Mateusz Buczek
Wojskowa Akademia Techniczna
Wydział Cybernetyki, Instytut Matematyki i Kryptologii

Dobre, bo polskie — analiza polskich konstrukcji funkcji skrótu

Od kilku lat najważniejszym i najszerzej komentowanym zagadnieniem w kryptologii są funkcje skrótu. Związane jest to zarówno z odkrywaniem coraz to nowych słabości w obecnie stosowanym standardzie, jak i powodowaną tym chęcią ustalenia nowego. W wyłonieniu go ma pomóc konkurs na nowy standard funkcji skrótu SHA-3, którego zakończenie jest planowane na przyszły rok.

Poza zmaganiami konkursowymi pozostaje jednak wiele funkcji skrótu, których zasady działania i zastosowane w nich pomysły są nie mniej godne uwagi. Mimo to nie spotykają się one z wystarczającym zainteresowaniem i często niesłusznie zostają pominięte. W ramach pracy przyjrzymy się jednej z takich funkcji. Ciekawej szczególnie dlatego, że jest ona polskiego autorstwa. Zostanie zaprezentowana jej budowa wewnętrzna, oczekiwane poziomy bezpieczeństwa i proponowane przez autora nowatorskie rozwiązanie.

Niestety w dalszej części pracy zostaną także pokazane ataki na tę funkcję skrótu. Okazuje się bowiem, że mimo zapewnień twórcy nie spełnia ona wszystkich stawianych wymogów bezpieczeństwa i potrzebna jest jeszcze pewna praca, zanim będzie mogła być używana szerzej. Mimo tych wad nie należy jednak dyskwalifikować tego algorytmu całkowicie, ponieważ zastosowane w nim rozwiązania mogą zostać wykorzystane w kolejnym konkursie. Kto wie, na jak długo wystarczy nowo wyłoniony standard.