

Spis treści

	Str.
Enigma — krótki rys historyczny	7
1. Geneza powstania, konstrukcja i sposób użycia maszyny szyfrującej typu Enigma	39
1.1. Wstęp	39
1.2. Konstrukcja maszyny szyfrującej Enigma typu wojskowego	45
1.3. Porównanie Enigmy wojskowej z innymi szyfrowymi maszynami wirnikowymi okresu II wojny światowej	52
ELEMENTY TEORII PERMUTACJI	59
<i>A. Pojęcia podstawowe</i>	<i>59</i>
1.4. Trzy tajemnice szyfru maszynowego	64
1.4.1. Połączenia wirników i inne cechy konstrukcyjne Enigmy	64
1.4.2. Tabele kluczy dziennych	68
1.4.2.1. Porządek bębneków	70
1.4.2.2. Usytuowanie pierścieni	70
1.4.2.3. Połączenia wtyczkowe	71
1.4.2.4. Pierwotne pozycje bębneków	72
1.4.3. Klucz depeszy	73
2. Metody odtworzenia połączeń wirników szyfrujących i innych elementów konstrukcji maszyny	75
2.1. Notka historyczna	75
ELEMENTY TEORII PERMUTACJI	78
<i>B. Twierdzenie o iloczynie transpozycji</i>	<i>78</i>
<i>C. Permutacje podobne</i>	<i>80</i>
2.2. Opis kryptologiczny	85
2.2.1. Wstępna analiza początków depeszy	85
2.2.2. Charakterystyka dnia	88
2.2.3. Jednoznaczne określenie permutacji A, B, C, D, E i F	89

2.2.4.	Układ równań	92
2.2.5.	Odtworzenie permutacji H	95
2.2.6.	Znalezienie połączeń wirników szyfrujących przy założeniu znajomości połączeń wtyczkowych	99
2.2.7.	Znalezienie połączeń wirników szyfrujących przy nieznanym połączeniach wtyczkowych	104
3.	Metody odtwarzania kluczy dziennych	112
3.1.	Metoda „rusztu”	112
3.1.1.	Odtwarzanie permutacji $A \div F$ (znajdowanie kluczy depesz)	112
3.1.2.	Określanie numeru prawego bębna (metoda zegara Różyckiego)	120
	ELEMENTY TEORII PERMUTACJI	123
	<i>D. Schemat mnożenia permutacji o pewnej charakterystycznej postaci</i>	123
3.1.3.	Określanie połączeń łącznicy (metoda „rusztu”)	124
3.1.4.	Wyznaczanie położenia wirnika środkowego i lewego (katalog permutacji T')	130
3.1.5.	Znajdowanie położenia pierścieni (metoda anx)	130
3.2.	Katalog charakterystyk	132
3.3.	Polskie bomby kryptologiczne	136
3.4.	Plachty (arkusze perforowane Zygałskiego)	139
3.5.	Typy Herivela i „głupstewka” (<i>Herivel tips and „sillies”</i>)	143
3.5.1.	Odtwarzanie położenia pierścieni	144
3.5.2.	Odtwarzanie kolejności bębneków na osi i połączeń łącznicy	144
3.6.	Angielski: bomby kryptologiczne	148
3.6.1.	„Ściągawki” (<i>cribs</i>)	149
3.6.2.	Zasada działania bomby kryptologicznej	150
3.6.3.	Budowa bomby kryptologicznej i schemat połączeń realizowany przez odpowiednie nastawienie bomby	153
	Zakończenie	158
	Bibliografia	161
	Załącznik 1 Program symulacji Enigmy wojskowej	162
	Załącznik 2 Ruszt Rejewskiego	185