Kryptografia
Laboratorium - lista nr 7, 5 VI

Dowody z wiedzą zerową

Wybierz jedno z poniższych zadań (w zależności od interesujących Cię punktów):

Zadanie 1 (5 pkt) Zaimplementuj dowód z wiedzą zerową na znajomość dyskretnego logarytmu na bazie schematu podpisu Schnorra (4 pkt). Wykorzystaj w tym celu jedną z grup zdefiniowanych w dokumencie `http://tools.ietf.org/html/rfc5114` (1 pkt)

Zadanie 2 (10 pkt) Zaimplementuj interaktywny dowód na znajomość dyskretnego logarytmu na bazie protokołu identyfikacji Schnorra dla krzywych eliptycznych `http://www.stanford.edu/class/cs259c/lectures/schnorr.pdf` (6 pkt).

Twój program powinien wykorzystać jedną z krzywych zdefiniowanych w dokumencie `http://www.secg.org/collateral/sec2_final.pdf` (1 pkt).

Zaimplementuj własną arytmetykę dla krzywych eliptycznych. Opis arytmetyki możesz znaleźć w dokumencie `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.pdf`. (3 pkt)