Abstrakt:

V predloženej práci sa venujeme kryptoanalýze jednej z najznámejších prúdových šifier - šifre A5/1. Táto šifra sa používa na zabezpečenie komunikácie mobilných telefónov, ktoré sú v súlade so štandardom GSM. Základným prvkom šifry A5/1 je LFSR(posuvný register s lineárnymi spätnými väzbami), ktorý sa používa v prúdových šifrách, pretože produkuje postupnosť bitov s vysokou periódou, má dobré štatistické vlastnosti a ľahko sa analyzuje pomocou rôznych algebraických metód. V práci sme popísali a implementovali tri útoky na šifru, ktoré predpokladajú znalosť otvoreného textu. Prvé dva útoky sú typu uhádni a odvoď a posledný je korelačný. Ťažiskom práce je kryptoanalýza od Golića, ktorá predpokladá len 64 bitov otvoreného textu. Charakter jeho implementácie dovoľuje úlohu rozdeliť na paralelne prebiehajúce výpočty, vďaka čomu je možné používať program aj v praxi. Na záver práce sa venujeme korelačnému útoku, ktorý je podstatne rýchleší, ale predpokladá znalosť pomerne veľkého množstva otvoreného textu.