



WIKIPEDIA  
The Free Encyclopedia

Main page  
Contents  
Featured content  
Current events  
Random article  
Donate to Wikipedia  
Wikipedia store

Interaction  
Help  
About Wikipedia  
Community portal  
Recent changes  
Contact page

Tools  
What links here  
Related changes  
Upload file  
Special pages  
Permanent link  
Page information  
Wikidata item  
Cite this page

Print/export  
Create a book  
Download as PDF  
Printable version

Languages  
Български  
Català  
Čeština  
Deutsch  
Español  
Euskara  
فارسی  
Français  
한국어  
Italiano  
עברית  
Nederlands  
日本語  
Polski  
Português

★ Русский  
Simple English  
Slovenščina  
Suomi  
Тоҷикӣ  
Türkçe  
Українська  
Tiếng Việt  
中文

Edit links

Create account Log in

Article **Talk**

Read **Edit** View history

Search

# International Data Encryption Algorithm

From Wikipedia, the free encyclopedia

In **cryptography**, the **International Data Encryption Algorithm** (**IDEA**), originally called **Improved Proposed Encryption Standard (IPES)**, is a **symmetric-key block cipher** designed by **James Massey** of **ETH Zurich** and **Xuejia Lai** and was first described in 1991. The algorithm was intended as a replacement for the **Data Encryption Standard (DES)**. IDEA is a minor revision of an earlier **cipher**, **Proposed Encryption Standard (PES)**.

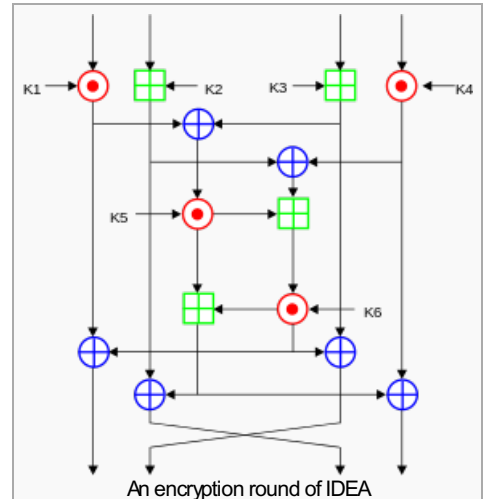
The cipher was designed under a research contract with the Hasler Foundation, which became part of Ascom-Tech AG. The cipher was patented in a number of countries but was freely available for non-commercial use. The name "IDEA" is also a **trademark**. The last **patents** expired in 2012 and IDEA is now patent-free and thus free to use.<sup>[2][3]</sup>

IDEA was used in **Pretty Good Privacy (PGP)** v2.0, and was incorporated after the original cipher used in v1.0, **BassOmatic**, was found to be insecure.<sup>[4]</sup> IDEA is an optional algorithm in the **OpenPGP** standard.

## Contents [hide]

- Operation
  - Structure
  - Key schedule
  - Decryption
- Security
  - Weak keys
- Availability
- Literature
- References
- External links

## IDEA



## General

**Designers** Xuejia Lai and James Massey  
**Derived from** PES  
**Successors** MMB, MESH, Akelarre, IDEANXT (FOX)

## Cipher detail

**Key sizes** 128 bits  
**Block sizes** 64 bits  
**Structure** Lai-Massey scheme  
**Rounds** 8.5

## Best public cryptanalysis

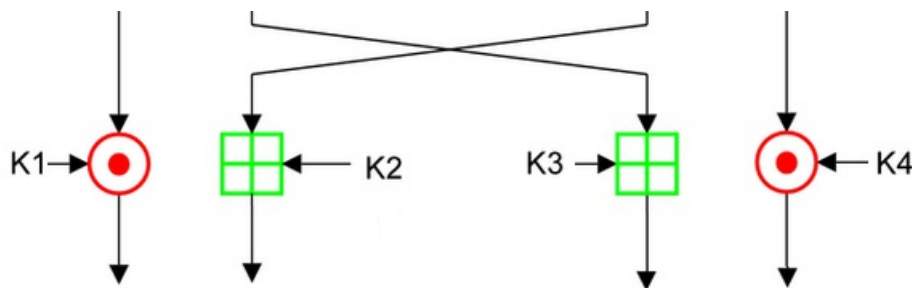
The key can be recovered with a computational complexity of  $2^{126.1}$  using narrow **bidiques**. This attack is computationally faster than a full brute force attack, though not, as of 2013, computationally feasible.<sup>[1]</sup>

