Kroz cijelu povijest čovječanstva postojala je potreba za sigurnom razmjenom informacija. Problemom sigurne komunikacije bavili su se već Egipćani i Indijci prije više od 3000 godina i od tada do danas osnovna ideja se nije promijenila – prenijeti neku poruku s jednog mjesta na drugo što je sigurnije moguće, tj. napraviti algoritam koji bi omogućio skrivanje originalne poruke tako da bude potpuno (u idealnom slučaju) nerazumljiva osobama koje bi neovlašteno došle u njen posjed. Prve korištene metode nisu bili složeni matematički algoritmi nego se počelo korištenjem alternativnih jezika koji su bili poznati samo malom broju ljudi. Razvoj složenijih metoda sigurne komunikacije počeo je tek razvojem pisma, što je omogućilo da se bilo koja informacija prikaže određenim brojem znakova koji bi, nakon upotrebe određenog ključa, formirali ponovno početnu poruku. S vremenom se javila i ideja prikaza slova drugim simbolima. Primjeri koji su i danas u upotrebi su: Morseov kod, Braille-ovo pismo i ASCII kod.