

Spis treści

Rozdział I – Wprowadzenie do szyfrów 9

1. Rola szyfrów w historii: ich zastosowanie na wojnach, w dyplomacji i na innych polach 9
2. Szyfry przez wieki 13

Rozdział II – Szyfry starożytne 28

1. Egipskie hieroglify: od pisma jerozolimskiego do Atbasha 28
2. Atbash – szyfr Biblii 37
3. Skytale – szyfry starożytnej Grecji. Szyfr Polibiusza. Początki stenografii 42
4. Szyfr Cezara: prostota i skuteczność 48
5. Wielkie cywilizacje Azji: szyfry w Chinach i Japonii 53

Rozdział III – Szyfry średniowieczne 59

1. Legendy i rzeczywistość szyfrów templariuszy. Szyfry krzyżaków 59
2. Dar od boga Odyna: pismo runiczne Wikingów 69
3. Początki szyfrów polialfabetycznych: Tarcza Albertiego, Tabula recta Trithemiusa 74
4. Nomenklator – podpowiadający imiona 83
5. Kryptoanaliza al-Kindiego. Szyfry homofoniczne 85

Rozdział IV – Szyfry renesansu i oświecenia 91

1. Cyfra Pana: szyfr Bellasa 91
2. Rzecz o przejmowaniu pomysłów – szyfr Vigenère'a 94
3. Kompromitujący syn – szyfr Jana Żdżarowskiego 108
4. Sherlock Holmes i szyfr książkowy 112
5. Królowa na szafocie – szyfr Marii Stuart 117
6. Wielki Szyfr (*Grand Chiffre*) – tajna broń Ludwika XIV 129

Rozdział V – Szyfry „made in USA” 135

1. Wojna o niepodległość: Thomas Jefferson i Szyfr Powtórzeń 135
2. Bratobójczy konflikt: szyfry wojny secesyjnej 145

Rozdział VI – Szyfry „wieku pary i elektryczności” 157

1. Szyfr Playfair sir Charlesa Wheatstone'a 157
2. Złoty żuk – jak amerykański pisarz przyczynił się ocalenia polskiej niepodległości 162

3. Książę Czartoryski i szyfry Agencji Wschodniej 168
4. Zaszifrowana Literatura: Szyfry rosyjskich dyplomatów, wojskowych i rewolucjonistów 175

Rozdział VII – Kryptologia w czasie I wojny światowej 190

1. Telegram Zimmermanna 190
2. Niemożliwy do złamania – szyfr z kluczem jednorazowym Vernama 201
3. ADFGX/ADFGVX – kod, który przypominał czary. ÜBCHI. ABC. „Oko bóstwa” 207
4. Andreas Figl i Hermann Pokorny: szyfry CK Austrii 220
5. Bądź jak „Skała” – szyfry armii Imperium Rosyjskiego 227

Rozdział VIII – Jan Kowalewski i Cud nad Wisłą 248

Rozdział IX – II wojna światowa 263

1. Sekret Enigmy 263
2. Purpurowy kod 282
3. „Zaszifrowane” dziewczyny: rola kobiet w amerykańskiej kryptologii 298
4. Diné bizaad – język, który stał się bronią 307
5. Mikropunkty Abwehry. „Ryba” i „Tuńczyk” 317
6. Sowieckie szyfry 324

Rozdział X – Zimna wojna i nowoczesna kryptologia 334

1. Projekt Venona: rozpracowanie sowieckich szyfrów 334
2. Przejęcie USS „Pueblo”. VIC. Szyfry „gorącej linii” 347
3. RSA i kryptografia asymetryczna: rewolucja w dziedzinie bezpieczeństwa 362

EPILOG – Nowe wyzwania: szyfry w erze cyfrowej 378

Bibliografia 387