## Operation [edit]

IDEA operates on 64-bit **blocks** using a 128-bit **key**, and consists of a series of eight identical transformations (a *round*, see the illustration) and an output transformation (the *half-round*). The processes for encryption and decryption are similar. IDEA derives much of its security by interleaving operations from different **groups** — **modular** addition and multiplication, and bitwise **eXclusive OR (XOR)** — which are algebraically "incompatible" in some sense. In more detail, these operators, which all deal with 16-bit quantities, are:

- Bitwise **eXclusive OR** (denoted with a blue circled plus  $\oplus$ ).
- Addition modulo  $2^{16}$  (denoted with a green boxed plus  $\boxplus$ ).
- Multiplication modulo  $2^{16}+1$ , where the all-zero word (0x0000) in inputs is interpreted as  $2^{16}$  and  $2^{16}$  in output is interpreted as the all-zero word (0x0000) (denoted by a red circled dot  $\odot$ ).

After the eight rounds comes a final "half round", the output transformation illustrated below (the swap of the middle two values cancels out the swap at the end of the last round, so that there is no net swap):



### Structure [\[edit\]](#)

The overall structure of IDEA follows the [Lai-Massey scheme](#). XOR is used for both subtraction and addition. IDEA uses a key-dependent half-round function. To work with 16 bit words (meaning four inputs instead of two for the 64 bit block size), IDEA uses the Lai-Massey scheme twice in parallel, with the two parallel round functions being interwoven with each other. To ensure sufficient diffusion, two of the sub-blocks are swapped after each round.

### Key schedule [\[edit\]](#)

Each round uses six 16-bit sub-keys, while the half-round uses four, a total of 52 for 8.5 rounds. The first eight sub-keys are extracted directly from the key, with K1 from the first round being the lower sixteen bits; further groups of eight keys are created by rotating the main key left 25 bits between each group of eight. This means that it is rotated less than once per round, on average, for a total of six rotations.

### Decryption [\[edit\]](#)

Decryption works like encryption, but the order of the round keys is inverted, and each value of subkeys K1 – K4 is replaced by its inverse for the respective group operation (K5 and K6 of each group should not be changed for decryption).

### Security [\[edit\]](#)

The designers analysed IDEA to measure its strength against [differential cryptanalysis](#) and concluded that it is immune under certain assumptions. No successful [linear](#) or algebraic weaknesses have been reported. As of 2007, the best attack which applied to all keys could break IDEA reduced to 6 rounds (the full IDEA cipher uses 8.5 rounds).<sup>[5]</sup> Note that a "break" is any attack which requires less than  $2^{128}$  operations; the 6-round attack requires  $2^{64}$  known plaintexts and  $2^{126.8}$  operations.

[Bruce Schneier](#) thought highly of IDEA in 1996, writing, "In my opinion, it is the best and most secure block algorithm available to the public at this time." (*Applied Cryptography*, 2nd ed.) However, by 1999 he was no longer recommending IDEA due to the availability of faster algorithms, some progress in its cryptanalysis, and the issue of patents.<sup>[6]</sup>

In 2011 full 8.5-round IDEA was broken using a meet-in-the-middle attack.<sup>[7]</sup> Independently in 2012, full 8.5 round IDEA was broken using a narrow-[bicliques attack](#), with a reduction of cryptographic strength of about two bits, similar to the effect of the previous bicliques attack on [AES](#).<sup>[8]</sup>

### Weak keys [\[edit\]](#)


The very simple key schedule makes IDEA subject to a class of [weak keys](#); some keys containing a large number of 0 bits produce weak encryption.<sup>[9]</sup> These are of little concern in practice, being sufficiently rare that they are unnecessary to avoid explicitly when generating keys randomly. A simple fix was proposed: exclusive-ORing each subkey with a 16-bit constant, such as `0x0DAE`.<sup>[9][10]</sup>

