AZ ENIGMA FELTÖRÉSE

Szemelvények a matematika történelméből

Erdély Martin

2

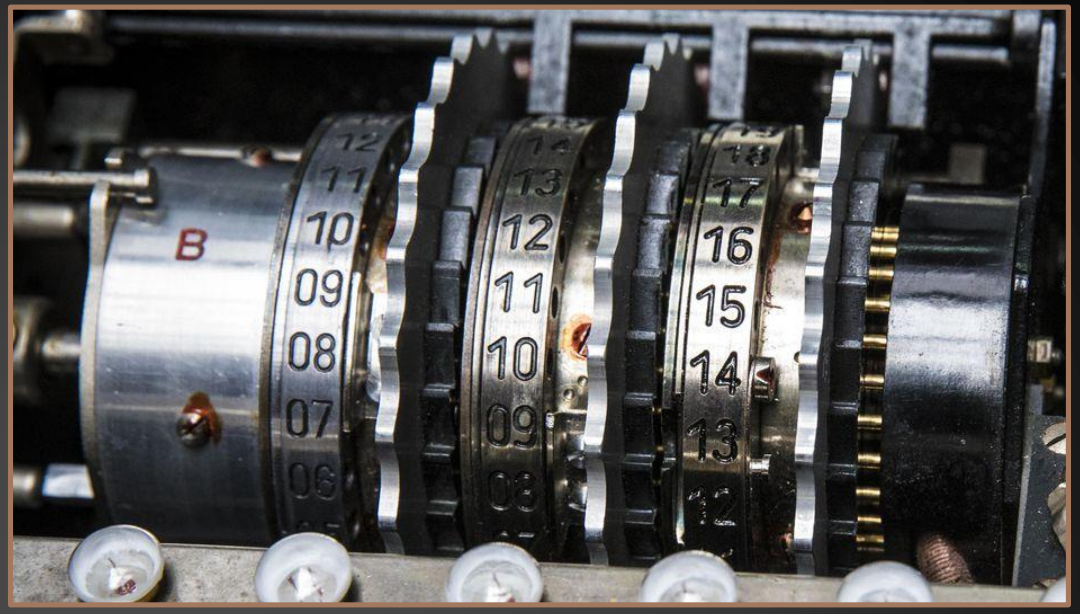
ENIGMA

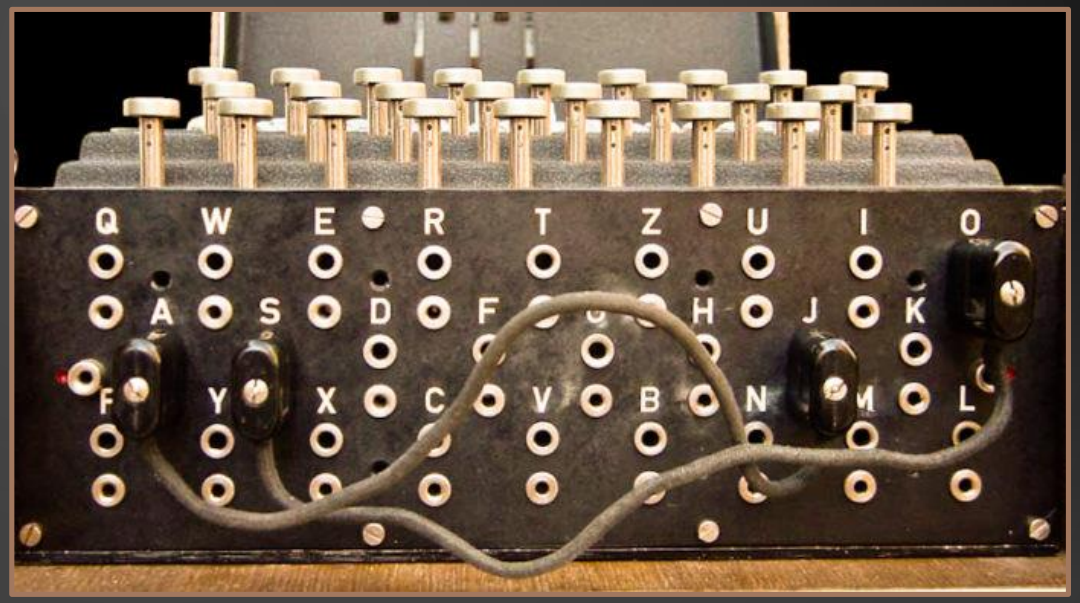
- Német találmány
- Szöveg kódolására, dekódolására használható
- Forradalmi rejtjelezés
- Akkoriban feltörhetetlennek gondolták

FELÉPÍTÉSE

- Billentyűzet
- Indikátor lámpák
- Forgótárcsák
- Kapocstábla

4


B
10
09
08
07
12
11
10
09
16
15
14
13


Q W E R T Z U I O
A S D F H J K
F Y X C V B N M L

MŰKÖDÉSE

- Gomb lenyomásakor zárul az áramkör az áramforrás és egy lámpa között
- 5 féle forgótárcsa, 3 hely
- Billentyű leütésére egy vagy több tárcsa léptetése
- Kapocstáblán betűpárok felcserélhetők, németek 10 betűpárt cseréltek fel

