Abstract

This paper establishes the need for a small Domain Specific Language to support rapid testing and diagnosis of cryptographic algorithm. Such a language will require built-in support for modulo arithmetic, which is used for creating mathematical locks in modern crypto systems. The paper also provides a framework/prototype for such a language. It can further be used as a building block for broader set of language specific features.
Indian Branch, Delhi, p 215.
- Andrew W. Appel; 2001; “Modern Compiler Implementation in C”; Special Edition for Sale in South Asia; Cambridge University Press.

**Index Terms**

Computers

**Keywords**

cryptography flex bison lex yacc ply parser grammar tokenizer compiler

lexer

llvm

llvmpy.