Abstrakt:
Práce se zabývá teorií řetězových zlomků, na níž je založen návrh proudové šifry z článku On the use of continued fractions for stream ciphers. Jelikož fakta o rozdělení pravděpodobnosti výskytu jednotlivých čísel jako částečných podílů v zobecněných řetězových zlomcích potřebné k prokázání bezpečnosti navrhované šifry nebyla dosud dokázána, v práci jsou shrnuty dosavadní poznatky, které by mohly vést k jejich prokázání. Jde zejména o základní vlastnosti klasických a zobecněných řetězových zlomků a důkaz Kuzminovy věty, jejímž důsledkem je rozdělení pravděpodobnosti výskytu jednotlivých přirozených čísel jako částečných podílů klasických řetězových zlomků. V práci je také návrh šifry z článku stručně představen.