6

ÖSSZES LEHETSÉGES KEZDŐPOZÍCIÓ

Forgótárcsák lehetséges elrendezése:

5*4*3 = 60

Forgótárcsák állásainak száma:

26*26*26 = 17,576

Kapocstábla lehetséges kábelezése 10 párnál:

$$\frac{\binom{26}{2} * \binom{24}{2} * \binom{22}{2}_{*\cdots*}\binom{8}{2}}{10!} = \mathbf{150{,}738{,}274{,}937{,}250}$$

ÖSSZES LEHETSÉGES KEZDŐPOZÍCIÓ

60 * 17,576 * 150,738,274,937,250 =

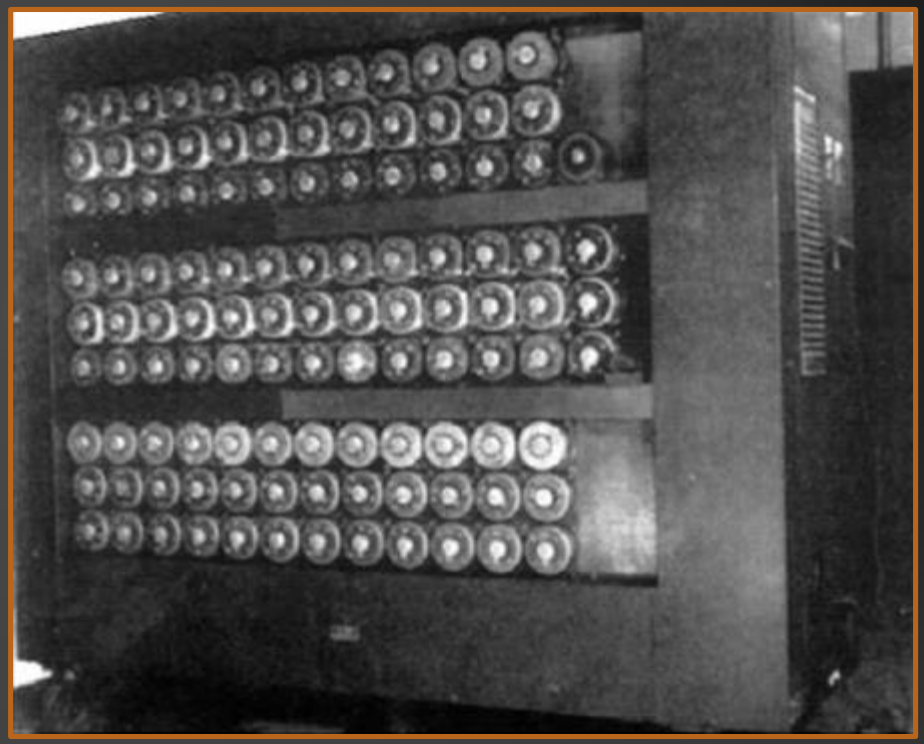
158,962,555,217,826,360,000

MI TETTE LEHETŐVÉ A FELTÖRÉSÉT?

- Adott betű sosem lehet önmaga kódolva
- Ismétlődő kiszámítható üzenetek, mint például a reggelenkénti időjárásjelentés
- Német szavak hosszúsága
- Enigma megszerzése, elemzése

TURING BOMBA

- Alan Turing
- Gordon Welchman
- Elektromechanikus
- Cél megfejteni a forgótárcsák pozícióját és kezdőállását, illetve néhány összekötést a kapocstáblán
- Tartalma 36 enigmával egyenértékű



