Machine Learning eBook

Basics To Advanced Techniques. Get Access To Examples, Videos & More. Then Try MATLAB

OPEN

        - General
        - CString Alternatives
        - CString Extensions
        - CString Manipulation
        - Open FAQ
        - Regular Expressions
        - String Arrays
        - String Conversions
        - .NET
    - COM-based Technologies »
        - ATL & WTL Programming »
            - General
            - ATL
            - Active Scripting
            - ActiveX Controls
            - Database
            - Debugging
            - External links
            - Graphics Support
            - Misc.
            - Performance
            - Printing
            - Tutorials
            - Utilities
            - Windows Template Library (WTL)
        - ActiveX Programming »
            - General
            - Active Scripting
            - ActiveX Controls
            - ActiveX Documents
            - Apartments & Threading
            - Error Handling
            - External links
            - General COM/DCOM
            - Misc.
            - Registry
            - Security
            - Structured Storage
            - Tutorials
            - Wrappers
        - COM+ »
            - General
            - COM Interop
            - Managed Code / .NET
            - SOAP and Web Services
        - Shell Programming »
            - General
            - Open FAQ
            - Shortcuts
            - Tray Icons
            - Previous Section Manager
    - Controls »
        - Property Sheet »
            - Open FAQ
            - Property Sheet Buttons
            - Sizing
            - Wizards
        - Button Control »
            - Advanced Buttons
            - Bitmap Buttons
            - Flat Buttons
            - Menus
            - Non-Rectangular buttons
            - Windows XP
        - ComboBox »
            - Colour Pickers
            - DropDown
            - Font selection combos
            - Multicolumn combos
            - Special Effects
            - Tooltips
        - Edit Control »
            - Background & Color
            - Editors
            - Keyboard
            - Masked Edit Controls

- Passwords and Security
- Spin Controls
- Transparent
- ImageList Control »
  - Open FAQ
- ListBox Control »
  - Checkboxes
  - Color Listboxes
  - Drag & Drop
  - LEDs
- ListView Control »
  - Advanced
  - Background color and image
  - Checkboxes
  - Columns
  - Custom Drawing
  - Data
  - Deleting
  - Drag & Drop
  - Editing items and subitem
  - FilterBar
  - Grid lines
  - Header Control
  - Introduction
  - Miscellaneous
  - Navigation
  - New ListView control (IE 4.0)
  - Printing
  - Property Lists
  - Reports
  - Scrollbars
  - Selection
  - Sorting
  - Tooltip & Titletip
  - Using images
  - Views
- Menu »
  - Alternative menu
  - Bitmapped menus
  - Dockable menus
  - Message and Command Routing
  - Miscellaneous
  - XML
  - XP-Style Menus
- Other Controls »
  - Bitmap Buttons
  - Charting and analogue controls
  - Check Box Controls
  - Clocks & Timers
  - Cool Controls
  - Date Selection Controls etc.
  - Digital Controls
  - Extending/Subclassing Techniques
  - File and Directory choosers
  - Grid Control
  - Group Box
  - HyperLink controls
  - Internet & Web Related
  - Lists, Trees and Combos
  - Minimize Button
  - Progress Controls
  - Resizing
  - Scroll Bars
  - Slider Controls
  - Spin Control
  - System Tray
  - Tab Controls
  - Tooltip controls
  - Charting and analogue controls
  - Extending/Subclassing Techniques
- Rich Edit Control »
  - Conversions
  - Editors and Editing
  - Syntax Hilighting
  - Windowless
- Static Control »

        - Bevel lines
        - Data display controls
        - Scrolling Text
    - Status Bar »
        - Advanced
        - System Tray
    - Toolbar »
        - Customizing Toolbars
        - Docking
        - Flat Toolbar
        - Miscellaneous
        - Placing Controls in Toolbars
        - Placing Controls in Toolbars
    - Treeview Control »
        - Classes
        - Directory Browsers
        - Drag & Drop
        - Editing labels
        - Expand - Collapse
        - Misc - Advanced
        - Multiview
        - New Listview control (IE 4.0)
        - Searching
        - Tree traversal
        - Using images
- Data »
    - Database »
        - ADO
        - ADO.NET
        - ATL
        - DAO
        - Dynamic Data Access
        - Microsoft Access
        - Microsoft Excel
        - Misc.
        - Object Oriented
        - ODBC
        - OLE DB
        - Oracle
        - SQL Server
        - Stored Procedures
        - XML
    - Miscellaneous »
        - File Information
        - INI Files
        - Values
        - XML
- Frameworks »
    - UI & Printing Frameworks »
        - Component Libraries
        - Outlook Controls
        - Reporting and Report Writing
        - Skins
        - Reporting and Report Writing
        - Windowing Techniques and Classes
- Graphics & Multimedia »
    - Bitmaps & Palettes »
        - Capturing
        - Compressing
        - Displaying and Sizing
        - External Links
        - Icons
        - Image Manipulation
        - Merging
        - Other formats...
        - Palettes and Color Tables
        - Special Effects
        - Using regions
        - Viewers
        - Views & MDI clients
    - DirectX »
        - DirectDraw
        - DirectInput
        - DirectShow
        - DirectX 8
    - GDI »

