan *Prinsip Kerckhoff*; secara alternatif dan blak-blakan, hal ini dijelaskan kembali oleh *Claude Shannon*, penemu teori informasi dan fundamental dari teori kriptografi, seperti *pribahasa Shanon* - 'musuh mengetahui sistemnya'.

Alat-alat bantu yang berbeda telah banyak digunakan untuk membantu sandi. Salah satu alat paling tua yang dikenali merupakan scytale dari Yunani, tangkai yang digunakan oleh Spartan sebagai alat bantuk untuk memindahkan sandi. Pada zaman pertengahan, alat bantu lainnya ditemukan seperti *jerejak sandi*, yang juga dikenal sebagai jenis steganografi. Dengan penemuan polialfabetik, sandi menjadi lebih mutakhir dengan bantuan disk sandi milik Alberti, skema *tabula recta Johanner Trithemius*, dan silinder multi *Thomas Jefferson* (tidak banyak diketahui, dan ditemukan kembali oleh *Bazeries* sekitar tahun 1900. Banyak alat