

Obsah

ÚVOD | **Tvůrci versus luštitelé** 6

1. KAPITOLA | **Starověké šifry** 10

Umění tajného písma • Transpoziciční šifry

2. KAPITOLA | **Arabské anagramování** 20

Tajný jazyk • Frekvence písmen v angličtině • Mukaddima a Prozření slepého • Výuka luštění

3. KAPITOLA | **Evropští šifrátoři** 32

První špioni • Le chiffre indéchiffrable • Homofonická substituce

4. KAPITOLA | **Rozluštění nerozluštitelného** 44

Jak rozluštit le chiffre indéchiffrable • Playfairova šifra • Bealeovy papíry

5. KAPITOLA | **Místnost 40** 58

Rádiová komunikace • Sloupcová transpozice • Zimmermannův telegram
Německé polní šifry • Jednorázové heslo

6. KAPITOLA | **Zrození mechanizace** 72

Kola v kolech • Wheatstoneova šifra

7. KAPITOLA | **Vytvoření Enigmy** 92

Scherbiusův stroj

8. KAPITOLA | Rozluštění Enigmy 100

Polská zpravodajská služba • Francouzské štěstí • Bomba

9. KAPITOLA | Bletchley Park 112

Škola šifer • Přesun do Bletchley • Námořní kódy • Ultra

10. KAPITOLA | Červený a fialový 130

Americká rozvědka a japonské šifry • Spojené přepínače • Zásadní vojenská rozvědka

11. KAPITOLA | Japonské námořní šifry 140

JN25 • Jednotka bojového zpravodajství • Přípravy na válku • Vyhlášení války

12. KAPITOLA | Kryptologie vrací úder 154

Stanice Hypo • Midway

13. KAPITOLA | Počítačová kryptoanalýza 162

„Tunny“ • Diferencování • Colossus

14. KAPITOLA | Kryptografie ve studené válce 172

Špiónské kruhy • Sněžení

15. KAPITOLA | Počítače přebírají vládu 178

Jiný svět, stejná tajemství • Distribuce klíčů

16. KAPITOLA | Konec luštění šifer, jak ho známe? 192

Digitální revoluce • Další způsoby útoku

SLOVNÍČEK 202

REJSTRÍK 206