        - Capturing Images
        - Fills
        - Font Handling and Detection
        - GDI+
        - Icons and Cursors
        - Lines
    - Multimedia »
        - Audio
        - Desktop Effects
        - Graphics
        - Imaging
        - Timers
        - Twain
        - Video
    - OpenGL »
        - Game Programming
        - Printing
        - Texture Mapping
- Internet & Networking »
    - Internet Protocols »
        - ActiveX
        - Browser Control
        - Chat Programs
        - DHTML
        - Dial-up
        - DNS
        - Email
        - File Transfer
        - FTP
        - General Internet
        - HTML
        - HTTP
        - Instant Messaging
        - Internet Protocol (IP)
        - Network
        - Secure Socket Layer (SSL)
        - Security
        - Streaming Media
        - Web Services
        - XML
    - IE Programming »
        - Displaying Information
        - Security
        - Voice
    - ISAPI »
        - Cookies
        - Data/Databases
        - Extensions
        - Filters
        - Related CODEGURU sections
    - Network Protocols »
        - Active Directory
        - Basic Network Operations
        - Dial-up Networking
        - Games
        - IPX
        - Messaging
        - Named Pipes
        - Network Information
        - Remote Administration
        - Remote Invocation
        - Serial Communications
        - TCP/IP
        - Winsock Solutions
- Miscellaneous »
    - Miscellaneous »
        - Application Control
        - Assembly Language
        - CD-ROM
        - Compiler and Pre-Compiler
        - Console Apps
        - CryptoAPI
        - Drag and Drop
        - File and Directory Naming
        - File I/O
        - Flicker Free Drawing

        - Fonts
        - Graphics
        - ImageList
        - Intellisense
        - Interfacing to other languages
        - Internet Explorer
        - IPC Techniques
        - Keyboard
        - Log and Trace Files
        - MAPI
        - Math
        - Memory
        - Message Box Handling
        - MFC Help
        - Microsoft Office / Outlook
        - Microsoft Shell (MSH)
        - Mouse and Cursor Handling
        - MSN
        - Multi-Lingual Support
        - Plug-ins / Add-ins
        - Power Management API
        - Screen Savers
        - Splash Screens
        - Stack
        - System
        - System Tray
        - Task Scheduler
        - Templatized Classes
        - Threads/Processes
        - Timers
        - Titlebar
        - Tools
        - UML
        - Version Info
        - Video
        - Visual InterDev
        - Windows Messaging
    - Samples »
        - Basic Programming
        - Code Highlighting
        - Games
        - System Information
        - Testing & Debugging
- Visual Studio »
    - Debugging »
        - Debuggers
        - Handling Crashes
        - Logging
        - Memory Issues
        - Reverse Engineering
        - Tracing
    - Add-ins & Macros »
        - Add-Ins
        - Bookmarks
        - Browser Windows
        - Code Generation
        - Code Navigation
        - Code Reformatting
        - Code Template Add-in
        - Comment Creators
        - Custom AppWizards
        - Debugging
        - File Creation
        - File Opening
        - Text Operations
        - Version Control
        - Visual Studio .NET
        - Window Management
    - Editor Tips »
        - Customizing the IDE
        - Debugging
        - Syntax Highlighting
- Windows Programming »
    - Vista
    - CE »
        - Bitmaps and the GDI

- COM
- Controls
- Database
- Embedded Visual C++
- Files
- Game Programming
- Memory Management
- Networking
- Pocket PC
- Registry
- Samples
- Shell and Related Programming
- SmartPhone

- Clipboard »
  - External Links
  - Previous Section Manager
- DLL »
  - Hooking
  - Import/Export issues
  - Interfacing to Visual Basic applications
  - Mixed DLLs
  - Tips
  - Interfacing to Visual Basic applications
- File & Folder »
  - Browser Functions & Dialogs
  - Controls & Dialogs
  - File Information
  - File I/O
  - Folder/Directory Maintenance
  - INI files
  - Installers
  - Shell API Functions
- Help Systems »
  - HTML
  - MSDN
- Printing »
  - Open FAQ
  - Print Preview
- Win32 »
  - Cursors
  - MessageBox
  - Security
  - Tutorials
  - Versioning
- System »
  - CD-ROM
  - Control Panel
  - Device Driver Development
  - Hardware Information
  - Keyboard
  - Logging
  - Message Handling
  - Misc
  - MMC Snapins
  - NT Services
  - Performance Statistics
  - Processes / Modules
  - Registry
  - Resource Detection/Management
  - Security
  - Services
  - Shared Memory
  - System Information
  - Taskbar
  - Task Manager
  - Threading
  - Timers
  - VxD

