

M. Jurkiewicz
Wojskowa Akademia Techniczna, Warszawa
E-mail: mjurkiewicz@wat.edu.pl

Kilka uwag dotyczących bezpieczeństwa RSA

Zaprezentujemy pewne ataki na RSA w zależności od relacji między wykładnikami szyfrowania, deszyfrowania oraz modułem.