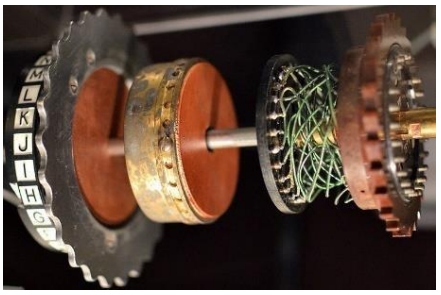
Moderní šifrování

Snad nikdy v historii neměla matematika a matematici tak zásadní vliv na další vývoj lidské civilizace, jako během 2. světové války. V USA nové matematické metody podstatně urychlily projekt vývoje atomové bomby, v Británii se skupině matematiků podařilo rozluštit kód německého šifrovacího stroje Enigma. Podle odhadů tyto úspěchy matematiky zkrátily válku o několik let a ušetřily milióny životů. Lepší představu o tom, jak obtížné bylo luštit šifry vytvořené Enigmou, můžete získat z pracovního listu. Video odkaz

Ve videu se mluví o elektromechanickém šifrovacím stroji Enigma. Na obr. 1a) je jednoduchá verze se třemi rotory. Na začátku šifrování se nastavil každý ze tří rotorů do smluvené polohy (na nějaké konkrétní písmeno). Text k zašifrování se psal na klávesnici podobné psacímu stroji. Po stisknutí klávesy se v horní části přístroje rozsvítila kontrolka pod zašifrovaným písmenem. „Síla“ Enigmy tkví v tom, že rotory se během šifrování otáčejí, čímž se pro každé písmeno mění substituční abeceda. Při každém stisknutí klávesy se jeden nebo více rotorů pootočilo o $\frac{1}{26}$ otáčky. Každý rotor měl na vstupu 26 kolíků propojených tajným způsobem s kontaktními plochami (viz obr. 1b) na opačné straně rotoru. Propojení uvnitř rotoru představovalo neznámou permutaci písmen (obr. 1c). Na každém rotoru byl jeden zářez, který udával místo, kdy se pohyb tohoto rotoru přenášel na sousední rotor vlevo (rotor na obr. 1b) má zářez u písmene *D*. Rotory bylo možné vyjmout a měnit jejich pořadí.

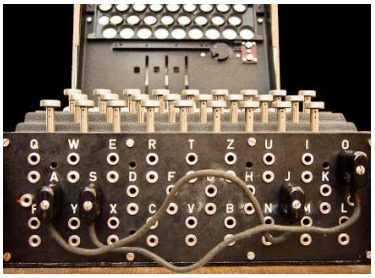
Obr. 1a) celkový pohled

b) rotor



c) tajné propojení písmen

d) trojice rotorů



e) propojovací deska

1. Původní verze Enigmy se vyráběla s pěti rotory označenými římskými čísly I, II, III, IV, V, z nichž se vždy vybírala konkrétní trojice.

a) Kolik různých trojic rotorů bylo možné vybrat?

b) Kolika různými způsoby můžeme tři vybrané rotory seřadit za sebe (obr. 1d)?
c) Kolik je celkem různých možností, jak můžeme vybrat a seřadit za sebe tři rotory z pěti nabízených?

2. Každý rotor bylo nutné na začátku šifrování nastavit na smluvené písmeno (celkem 26 možných pozic – počet písmen v německé abecedě).
   a) Kolik existuje všech možných trojic písmen, na které lze nastavit tři rotory Enigmy?
   b) Každý rotor měl jeden zářez u konkrétního z 26 písmen. Kolik různých poloh zářezů může mít daná trojice rotorů?
   c) Kolik existovalo všech možných „šifrovacích možností“, bereme-li v úvahu nastavení rotorů i polohy zářezů?

3. Propojovací deska (obr. 1e) umožňovala pomocí deseti kabelů propojit do páru 20 libovolných písmen a v rámci dvojice je vzájemně zaměňovat. Pokud bylo spojeno například *D* s *M* a v šifrování mělo padnout písmeno *D*, tak se rozsvítilo *M*. Kolik je všech možných propojení 26 písmen při použití deseti kabelů?

4. Kolik různých nastavení má Enigma, pokud vybíráme tři rotory z pěti nabízených a použijeme propojovací desku s deseti kabely?