- Windows & Dialogs »
  - Console »
    - Redirection
  - Dialog »
    - Animation
    - Background
    - Bitmaps/Images
    - Browse Namespace

- Colors
- CommandUI
- Common Dialogs
- Credits Dialog
- DDX/DDV
- Dialog-based applications
- Dialog Bars
- Dialog for selecting folders
- Dialog Layout Manager
- Dialog Template Resources
- Displaying in a window
- Display Performance
- Font Handling
- Help
- Image Preview
- Menu Handling
- Miscellaneous
- Modeless Dialogs
- Non-Rectangular Dialogs
- Options Dialogs
- Progress Indicators
- Resizable Dialogs
- Scrolling
- Splash Screens
- Splitter Windows withing Dialogs
- Threads
- Tip of the Day
- Title Bar
- Toolbars and Statusbars
- Tooltips for Dialog Controls
- Tutorials
- Win32
- Wizards
- Splitter Windows withing Dialogs

- Docking Window »
  - Open FAQ
- Doc/View »
  - Background
  - CHtmlView
  - Command Routing
  - Control Views
  - DDX/DDV
  - File Open/Save
  - Help
  - Message Maps
  - Misc
  - MRU (Most Recent Used file list)
  - Printing
  - Scrolling
  - SDI
  - Splitter Views
  - Tabs
  - Title Bar
  - View Management
  - Window Positions/Sizes
- Splitter »
  - Open FAQ
  - Sizing
  - Toolbars
  - Tutorials

- Standard Template Library

- .NET / C# »
  - Sample Chapter
  - .NET »
    - Silverlight
    - WCF
    - WPF
    - Windows Workflow
    - Data & Databases »
      - DataGrid
      - Sorting and Iterating
      - Web Grid
    - Debugging »
      - Debugging
      - Logging
      - State Management

- Techniques
- Tracing
- Framework »
  - Licensing
  - Microsoft Namespace
  - System Namespace
- General »
  - Arithmetic
  - Assemblies
  - Code-Behind
  - COM/COM+
  - Common Type System (CTS)
  - Debugging and Error Handling
  - Events and Delegates
  - Graphics
  - IL
  - Internet
  - Keyboard
  - Macros
  - .NET Framework Classes
  - .NET My Services
  - Patterns
  - Performance
  - Rotor
  - System Information
  - Threads
  - Tips & Tricks
  - Tools and 3rd Party
  - Visual Studio .NET Add-Ins
  - Debugging and Error Handling
- JScript .NET »
  - Essam Ahmed on JScript .NET
- Managed C++ »
  - Windows Services
- Net Security »
  - Authentication
  - Encryption
  - PGP
- VS Add-Ins »
  - UML and Design
  - Visual Studio Add-ins
  - Visual Studio .NET 2003 Add-ins
- General ASP.NET »
  - Controls
  - Email
  - Files
  - Miscellaneous
  - Scripting
  - Themes
  - Tutorials
  - Web Forms

- Azure »
- C# »
  - .NET 3.0 / .NET 3.5
  - LINQ
  - Basic Syntax »
    - Anand C# Tutorials
    - Attributes
    - Component Development
    - Controls
    - Enumerations
    - Error Handling
    - Indexers
    - Inheritance
    - Interfaces
    - Operators
    - Reflection
    - Remoting
    - Serialization
    - Threading
    - Unmanaged Code
    - Unsafe
  - Collections
  - Controls »
    - Custom
    - Data Grid

        - Property Grid
        - Rich Text
        - Tree View
        - Tutorials
        - Wizards
    - Data & I/O »
        - Caching and Peformance
        - Searching
        - Streaming
        - Tutorials
        - XML
    - Date & Time »
        - Formatting
        - Time Routines
    - Delegates »
        - Event Handling
    - Graphics & Multimedia »
        - Charts and Graphing
        - Customizing User Interfaces
        - Drawing
        - Mouse
        - Screen Captures
        - Sound
        - Threading
        - Wav Files
        - Customizing User Interfaces
    - Internet »
        - Desktop Applications
        - Mail
    - Miscellaneous »
        - COM
        - Design/Techniques
        - DLLs and Executables
        - E-Mail
        - Graphics and Images
        - Icons
        - Mathematics
        - Reflection
        - Sample Programs
        - Security
        - User Interface
    - Network & Systems »
        - Configuration Files / INIs
        - Database
        - Directory Services
        - HTTP
        - Internet/Web
        - IP
        - Remoting
        - Sockets
        - Windows Services
        - WMI
    - Web Services »
        - Security
        - Tutorials
  - Windows 8/RT »
  - XAML »
- Visual Basic »
  - Sample Chapter
  - .NET 3.0 (VB)
  - LINQ (VB)
  - Internet »
    - ASP .NET
    - Database
    - HTML
    - SMTP / eMail
    - Web Services
    - Indexing
  - VB Controls »
    - VB Other Controls »
      - OCX Controls
    - VB ListView
    - VB ListBox
    - VB ComboBox
    - VB ActiveX »
      - ActiveX

