MediaCrypt®

IDea™

International Data Encryption Algorithm

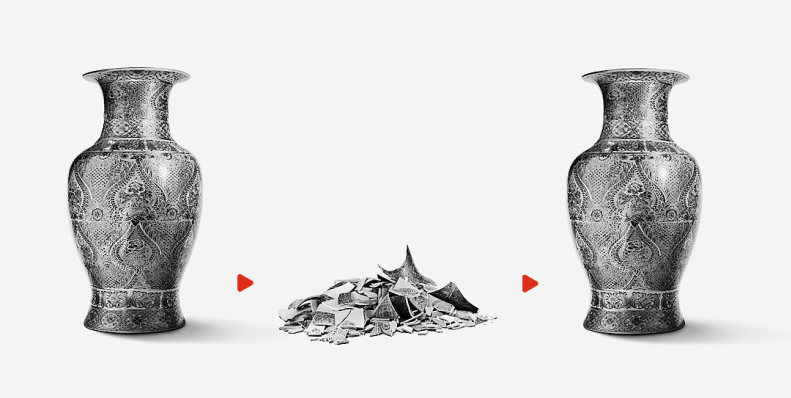
The IDEA data encryption algorithm...

- provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key
- is fully specified and easily understood
- is available to everybody
- is suitable for use in a wide range of applications
- can be economically implemented in electronic components (VLSI chip)
- can be used efficiently
- may be exported worldwide
- is strong, small and fast

IDEA is the name of the patented and universally applicable block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties. With a key of 128 bits in length, IDEA is far more secure than the widely known DES based on a 56-bit key. The fundamental criteria for the development of IDEA were military strength for all security requirements and easy hardware and software implementation. The algorithm is used worldwide in various banking and industry applications. They predestine the algorithm for use in a great number of commercial applications.

IDEA algorithm

The IDEA algorithm was developed in a joint project involving the Swiss Federal Institute of Technology in Zurich and Ascom.



The aim of the project was to develop a strong encryption algorithm, which would replace the DES procedure developed in the U.S.A. in the seventies.

MediaCrypt®

Factsheet IDEA_0304

IDEA International Data Encryption Algorithm

Data protection by means of encryption

As electronic communications grow in importance, there is also an increasing need for data protection. Encryption ensures that:

- Only authorized persons can access information.
- Data cannot be amended or manipulated by unauthorized persons.
- Unbreakable crypt system warrants military strength security level.

IDEA solutions

When PGP (Pretty Good Privacy) was designed, the developers were looking for maximum security. IDEA was their first choice for data encryption based on its proven design and its great reputation. Today, there are hundreds of IDEA-based security solutions available.

IDEA registration in standards

- ISO 9979/002: ISO Register of Cryptographic Algorithms
- UN/EDIFACT: EDIFACT Security Implementation Guidelines
- ITU-T Recommendation H.233: Confidentiality System for Audiovisual Services
- IETF RFC 3058: Use of the IDEA Encryption Algorithm in CMS
- TBSS: Telematic Base Security Services
- OpenSSL Cryptographic Library
- WAP Wireless Transport Layer Security
- NESSIE (New European Schemes for Signature, Integrity, and Encryption): Call for Cryptographic Primitives – finalist

Submitted to:

- ISO NP 18033: Encryption algorithms

Applications

The IDEA algorithm can easily be embedded in any encryption software.
Data encryption can be used to protect data transmission and storage. Typical fields are:

- Audio and video data for cable TV, pay TV, video conferencing, distance learning, business TV, VoIP
- Sensitive financial and commercial data
- Email via public networks
- Transmission links via modem, router or ATM link, GSM technology
- Smart cards

Hardware

The IDEA crypt-kernel is the right choice whenever maximum security combined with high-speed performance is demanded. This kernel features extraordinary encryption/decryption performance in the range of 7 Gbit/s and is designed for any kind of hardware implementation.

Our products and services

- IDEA algorithm in ANSI C/C++, and Java code
- Crypto toolkit for optimized implementation of IDEA into products
- IDEA crypt-kernel
- Security consulting/engineering for secure data, voice and video communication solutions

How secure is IDEA

It would take one billion computers testing one billion combinations per second, 10'000 billion years to crack the code (2^{128} variants) - longer than the universe has existed.

Licenses

Companies wishing to deploy the IDEA algorithm on a commercial basis can obtain a license in return for a small fee. There are several types of licenses available.
Additional licensing information is available on our web page at: www.mediacrypt.com

...at a glance

- **Strong, small, fast**
- **Resistant against all known crypto attacks**
- **Available worldwide**
- **Patent protection**
  EU: 0 482 154 B1
  US: 5,214,703
  JP: 3,225,440 B2

MEDIACRYPT AG | TECHNOPARKSTRASSE 1 | 8005 ZURICH SWITZERLAND
TEL. + 41 44 445 30 70 | FAX + 41 44 445 30 71 | WWW.MEDIACRYPT.COM