Michał Misztal
Wojskowa Akademia Techniczna
Instytut Matematyki i Kryptologii

Metoda wyznaczania na podstawie parametru S/N liczby wymaganych tekstów jawnych dla kryptoanalizy różnicowej 9 rund DES'a

Przedstawiono atak za pomocą kryptoanalizy różnicowej na algorytm DES zredukowany do 9 rund. Przeprowadzono dokładniejsze oszacowanie parametru S/N niż w pracy Bihama i Shamira oraz zaproponowano sposób wykorzystania tego parametru do wyznaczenia liczby par tekstu jawnego wymaganej do powodzenia ataku. Podano wyniki (czas ataku) i problemy implementacyjne powstałe podczas praktycznej realizacji tego ataku.