- .NET Controls »
  - DataGrid Control
  - Listview
- VB Files »
  - Directory
  - Drive
- VB Shell

- General »
  - VB Multimedia »
    - MP3s
  - VB Graphics »
    - Animation
    - File Formats
    - GDI
    - Transparency
  - Database »
    - ADO
    - ADO.NET
    - Database Access
    - DataSets
    - Microsoft Access
    - SQL Server
    - Stored Procedures
    - Strongly Typed Data
    - DataGrid
  - Forms & Controls »
    - Backgrounds
    - Icons
    - ListBox
    - ListView Controls
    - Resizing
  - IDE & Language »
    - Attributes
    - Error Handling
    - IDE (including Visual Studio .NET)
    - IDE & Language
    - Indexers
    - Miscellaneous
    - IDE (including Visual Studio .NET)
  - Misc »
    - Algorithms
    - Console Applications
    - Date
    - Debugging and Tracing
    - Encryption
    - Games and Fun
    - Icons
    - Multi-Language Support
    - Numbers
    - OOP
    - PDF
    - Plugins
    - Printing
    - Samples
    - Text
    - Tips
    - User Defined Types (UDTs)
  - System »
    - Directories and Files
    - Keyboard
    - Network
    - Services
    - Win32
  - Mobile/Wireless »
    - Mobile Internet Toolkit
    - Pocket PC
  - Windows 8/RT »
- Others »
  - Windows Mobile Dev Center
  - Internet of Things (IoT)
  - CodeGuru Blogs
  - Codeguru Live Chats
  - Azure Activities
  - Videos
  - Whitepapers
  - Slideshows

- Forums
;
- Submit an Article
- Newsletter
Stay up-to-date with our free Microsoft Tech Update Newsletter

Enter your Email Address Subscribe

By submitting your information, you agree that codeguru.com may send you codeguru offers via email, phone and text message, as well as email offers about other products and services that codeguru believes may be of interest to you. codeguru will process your information in accordance with the Quinstreet Privacy Policy.

Close
- Slideshows
- Sponsored

C++ Programming: Implementation of the Licensing System For a Software Product

Posted by **Apriorit Inc.** on **September 13th, 2010**

WEBINAR: On-Demand
Building the Right Environment to Support AI, Machine Learning and Deep Learning
Watch→

Table Of Contents

Introduction
Types of algorithms
Hardware Serial Key
The scheme of the licensing system
The folders structure
Bibliography list

Introduction

This article is devoted to the development of the key licensing system for the applications. In the theoretical part of the article, we will examine the cryptography methods, which can be used while implementing the licensing system. Also we will discuss all pros and cons of these methods and select the possible ones for using in the application. In the practical part of the article, we will provide the implementation of the simplest licensing system, which guaranties the protection from cracking even if a hacker knows the source code of an algorithm.

Types of algorithms

Results: 3
Matching School Ads

Purdue University Global
Building on Purdue's mission to provide greater access to affordable, world-class education, Purdue University Globaldelivers a fully personalized online experience that's tailored to working adults.

Visit https://go.purdueglobal.edu
Selected Campus Locations:
- Online

Selected Programs:
- BSIT - Programming and Software Development
- BS in Information Technology
- AASIT - Programming and Software Development
- AAS in Information Technology

PURDUE UNIVERSITY GLOBAL
Request Info
Visit School Site

Stevens-Henager

The Secret to Getting Ahead is Getting Started

Congratulations! Your interest in Stevens-Henager College is an important first step toward changing your life. A career-focused degree is the key to a new career with a potentially higher income, better benefits, and more satisfaction.

Selected Campus Locations:

- Salt Lake City

Selected Programs:

- Software and Mobile Application Development (BS)
- Web Design and Development (BS)
- Networking and Information Systems Security (BS)
- Computer Technology & Networking (AAS)

Request Info

Lincoln Tech

Lincoln Tech is your LINC to a new career!

Selected Campus Locations:

- Mount Laurel

Selected Programs:

- Computer and Network Support Technician

Request Info

Matching School Ads

The cryptographic algorithm, also called cipher, is a mathematical function used for encryption and decryption. Usually, these are two interconnected functions: one is used for encryption, another is for decryption.

If the reliability of the algorithm is based on keeping the algorithm itself in secret, then this algorithm is limited. Limited algorithms do not correspond to the nowadays standards and represent only the historical value.

