Kryptografie neboli **šifrování**

je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Slovo kryptografie pochází z řečtiny – *kryptós* je skrytý a *gráphein* znamená psát. Někdy je pojem obecněji používán pro vědu o čemkoli spojeném se šiframi jako alternativa k pojmu **kryptologie.** Kryptologie zahrnuje kryptografii a kryptoanalýzu, neboli luštění zašifrovaných zpráv.

Kryptografie se po staletí vyvíjela k větší složitosti zároveň s lidskou civilizací a mnohokrát ovlivnila běh dějin. Zejména utajení či vyzrazení strategických vojenských informací může mít zásadní vliv. Ale také prozrazení politických intrik, přípravy atentátů nebo i jen prozrazení milenců a podobně, to vše může úzce záviset na bezpečném přenosu informací a na schopnostech protivníka šifru rozbít. První doložení o zašifrování zprávy pochází z roku 480 př. n. l. za období Řecko-Perských válek v bitvě u Salamíny. Do historie kryptografie se zapsal i významný římský vojevůdce a politik Julius Caesar, a to vynalezením šifry, která byla pojmenována jako Caesarova šifra.

Celé období kryptografie můžeme rozdělit do dvou částí. Tou první je klasická kryptografie, která přibližně trvala do poloviny 20. stol. První část se vyznačovala tím, že k šifrování stačila pouze tužka a papír, případně jiné jednoduché pomůcky. Během 1. poloviny 20. stol. ale začaly vznikat různé sofistikované přístroje, které umožňovaly složitější postup při šifrování. Tím přibližně začala druhá část, kterou nazýváme moderní kryptografie. V dnešní době se k šifrování zpravidla nepoužívají žádné zvlášť vytvářené přístroje, ale klasické počítače.