

# ADSYSTECH NETWORK OPERATING CENTER

## SOFTWARE ENCRYPTION TECHNIQUES



Adsytech, Inc.  
Network Operating Center  
200 Oceangate, Suite 800  
Long Beach, CA 90802  
**888 602.2225 - Office**  
**562 436.8419 - Fax**

Adsystem Inc. - Network Operating Center  
200 Oceangate, Suite 800  
888 602.2225 Office  
562 436.8419 Fax  
[www.Adsystem.com](http://www.Adsystem.com)

# Contents

<b>ADSYSTECH NETWORK OPERATING CENTER SOFTWARE SECURITY</b>	<b>4</b>
<b>CHAPTER 1 - OVERVIEW</b>	<b>4</b>

# Adsystem Network Operating Center Software Security

## Chapter 1 - Overview

### Introduction

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *codebreaking*, although modern cryptography techniques are virtually unbreakable.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and *public-key* systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

- **Encryption Adsystem uses:**
  - SSL encryption & Rijndael (*Rain-Doll*)
- **Secure Socket Layer (SSL)**
  - Adsystem uses SSL to protect Security Manager and User Logon's during the application logon process. This connection uses port 443.
  - SSL uses a [cryptographic](#) system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. By convention, URLs that require an SSL connection start with *https:* instead of *http:*.
- **Rijndael**
  - Adsystem uses Rijndael at the database level. Flags are turned on to determine what fields will be passed using encryption. From the dbase level encrypted information is passed to our application using port 80.
  - Short for ***Advanced Encryption Standard***, a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it

used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called **Rijndael** (pronounced *Rhine Dahl* or *Rain Doll*), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM.

- While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.

- **More about Rijndael from Federal Information Processing Standards Publications**

- The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. Rijndael is one of only five approved standards.

The [National Security Agency](#) (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for [US Government](#) non-classified data. In June 2003, the US Government announced that AES may be used for [classified information](#):

*"The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the **SECRET level**. **TOP SECRET information** will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use." — [2]*

This page is intentionally left blank



Adsystem, Inc.  
Network Operating Center  
200 Oceangate, Suite 800  
Long Beach, CA 90802  
**888 602.2225 - Office**  
**562 436.8419 - Fax**