The modern cryptography solves these problems with the help of the key. The key can be of any value selected from a wide range of values. The set of possible keys is called the key space.

There are two main types of algorithms based on the key usage: symmetric-key algorithm and algorithm with the public key.

Symmetric-key algorithms, sometimes called the conditional algorithms, are the algorithms where the encryption key can be calculated by the decryption key and vice versa. The encryption and decryption keys are the same in most symmetric-key algorithms. These algorithms, also called one-key or secret-key algorithms, require that the sender and the recipient reconcile the used key before the beginning of the secure message exchange. The safety of the symmetric-key algorithm is defined by the key. The key disclosure means that anyone can encrypt and decrypt messages. The key must be kept in secret as long as the transmitted messages should be secret.

Algorithms with the public key, also called asymmetric-key algorithms, are developed in the way that the key used for the encryption differs from that for decryption. Moreover, the decryption key can't be calculated by the encryption key (at least, during the reasonable period of time). These algorithms are called "algorithms with the public key" because the encryption key can be open: anyone can use the encryption key for the encryption of the message but only one concrete person can decrypt the message with the corresponding decryption key. In these systems, the encryption key is often called the public key and the decryption key is called the private key. The private key is sometimes called the secret key.

It is obvious that the only type of the algorithm which suites us is the algorithm with the public key because we have to store the key in the program for the authentication of the entered serial key. When choosing these algorithms, we have the guarantee that the intruder, having the public key and the source code of the algorithm, won't be able to make the key generator and create serial keys for another program copies.

There are many computer algorithms. The following three algorithms are most frequently used:

- **DPS** (Data Encryption Standard) is the most popular computer encryption algorithm. It is the American and international standard. It is the symmetric-key algorithm where one and the same key is used for encryption and decryption.

- **RSA** (which stands for Rivest, Shamir and Adleman who first publicly described it) is the most popular algorithm with the public key. It is used both for the encryption and for digital signature.

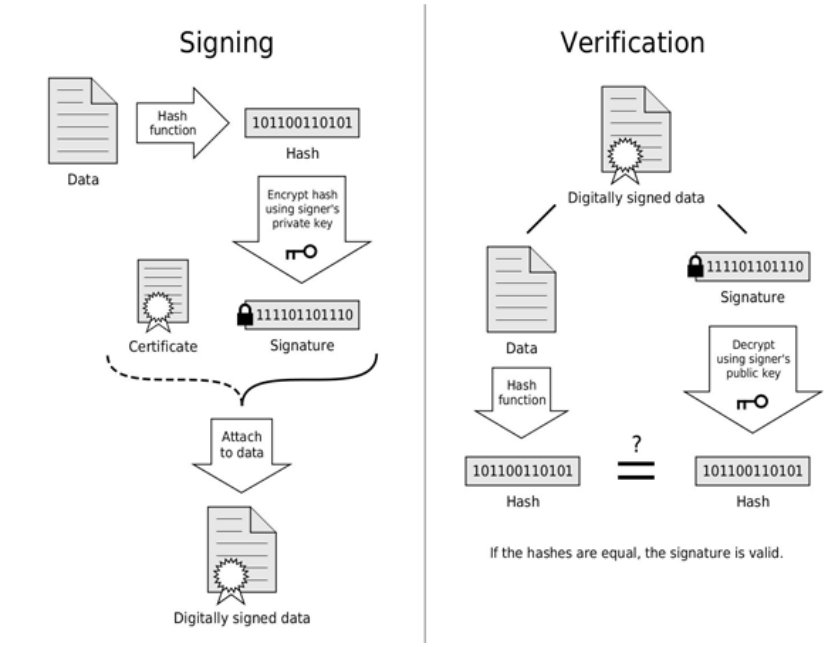
- **DSP** (Digital Signature Algorithm, is used as the part of the Digital Signature Standard) is another algorithm with the public key. It is used only for the digital signature and can't be used for the encryption.

DES does not suit us because it is the symmetric-key algorithm.

Two algorithms are left: **RSA** and **DSA**. It is easy to choose between them if we look at the structure of the work of these algorithms.

RSA uses the public key for the creation of the cipher text from the source text. We don't need it as it is supposed that we create and send keys and they will be decrypted and compared with the source value on the client side. As it was mentioned above, we can use only the public key on the client side in order not to compromise the licensing system.

Now some words about the work of **DSA.** Using the source text, DSA calculates the hash code and then "decrypts" it using the private key and receives the required serial key. It "encrypts" the received value on the client side and receives the hash code. Then it calculates the hash code from the source text in the usual way and compares two values. If these values coincide, then the serial key is valid.