FELÉPÍTÉS

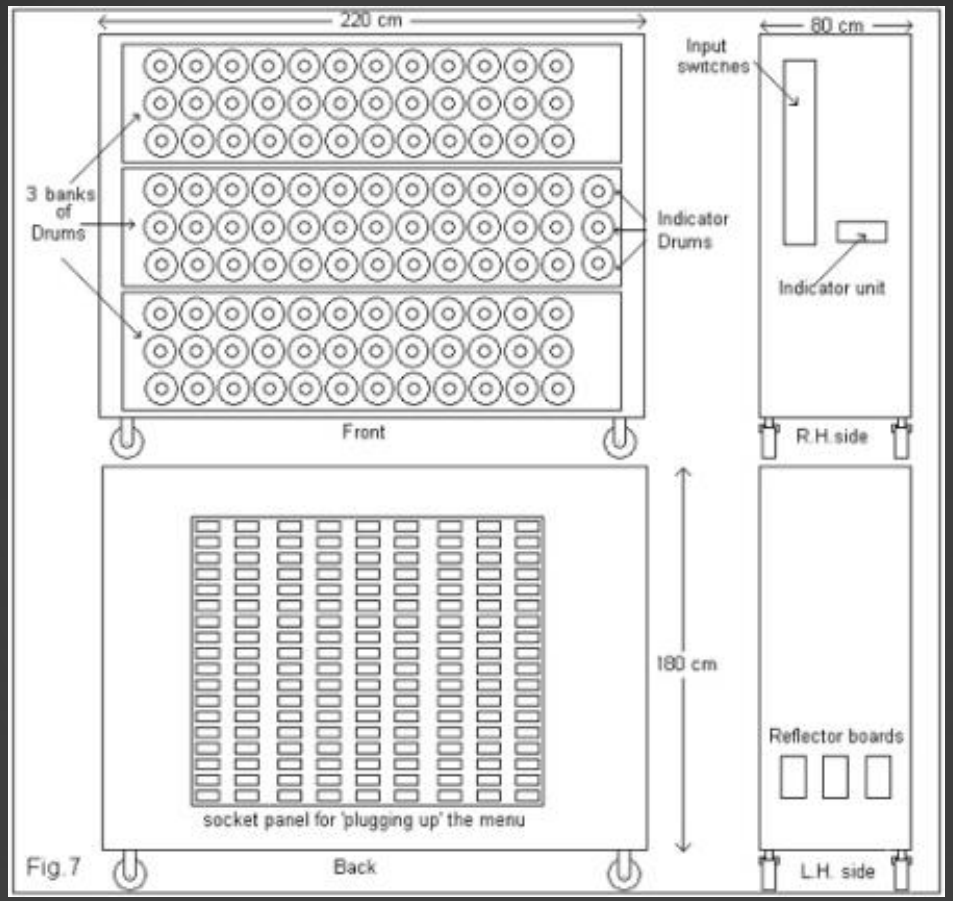
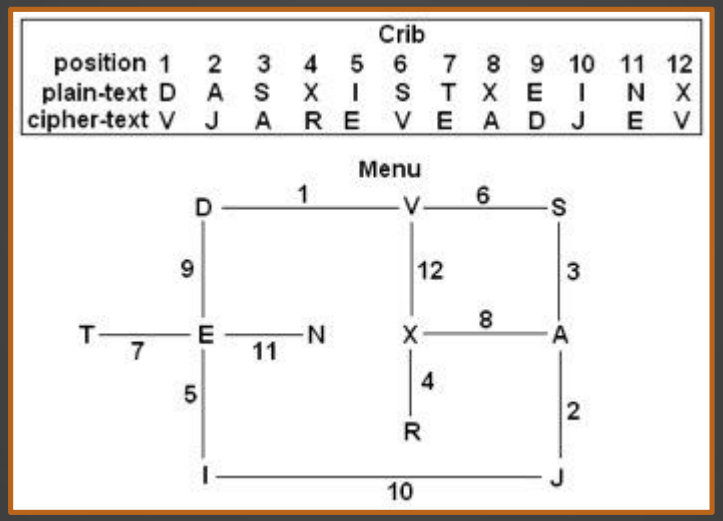


Fig.7

LEHETŐSÉGEK LECSÖKKENTÉSE

- „Crib” és menü használata

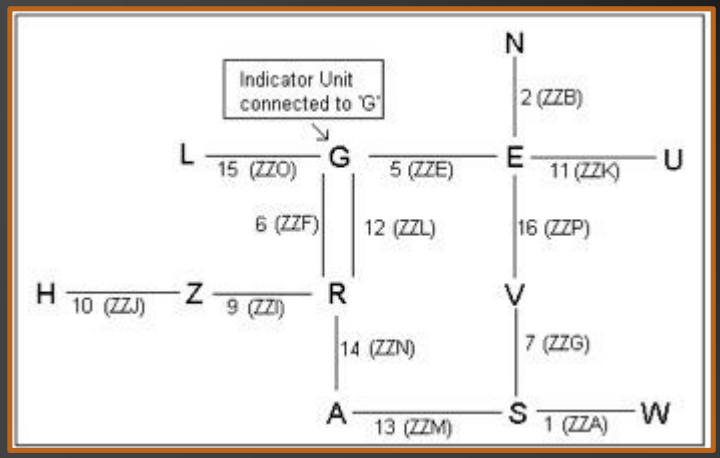


LEHETŐSÉGEK LECSÖKKENTÉSE

Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E	Z
			W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A			

MŰKÖDÉS

- A bomba ellentmondásokat keres
- A gép kizárja az ellentmondásos kezdőbeállításokat
- Ellentmondás hiányában megáll
- False stop – good stop
- Átlagosan 18 perc



ÚJRAÉPÍTÉS

2008-ban újraépítették, Bletchley Park Múzeumban a mai napig megtekinthetőműködés közben.

TOVÁBBI ANYAGOK

- 2014-ben megfilmesítették Kódjátszma néven
- Működő online szimulátor: http://www.lysator.liu.se/~koma/turingbombe/
- Enigma működésének bemutatása: https://www.youtube.com/watch?v=G2_Q9FoD-oQ
- Enigma hibái: https://www.youtube.com/watch?v=V4V2bpZlqx8