



CryptoTools 3.0 General Overview



Table of contents

TABLE OF CONTENTS	2
INTRODUCTION.....	3
LANGUAGES	3
CRYPTOTOOLS FOR C	3
CRYPTOTOOLS FOR C++.....	3
CRYPTOTOOLS FOR COM.....	4
CRYPTOTOOLS FOR .NET	4
CRYPTOTOOLS FOR JAVA.....	5
ALGORITHMS	5
DES & TRIPLEDES ENCRYPTION ALGORITHMS	5
BASE64 ENCODING ALGORITHM.....	5
MD5 HASHING ALGORITHM	6



Introduction

CryptoTools is a multi-language suite of encryption components and libraries. CryptoTools can be incorporated into your program written in C, C++, COM, VB, .Net, Java and many other popular languages.

CryptoTools provides the well known and strong encryption algorithms DES and TripleDES, as well as Base64 encoding and MD5 hashing.

Languages

CryptoTools has been developed into many different languages to help programmers add encryption capabilities into their programs and web applications without having to learn and buy multiples encryption products.

Components, files and sample programs for all languages are distributed in one single package.

CryptoTools for C

The C version of CryptoTools is distributed as a DLL and comes with a library, the appropriate headers files and documentation. The following files are required to add CryptoTools to your application.

- ❑ bin\CryptoDLL.dll
- ❑ bin\CryptoDLL.lib
- ❑ ICryptoBase64.h
- ❑ ICryptoMD5.h
- ❑ ICryptoDES.h
- ❑ ICryptoTripleDES.h

You will also find help files in the “doc” directory, as well as sample code in the “samples” folder.

CryptoTools for C++

You can use CryptoTools in C++ using many of the components distributed in this package. You can link with the CryptoDLL.dll library, which contains class definitions for the CryptoTools components. You may also use the COM version of the component or the .Net version in managed C++. These last two methods are described in more detail in the following sections.



The classes in the DLL can only be used with Microsoft Visual C++ because of the name mangling. The following files are required to add CryptoTools C++ object classes to your application.

- ❑ bin\CryptoDLL.dll
- ❑ bin\CryptoDLL.lib
- ❑ ICryptoBase64.h
- ❑ ICryptoMD5.h
- ❑ ICryptoDES.h
- ❑ ICryptoTripleDES.h

CryptoTools for COM

The COM version of CryptoTools components can be used in a wide variety of programming languages. Any language that supports COM objects can integrate CryptoTools functionalities. The following is a list of the major languages supported:

- ❑ C++
- ❑ VB6
- ❑ ASP
- ❑ VBScript
- ❑ JScript
- ❑ Coldfusion

The only file required to add CryptoTools functionalities to your COM application is the CryptoCOM.dll file.

CryptoTools for .Net

CryptoTools has also been developed for the .Net platform. All languages compatible with the .Net framework work with the CryptoTools for .Net component. This version has been developed in native .Net and is not an “Interop” for the COM version of CryptoTools.

The following is a list of the major .Net languages supported by CryptoTools:

- ❑ C#
- ❑ VB.Net
- ❑ ASP.Net
- ❑ Managed C++
- ❑ J#



To add CryptoTools functionalities to your .Net application, you have to add the CryptoNET.dll assembly to your project references.

CryptoTools for Java

The Java version of the CryptoTools suite of components implements the same objects and APIs as the other languages. This version has been developed in native Java with the J2 SDK 1.4.

To add CryptoTools to your Java application you must add the CryptoTools.jar library into your application classpath. Only the jar file is required to compile your application with CryptoTools.

CryptoTools for Java allows you to run your application on all platforms supporting Java.

Algorithms

The CryptoTools suite of components and libraries offers DES and CryptoDES encryption, as well as base64 encoding and MD5-hashing algorithms.

DES & TripleDES encryption algorithms

You can encrypt binary data, text and files using the DES (56 bit) and TripleDES (168 bit) encryption algorithms.

Both the DES and the TripleDES encryption components provide a function to derive an encryption key from a text password.

The DES and TripleDES encryption process' result is binary. You can convert it to base4 using Crypto Tools' base64 encoding component of CryptoTools.

Base64 encoding algorithm

Base64 is an encoding algorithm that allows you to convert binary data to ASCII text. This allows you, for example, to send encoded data over email. Text encoding is also useful for persisting data into databases or text files like XML.



MD5 hashing algorithm

A hashing algorithm is a one-way encryption process. The MD5 algorithm produces a 128 bit hash value that is said to be unique for every piece of data it processes. This is often used to digitally sign data when used in conjunction with public/private key algorithms.