The **Crypto++B. Library** contains the implementation of many algorithms. I used this library in the example. For more information, see http://www.cryptopp.com/.

```
.............................
bool RsaVerifyVector(const std::string & publicKeyStrHex, const std::string& source, const std::vector<char>& sign)
    {
        CryptoPP::HexDecoder decoder;
        decoder.Put( (byte*)publicKeyStrHex.c_str(), publicKeyStrHex.size() );
        decoder.MessageEnd();

        CryptoPP::RSA::PublicKey publicKey;
        publicKey.Load( decoder );

        // Verifier object
        CryptoPP::RSASS<CryptoPP::PSS, CryptoPP::SHA1>::Verifier verifier( publicKey );

        std::vector<char> rawSignature;
        std::string signStr(utils::GetBeginOf(sign), sign.size());
        utils::FromHexString(utils::string2wstring(signStr), &rawSignature);
        // Verify
        const char * pData = utils::GetBeginOf(source);
        return verifier.VerifyMessage( (const byte*) pData,
            source.size(), (const byte*) utils::GetBeginOf(rawSignature), rawSignature.size() );
    }
................................................
void RsaSignVector(const std::string & privateKeyStrHex, const std::vector<char> & vec, std::string & sign)
    {
        // Pseudo Random Number Generator
        CryptoPP::AutoSeededRandomPool rng;
        // Generate Parameters
        CryptoPP::InvertibleRSAFunction params;
        params.GenerateRandomWithKeySize( rng, 1536 );

        CryptoPP::HexDecoder decoder;
        decoder.Put( (byte*)privateKeyStrHex.c_str(), privateKeyStrHex.size() );
        decoder.MessageEnd();

        CryptoPP::RSA::PrivateKey privateKey; // Private
        privateKey.Load( decoder );
```

```
        CryptoPP::RSASS<CryptoPP::PSS, CryptoPP::SHA1>::Signer signer( privateKey );

        size_t length = signer.MaxSignatureLength();
        CryptoPP::SecByteBlock signature( length );

        // Sign message
        signer.SignMessage( rng, (const byte*) utils::GetBeginOf(vec),
            vec.size(), signature );

        sign  = utils::wstring2string(utils::ToHexString<byte>(signature, signature.size()));
    }
.........................................
void RsaGenerateStringKeys(std::string & publicKeyStr, std::string & privateKeyStr)
    {
        // Pseudo Random Number Generator
        CryptoPP::AutoSeededRandomPool rng;

        // Generate Parameters
        CryptoPP::InvertibleRSAFunction params;
        params.GenerateRandomWithKeySize( rng, 1536 );

        CryptoPP::RSA::PrivateKey privateKey( params );
        CryptoPP::RSA::PublicKey publicKey( params );

        CryptoPP::HexEncoder encoder;

        // save public Key
        encoder.Attach( new CryptoPP::StringSink( publicKeyStr ) );
        publicKey.Save( encoder );

        // save private Key
        encoder.Attach( new CryptoPP::StringSink( privateKeyStr ) );
        privateKey.Save( encoder );
    }
.................................
```

Related Articles

- C++ Programming: Versionable Object's Serialization using MFC - Part 1
- C++ Programming: Versionable Object's Serialization using MFC - Part 2
- The Smart Pointer That Makes Your C++ Applications Safer - std::unique_ptr

