Technology Fact Sheet

MIMOS – National R&D Centre in ICT, Malaysia

MIMOS Cryptographic Module (Mi-Crypto)

Secured communication of information is essential especially in the presence of third parties. The ability to protect and secure such information is vital to ensure that its integrity has not been tampered. MIMOS Mi-Crypto is a homegrown general purpose cryptographic library that provides well-known cryptographic ciphers used in the encryption and decryption of information.

Overview

MIMOS Mi-Crypto is a general purpose cryptographic module that offers MIMOS-developed ciphers together with a series of standard industry ciphers. These ciphers are designed by qualified cryptanalysts and tested locally in compliance with NIST standards and are specifically used for highly secure communications where data protection is vital. Mi-Crypto is designed based on Malaysian Armed Forces Cryptography Policy (Dasar Kriptografi Angkatan Tentera Malaysia) towards achieving self-reliance and self-sufficiency aside from foreign-based ciphers.

Features

Mi-Crypto comprises the following features:

- **Block Ciphers**
  Several industry ciphers such as AES, 3DES, Twofish and Blowfish, and MIMOS-developed ciphers that are poised to be on par if not stronger than AES are included in the Mi-Crypto library.
- **Comprehensive API**
  A set of comprehensive Application Programming Interfaces (APIs) in C language is provided for a choice to switch to the best cipher on-the-fly.
- **Multi-Platform**
  Mi-Crypto supports cross-platform and multi-platform systems such as Windows/Linux desktops/laptops with a roadmap to include mobile/smart devices and embedded systems.

Technology Benefits

The main impacts of Mi-Crypto are:

- **Homegrown and Industry Ciphers**
  Mi-Crypto offers homegrown as well as industry ciphers that can be programmed and utilised by any security application making the application protected impervious against various angles of security attack.
- **NIST-Compliant**
  Homegrown ciphers in Mi-Crypto have undergone cryptanalysis testing and comply with NIST's Statistical Test Suite. The tests determine if the outputs produced protect the cipher texts.
- **High-Profile Data Exchange Design**
  Mi-Crypto is designed for Public Safety and Security agencies where high profile data exchange that involve documents, files and transactions occur at every second.
- **Platform Integration**
  Principally, Mi-Crypto is designed to operate on multiple platforms and packaged for Windows/Linux desktops/laptops with the added C language API as the interface. Embedded/smart device support are in the roadmap.

MIMOS is the leader in ICT innovations, pioneering new market creations for partners through patentable technologies for economic growth. For more information on MIMOS technologies, contact mimossolutions@mimos.my or go to www.mimos.my.

Technology Summary

Mi-Crypto

A homegrown general purpose cryptographic module for data protection.

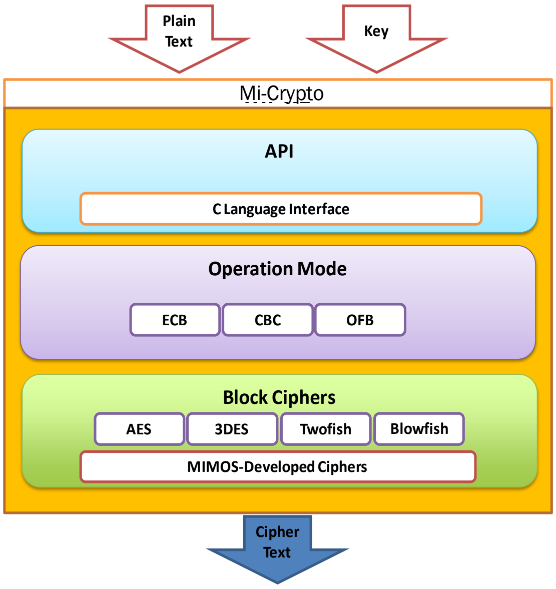
Industries: Public Safety, Government, Enterprise

Features

- Block ciphers
- Comprehensive API
- Multi-Platform

Technology Benefits

- Homegrown and industry ciphers
- NIST-compliant
- High-profile data exchange design
- Platform integration



MIMOS Mi-Crypto operation

System Requirements

Mi-Crypto		
Hardware Requirements		
System	32-bit	64-bit
Processor	Intel® Pentium 4	Intel Pentium Dual-Core
Memory	Minimum 2GB of RAM	Minimum 4GB of RAM
Disk Storage	Minimum 1GB of additional hard disk space	Minimum 1GB of additional hard disk space
Software Requirements		
System	Linux	Windows
Operating System	CentOS 3.9 with Linux Kernel 2.4.x (32-bit)	Windows® XP (32-bit)/ Windows 7 (32-bit)
C Compiler	GNU Compiler Collection (GCC) for C/C++	MinGW32 (with MSYS) Visual Studio C++ 2010
Mi-Crypto Library Type	Static (.a) and Dynamic (.so)	Static (.a) – supplied for MinGW Dynamic (.dll) – supplied for MinGW and Visual Studio C++ 2010 Stub file (.lib) – supplied for Visual Studio C++ 2010
Tool Prerequisite	Makefile or scripting language, Text editors (VI, Emacs)	-

Innovation for Life™