Enigma a jiné klasické šifry

Prolomení německé vojenské šifry Enigma polskými matematiky v roce 1932 bylo jednou z nejdůležitějších událostí předcházející druhé světové válce. Spojencům se podařilo tuto skutečnost utajit před německou armádou až do konce války.

Ukážeme si Vigenérovu šifru, která byla po celá dvě století považována za nerozluštitelnou. Úspěšný byl až anglický matematik Charles Babbage koncem 19. století. Později se podařilo nalézt jednoduchý algoritmus, který text o délce sta písmen vyřeší během vteřiny. O tomto algoritmu si také něco povíme.

Poté si ukážeme simulátor šifrovacího stroje Enigma a jakým způsobem byl tento stroj používán. Nakonec si vysvětlíme, co všechno musela skupina tří polských matematiků vedená Marianem Rejewskim dokázat, aby tuto šifru prolomila.