C++ Programming: Implementation of the Licensing System For a Software Product

Posted by **Apriorit Inc.** on **September 13th, 2010**

WEBINAR: On-Demand

Building the Right Environment to Support AI, Machine Learning and Deep Learning

Watch→

Hardware Serial Key

We need to have the unique identifier of the computer in order to make sure that our serial key is used on the computer where we granted a license. There are many methods of its obtaining. But we chose **HardDisk Serial Key** for this case. It has a rather readable form and small size, but the probability of collisions is very low.

```
BOOL CSmartReader::ReadSMARTInfo(BYTE ucDriveIndex)
{
    HANDLE hDevice=NULL;
    WCHAR wTempDriveName[MAX_PATH]={0};
    BOOL bRet=FALSE;
    DWORD dwRet=0;

    wsprintf(wTempDriveName,L"\\\\.\\PHYSICALDRIVE%d",ucDriveIndex);
    hDevice=CreateFile(wTempDriveName,GENERIC_READ|GENERIC_WRITE,FILE_SHARE_READ|FILE_SHARE_WRITE,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_SYSTEM,NULL);
    if(hDevice!=INVALID_HANDLE_VALUE)
    {
        bRet=DeviceIoControl(hDevice,SMART_GET_VERSION,NULL,0,&m_stDrivesInfo[ucDriveIndex].m_stGVIP,sizeof(GETVERSIONINPARAMS),&dwRet,NULL);
        if(bRet)
        {
            if((m_stDrivesInfo[ucDriveIndex].m_stGVIP.fCapabilities & CAP_SMART_CMD)==CAP_SMART_CMD)
            {
                if(IsSmartEnabled(hDevice,ucDriveIndex))
                {
```

```
                    bRet=CollectDriveInfo(hDevice,ucDriveIndex);
                    bRet=ReadSMARTAttributes(hDevice,ucDriveIndex);
                }
            }
        }
        CloseHandle(hDevice);
    }
    return bRet;
}
.....................
BOOL CSmartReader::CollectDriveInfo(HANDLE hDevice,UCHAR ucDriveIndex)
{
    BOOL bRet = FALSE;
    SENDCMDINPARAMS stCIP = {0};
    DWORD dwRet = 0;
    char szOutput[OUT_BUFFER_SIZE] = {0};

    stCIP.cBufferSize=IDENTIFY_BUFFER_SIZE;
    stCIP.bDriveNumber =ucDriveIndex;
    stCIP.irDriveRegs.bFeaturesReg=0;
    stCIP.irDriveRegs.bSectorCountReg = 1;
    stCIP.irDriveRegs.bSectorNumberReg = 1;
    stCIP.irDriveRegs.bCylLowReg = 0;
    stCIP.irDriveRegs.bCylHighReg = 0;
    stCIP.irDriveRegs.bDriveHeadReg = DRIVE_HEAD_REG;
    stCIP.irDriveRegs.bCommandReg = ID_CMD;

    bRet=DeviceIoControl(hDevice,SMART_RCV_DRIVE_DATA,&stCIP,sizeof(stCIP),szOutput,OUT_BUFFER_SIZE,&dwRet,NULL);
    if(bRet)
    {
        CopyMemory(&m_stDrivesInfo[ucDriveIndex].m_stInfo, szOutput+16, sizeof(ST_IDSECTOR));
        ConvertString(m_stDrivesInfo[ucDriveIndex].m_stInfo.sSerialNumber, 20);
    }
    else
    {
        dwRet=GetLastError();
    }
    return bRet;
}
```

As it can be seen, we receive the information about hard drives, including the `sSerialKey`, which was mentioned above.

IDC Futurescape Download Now

IDC Futurescape Download Now

So, we have the algorithms of signing, verification, and acquiring of the disk serial number.

The scheme of the licensing system

We can see the common scheme of the work of the licensing system.

[schema.png]

The **LicenseManager** source code is the following:

```
.....................................................
std::string publicKey;
    std::string privateKey;

    std::vector<char> vecPrivate;

    utils::SaveResToVector(L"PRIVATE_KEY", IDR_FILE_PRIVATE_KEY, &vecPrivate );

    //this is an example of how to generate public and private keys
    //you need to save them in .rc files or somewhere else after they are first generated
    if (vecPrivate.empty())
    {
        utils::RsaGenerateStringKeys(publicKey, privateKey);
        std::vector<char> vecPublic(publicKey.begin(), publicKey.end());
        vecPrivate.assign(privateKey.begin(), privateKey.end());
        utils::SaveVectorToFile(L"keys\\private.bin", vecPrivate);
        utils::SaveVectorToFile(L"keys\\public.bin", vecPublic);
    }
    else
    {
        privateKey.assign(vecPrivate.begin(), vecPrivate.end());
    }

    std::string sign;

    std::vector<char> smallFile;
    std::string serialKey;

    //Input the hardware serial key, that your client application will give you
    std::cout << "Input your serial key here : ";
    std::cin >> serialKey;
```

```
    //make it vector and sign using utils
    std::vector<char> hardwareSerialKey(serialKey.begin(), serialKey.end());
    utils::RsaSignVector(privateKey, hardwareSerialKey, sign);

    //save signed value to the file and send the file to user
    std::vector<char> vec(sign.begin(), sign.end());
    utils::SaveVectorToFile(L"License.dat", vec);

    std::cout << "Your license.dat file was saved in program's directory" << std::endl;
    std::cout << "Press any key...";
    std::cin.get();

    return 0;
..............................
```

The client side looks like the following:

```
........................................
std::string publicKey;
    std::vector<char> vecPublic;
    utils::SaveResToVector(L"PUBLIC_KEY", IDR_FILE_PUBLIC_KEY, &vecPublic);
    if (vecPublic.empty())
    {
        std::cout << "Cant find public key\nPress Any key..." << std::endl;
        std::cin.get();
        return 0;
    }
    publicKey.assign(vecPublic.begin(), vecPublic.end());
    CSmartReader reader;

    ST_IDSECTOR *pSectorInfo = NULL;

    reader.ReadSMARTValuesForAllDrives();

    pSectorInfo=&reader.m_stDrivesInfo[0].m_stInfo;

    std::string str(pSectorInfo->sSerialNumber);

    std::stringstream trimmer;
    trimmer << str;
    trimmer >> str;

    std::cout << "Your hardware Serial Key is : " << str << std::endl;

    try
    {
        std::vector<char> vec;
        const std::wstring fileName = L"License.dat";
        utils::LoadFileToVector(fileName, vec);

        if (utils::RsaVerifyVector(publicKey, str, vec))
        {
            std::cout << "License is valid. Continue working" << std::endl;
        }
        else
        {
            std::cout << "License is invalid. Program is being closed" << std::endl;
        }
    }
    catch(const std::logic_error& ex)
    {
        std::cout << "You do not have license.dat file installed. Please put it in program dir." << std::endl;
    }


    std::cout << "Press any key...";
    std::cin.get();
.....................................................
```

