Počas druhej svetovej vojny bola schopnosť čítať nepriateľové šifrované správy dôležitá k obrane vlastného územia a dokonca ku rýchlejšiemu ukončeniu vojny. Jednou zo šifrovacích strojov bola nemecká Enigma, ktorej zmocnenie sa ale ešte ani zďaleka neznamenalo úspech pri dešifrovaní, keďže počet všetkých jej možných nastavení pre jeden deň predstavoval číslo presahujúce trilióny. V predvojnových a vojnových rokoch sa prelomeniu Enigmy neústupne venovali najlepší poľskí a anglickí matematici, ktorí svoje úspechy museli striktne držať v tajnosti, dokonca aj desiatky rokov po vojne. Náplňou mojej bakalárskej práce je vytvorenie matematického modelu Enigmy a pomocou jeho zistených slabín zrekonštruovať postupy pri odhaľovaní denných kľúčov s dôrazom na ich matematické zdôvodnenie.