

Dagli antichi intrighi diplomatici alla diffusione della comunicazione elettronica e all'enorme mole di messaggi che si scambiano in questa forma, la crittografia ha svolto un ruolo cruciale nella storia divenendo una disciplina critica e complessa. Scopo di questo volume è darne una presentazione che associ il rigore matematico a una ragionevole semplicità di comprensione.

Il testo è nato nell'ambito dell'insegnamento universitario, ma è destinato anche agli operatori e agli utenti delle reti di calcolatori, che potranno apprendervi come funzionano i sistemi crittografici e cosa ci si possa legittimamente attendere da essi.

Poiché è impossibile affrontare oggi gli studi di crittografia senza passare attraverso l'algoritmica, il testo dedica una parte iniziale ai concetti di base di questa scienza prima di presentare i cifrari attuali, i loro prevedibili sviluppi, i problemi di riservatezza e protezione delle comunicazioni che nascono dall'impiego delle reti; e si conclude con la discussione del sistema crittografico maggiormente usato oggi su Internet.