

## Obsah

O české kryptologii	9
Úvod	12
1 Šifra Marie Stuartovny	17
Vývoj tajného písma	19
Arabští kryptoanalytici	28
Luštění šifry	33
Renesance na Západě	39
Babingtonovo spiknutí	44
2 Le chiffre indéchiffrable	56
Od Vigenèra k Muži se železnou maskou	61
Černé komnaty	68
Pan Babbage versus Vigenèrova šifra	71
Od sloupků utrpení k zakopanému pokladu	85
3 Mechanizace utajení	104
Svatý grál kryptografie	116
Vývoj šifrovacích strojů – od šifrovacích disků k Enigmě	124
4 Boj s Enigmou	141
Husa, která nikdy nezaštěbetala	156
Jak unést knihu kódů	175
Anonymní kryptoanalytici	178
5 Jazyková bariéra	183
Luštění ztracených jazyků a starých písem	193
Záhada lineárního písma B	206
Přemosťující slabika	213
Lehkovážná odbočka	218



6	Alice a Bob se baví veřejně	230
	Bůh odměňuje blázny	239
	Zrození kryptografie s veřejným klíčem	253
	Podezřelá prvočísla	256
	Alternativní historie kryptografie s veřejným klíčem	263
7	Docela dobré soukromí	275
	Šifrování pro masy... Nebo ne?	284
	Zimmermannova rehabilitace	295
8	Kvantový skok do budoucnosti	298
	Budoucnost kryptoanalýzy	299
	Kvantová kryptografie	311
	Dešifrovací soutěž	329
	Dodatky	345
	Slovníček	361
	Poděkování	365
	Doporučená literatura	369
	Rejstřík	376