dan bertimbal-balik. Teks sandi yang dihasilkan dengan *sandi klasik* (dan beberapa sandi modern) selalu mengungkapkan informasi statistik tentang teks awal, yang sering dapat digunakan untuk memecahkannya. Setelah ditemukannya *analisi frekuensi* oleh matematikawan Arab dan *polymath* Al-Kindi (juga dikenal sebagai *Alkindus*) pada abad ke-9, hampir semua jenis sandi menjadi lebih sulit dipecahkan oleh penyerang yang memiliki informasi tersebut. Seperti sandi klasik yang masih populer hingga saat ini, meskipun lebih banyak dalam bentuk puzzle. Al-Kindi menuliskan buku kriptografi yang berjudul *Risalah fi Istikhraj al-Mu'amma* (*Risalah untuk Mnejermahkan Pesan Kriptografi*), yang menjelaskan teknik analisis frekuensi kriptanalisis yang pertama kalinya.

Pada dasarnya semua sandi tetap rentan kepada kriptanalisis menggunakan teknik analisis frekuensi hingga pengembangan dari sandi polyalphabetic, yang dijelaskan oleh *Leon Battista Alberti* sekitar tahun 1467, meskipun terdapat beberapa indikasi bahwa hal ini telah terlebih dahulu diketahui oleh Al-Kindi. Penemuan Alberti menggunakan sandi yang berbeda (seperti subtitusi alfabet) untuk beberapa bagian pesan (mungkin untuk setiap teks surat berturut-turut hingga akhir). Dia juga menemukan apa yang mungkin menjadi alat sandi ototmatis untuk pertama kalinya, roda yang menerapkan pelaksanaan dari penemuannya. Pada sandi Vigenère polyalphabetic, enkripsi menggunakan *kata kunci*, yang mengatur substitusi surat berdasarkan surat mana dari kata kunci yang digunakan. Pada pertengahan abad ke-19 Charles Babbage menunjukkan bahwa sandi Vigenère sangat rentan terhadap *pemeriksaan Kasiski*, tetapi hal ini diterbitkan pertama sekali kira-kira sepuluh tahun kemudian oleh Friedrich Kasiski.