

world' menjadi 'ehlol owrdl' pada skema perubahan sederhana ini), dan sandi substitusi, di mana secara sistematis mengganti huruf atau grup kata dengan kata lainnya dari grup kata (contoh 'fly at once' menjadi 'gmz bu podf' dengan mengganti setiap huruf dengan yang lain di alfabet Latin. Substitusi sandi pada awalnya disebut sandi Caesar, di mana setiap kata pada teks diganti dengan huruf dari jumlah tetap pada posisi di alfabet.

Laporan *Suetonius* menyebutkan Julius Caesar menggunakannya untuk berkomunikasi dengan jendral-jendralnya. *Atbash* merupakan contoh dari sandi Ibrani pada mulanya. Penggunaan awal kriptografi yang diketahui merupakan teks sandi yang diukir pada batu di Mesir (1900 sebelum Masehi), tetapi teks sandi ini digunakan hanya sebagai hiburan untuk pengamat terpelajar daripada cara untuk menyimpan informasi.

Yunani kuno menyebutkan telah mengetahui sandi (contoh sandi transposisi scytale yang diklaim telah digunakan oleh militer Sparta. *Steganograf* (menyembunyikan kehadiran pesan sehingga pesan tersebut menjadi rahasia) juga pertama kali diperkenalkan pada masa kuno. Contoh awal seperti, dari *Herodotus*, menyembunyikan pesan - sebuah tato pada kepala budaknya - di bawah rambut yang kembali tumbuh. Contoh yang lebih modern dari steganografi termasuk penggunaan tinta tak tampak, mikrodot, dan tanda air digital untuk menyembunyikan informasi.

Di India, *Kamasutra* dari *Vātsyāyana* yang berumur 2000 tahun berbicara dengan dua jenis sandi yang berbeda yang disebut Kautiliyam dan Mulavediya. Di Kautiliyam, substitusi kata sandi berdasarkan relasi fonetik, seperti vokal menjadi konsonan. Di Mulavediya, alfabet sandi terdiri dari kata-kata yang berpasangan