

Spis treści

Przedmowa	9
Od autora	15
Wprowadzenie	17
Uwertura	17
Akt pierwszy – na scenie pojawia się Marian Rejewski	24
Akt drugi – w Getyndze i Poznaniu	26
Akt trzeci – w Biurze Szyfrów	28
Nieco o szyfrowaniu	30
Szyfry podstawieniowe monoalfabetyczne – <i>literówki</i>	30
Szyfr cezara (prosty) – „szyfr cykliczny”	30
Szyfr Argentiego, tzw. szyfr „cezara z hasłem”	31
Narodziny kryptoanalizy	33
Szyfry podstawieniowe polialfabetyczne	39
Szyfr Trithemiusa	39
Szyfr Vigenère’a	41
Atak Kasiskiego	44
Trochę o maszynach szyfrujących	46
Dysk Albertiego	46
Elektromechaniczne maszyny szyfrujące	51
Historia elektromechanicznych maszyn szyfrujących	54

Tajemnice wojskowej <i>enigmy</i>	60
Budowa wojskowej <i>enigmy</i>	63
Klucze	67
Atak na wojskową <i>enigmę</i>	69
Prefiks z kluczem sesyjnym	69
Przekazywanie kluczy	71
Charakterystyki dnia	76
Podejście heurystyczne	83
Metoda kluczy charakterystycznych	83
Metoda statystyczna	84
Metoda nierównych liter	85
Fabryka AVA	85
Historia toczy się dalej	87
Zmiany w życiu prywatnym Rejewskiego	87
Katalog cykli	88
Metoda „słów prawdopodobnych”	90
Koincydencja liter	92
Zmiany w systemie szyfrowania	97
Zawierucha wojenna	109
Spotkanie w Pyrach	109
Exodus we wrześniu 1939 roku	110
Francja	115
Tułaczka	120
Epilog	123
Dodatek A – Spadkobiercy	137
Bletchley Park	137
<i>Collossus</i>	140
Japońska maszyna <i>purple</i>	141
Dodatek B – Szyfry przestawieniowe	145

Szyfr plotowy	145
Spartańska skytala	146
Szablony (<i>patrony</i>) Fleissnera	146
Niemiecki szyfr podstawieniowy pojedynczy	149
Niemiecki szyfr podstawieniowy podwójny	154
Dodatek C – Szyfry poligraficzne	165
Szyfr Playfaira	166
Szyfr <i>Doppelkasten-Vefahren</i> (metoda podwójnej kaszty)	178
Literatura	185
Indeks	189