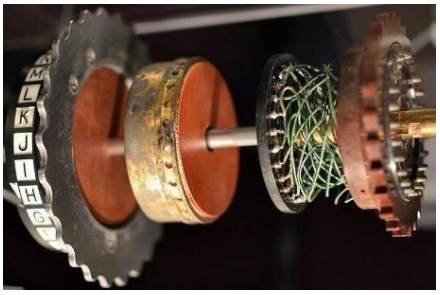
Moderní šifrování – řešení

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.

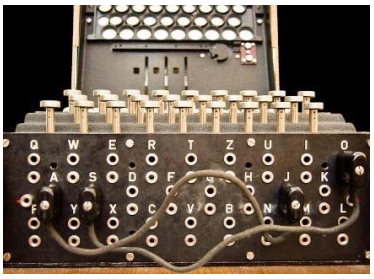
Obr. 1a) celkový pohled

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?

a) **1. řešení:** V tomto jednoduchém případě lze všechny možnosti systematicky vypsat.

I, II, III I, II, IV I, II, V I, III, IV I, III, V
I, IV, V II, III, IV II, III, V II, IV, V III, IV, V

Vidíme, že můžeme vybrat 10 různých trojic rotorů.

2. řešení: Použijeme-li základní kombinatorické poznatky, hledáme počet tříprvkových kombinací z pěti prvků. Odtud

$$\binom{5}{3} = \frac{5!}{3! \cdot (5-3)!} = 10.$$

b) **1. řešení:** Předpokládejme, že jsme vybrali rotory I, III, IV. Opět můžeme všechny možnosti seřazení rotorů za sebe systematicky vypsat.

I, III, IV I, IV, III III, I, IV III, IV, I IV, I, III, IV, III, I, Vidíme, že existuje celkem 6 způsobů, jak lze 3 rotory seřadit za sebe.

2. řešení: Použijeme-li kombinatoriku, hledáme počet tříprvkových permutací, těch je 3!, což je rovno 6.

c) **1. řešení:** Podle pravidla součinu vynásobíme počty možností z úloh a), b) a dostaneme

$$10 \cdot 6 = 60.$$

Vidíme, že existuje celkem 60 různých způsobů, jak lze vybrat a seřadit za sebe 3 rotory z 5 nabízených.

2. řešení: Ke stejnému výsledku dojdeme i jednoduchou úvahou. Na první místo vybíráme rotor z pěti nabízených, tj. máme 5 možností. Na druhé místo vybíráme jeden rotor ze 4 zbývajících. Rotor na třetím místě vybereme ze tří zbývajících. Podle pravidla součinu je tedy celkový počet možností roven

$$5 \cdot 4 \cdot 3 = 60.$$

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?

a) Každý z rotorů můžeme nastavit na některé z 26 písmen, tedy pro každý rotor je 26 možností. Pro tři rotory je tedy celkový počet možností roven

$$26 \cdot 26 \cdot 26 = 17\,576.$$

b) Analogicky jako v případě a) dostaneme, že pro trojici rotorů existuje celkem

$$26 \cdot 26 \cdot 26 = 17\,576$$

různých poloh zářezů.

c) Podle pravidla součinu vynásobíme počty možností z úloh a), b) a dostaneme

$$26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 = 308\,915\,776$$

různých šifrovacích možností.

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 např. *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?

První dvojici písmen můžeme vybrat $\binom{26}{2}$ různými způsoby. Pro výběr další dvojice máme k dispozici už jen 24 písmen, tedy takovou dvojici lze vybrat $\binom{24}{2}$ různými způsoby. Celkem dostaneme

$$\binom{26}{2} \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdot \binom{18}{2} \cdot \binom{16}{2} \cdot \binom{14}{2} \cdot \binom{12}{2} \cdot \binom{10}{2} \cdot \binom{8}{2} =$$

$$= 546\,999\,052\,092\,292\,800\,000 = 5{,}47 \cdot 10^{20}$$

různých propojení 26 písmen deseti kabely.

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

Hledaný počet dostaneme jako součin dílčích možností z předchozích úloh (1c, 2c, 3). Odtud plyne, že existuje celkem

$$60 \cdot 308\,915\,776 \cdot 5{,}47 \cdot 10^{20} = 1{,}01 \cdot 10^{31}$$

možností, jak Enigmu zapojit.