The folders structure

.\ClientTest - the client side.
.\DigitalSignature - the License Manager side.
.\Utils - utilities and wrappers for the Crypto++B. Library.
.\ cryptopp560 - Crypto++B. Library.

Bibliography list

1. C.M. Adams and H. Mailer, "Security Related Comments Regarding McEliece's Public-Key Cryptosystem" Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 224-230.
2. Cylink Corporation, Cylink Corporation vs. RSA Data Security, Inc., Civil Action No. C94-02332-CW, United States District Court for the Northern District of California, 30 Jun 1994.
3. G.I. Davida, "Chosen Signature Cryptanalysis of the RSA iMITJ Public Key Cryptosystem," Technical Report TR-CS-82-2, Department of EECS, University of Wis- consin, 1982.
4. I.M. DeLaurentis, "A Further Weakness in the Common Modulus Protocol for the RSA Cryptosystem," Cryptologia, v. 8, n. 3, Jul 1984, pp. 253-259.

5. Schneier, Bruce. *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996. ISBN 0-471-11709-9.

About the Author

Apriorit Inc.

ApriorIT is a Software Research and Development company that works in advanced knowledge-intensive scopes. Company offers integrated research&development services for the software projects in such directions as Corporate Security, Remote Control, Mobile Development, Embedded Systems, Virtualization, Drivers and others. Official site http://www.apriorit.com

Downloads

- bin.zip
- src.zip
- bin.zip
- src.zip

Comments

- There are no comments yet. Be the first to comment!
- You must have javascript enabled in order to post comments.

Leave a Comment

- Your email address will not be published. All fields are required.
- Name
- Email
- Title
- Comment
- I'm not a robot reCAPTCHA Privacy - Terms
- Post Comment

MOBILE APP DEVELOPMENT: HOW TO GROW THE POTENTIAL AND AVERT CHALLENGES

Download your free eBook today

PDF Adobe

Top White Papers and Webcasts

IDC: The Business Value of Cloud Management Platforms

vmware

This IDC Solution Brief provides insight for organizations looking to unify, automate, and proactively manage virtualized and cloud infrastructure and applications across on-premises and public cloud resources. It highlights VMware vRealize Suite, a comprehensive cloud management platform, as an example. IDC interviewed three organizations currently using a variety of VMware vRealize Suite capabilities to automate, monitor, and optimize their environments. One of these intervies is qith Chris Butler, a …

Multicloud Storage for Dummies - 2nd HPE Special Edition

Hewlett Packard Enterprise

Multicloud Storage for Dummies consists of five short chapters that explore the following: - How the multicloud storage model

Most Popular Programming Stories

- Today
- This Week
- All-Time

- There have been no articles posted today.

- 1 Creating a Bingo Game in .NET
- 2 Integrating ASP.NET MVC with GitHub

- 1 Creating a Bingo Game in .NET
- 2 Integrating ASP.NET MVC with GitHub
- 3 Connecting to an Azure SQL Database and Query Data from VS Code
- 4 Pythonic Operators on STL Set Algorithms
- 5 Creating a Typewriter Effect in .NET

More for Developers

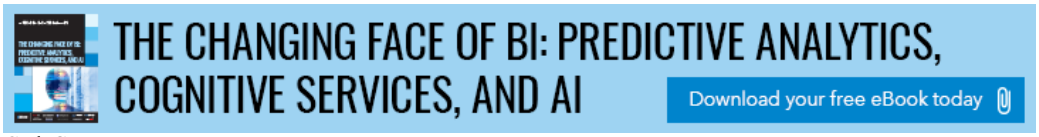
- Site Map
- News
- Windows Mobile

- Videos
- Discussions
- Blog

RSS Feeds

- All
- C#/.NET
- Win Mobile

- C++
- VB



CodeGuru

- About
- Contact Us
- FAQs
- List of Gurus
- Sitemap

Topics

- Visual C++ / C++
- .NET / C#
- Visual Basic
- Article Submission
- Video Submission

Legal

- Terms of Service
- Licensing and Permissions
- Privacy Policy
- Advertise

Copyright 2018 QuinStreet Inc. All Rights Reserved.

Thanks for your registration, follow us on our social networks to keep up-to-date