Larger classes of weak keys were found in 2002.<sup>[11]</sup>

This is still of negligible probability to be a concern to a randomly chosen key, and some of the problems are fixed by the constant XOR proposed earlier, but the paper is not certain if all of them are. A more comprehensive redesign of the IDEA key schedule may be desirable.<sup>[11]</sup>


### Availability [\[edit\]](#)

A patent application for IDEA was first filed in [Switzerland](#) (CHA 1690/90) on May 18, 1990, then an international patent application was filed under the [Patent Cooperation Treaty](#) on May 16, 1991. Patents were eventually granted in [Austria](#), [France](#), [Germany](#), [Italy](#), the [Netherlands](#), [Spain](#), [Sweden](#), [Switzerland](#), the [United Kingdom](#), (European Patent Register entry for [European patent no. 0482154](#) [↗](#), filed May 16, 1991, issued June

22, 1994 and expired May 16, 2011), the [United States](#) ([U.S. Patent 5,214,703](#) , issued May 25, 1993 and expired January 7, 2012) and [Japan](#) (JP 3225440) (expired May 16, 2011)).<sup>[12]</sup>

MediaCrypt AG is now offering a successor to IDEA and focuses on its new cipher (official release on May 2005) [IDEA NXT](#), which was previously called FOX.

## Literature [\[edit\]](#)

- Hüseyin Demirci, Erkan Türe, Ali Aydın Selçuk, A New Meet in the Middle Attack on The IDEA Block Cipher, 10th Annual Workshop on [Selected Areas in Cryptography](#), 2004.
- Xuejia Lai and James L. Massey, [A Proposal for a New Block Encryption Standard](#) , EUROCRYPT 1990, pp389–404
- Xuejia Lai and James L. Massey and S. Murphy, Markov ciphers and differential cryptanalysis, *Advances in Cryptology — Eurocrypt '91*, Springer-Verlag (1992), pp17–38.

## References [\[edit\]](#)

1.  <http://www.cs.bris.ac.uk/eurocrypt2012/Program/Tues/Rechberger.pdf> 
2.  ["Espacenet - Bibliografische Daten"](#)  (in German). Worldwide.espacenet.com. Retrieved 2013-06-15.
3.  ["Espacenet - Bibliografische Daten"](#)  (in German). Worldwide.espacenet.com. Retrieved 2013-06-15.
4.  [Garfinkel, Simson](#) (December 1, 1994), *PGP: Pretty Good Privacy*, [O'Reilly Media](#), pp. 101–102, ISBN 978-1-56592-098-9
5.  [Biham, E.](#); Dunkelman, O.; Keller, N. "A New Attack on 6-Round IDEA" . Springer-Verlag.
6.  ["Slashdot: Crypto Guru Bruce Schneier Answers"](#) . slashdot.org. Retrieved 2010-08-15.
7.  ["New Attacks on IDEA with at Least 6 Rounds"](#) .
8.  [Khovratovich, D.](#); Leurent, G.; Rechberger, C. "Narrow-Bicliques: Cryptanalysis of Full IDEA" . Springer-Verlag. (subscription required)
9.    [Daemen, Joan](#); Govaerts, Rene; Vandewalle, Joos (1993), "Weak Keys for IDEA" , *Advances in Cryptology, CRYPTO 93 Proceedings*: 224–231
10.  [Nakahara, Jorge Jr.](#); Preneel, Bart; Vandewalle, Joos (2002), *A note on Weak Keys of PES, IDEA and some Extended Variants* 
11.    [Biryukov, Alex](#); Nakahara, Jorge Jr.; Preneel, Bart; Vandewalle, Joos, "New Weak-Key Classes of IDEA"  (PDF), *Information and Communications Security, 4th International Conference, ICICS 2002*, Lecture Notes in Computer Science 2513: 315–326, "While the zero-one weak keys problem of IDEA can be corrected just by XORing a fixed constant to all the keys (one such constant may be 0DAE<sub>x</sub> as suggested in [4]) the problem with the runs of ones may still remain and will require complete redesign of the IDEA key schedule."
12.  ["GnuPG 1.4.13 released"](#) . Werner Koch. Retrieved 2013-10-06.















- [RSA FAQ on Block Ciphers](#)
- [SCAN entry for IDEA](#)
- [IDEA in 448 bytes of 80x86](#)
- [IDEA Applet](#)

<span>v · t · e</span>	Block ciphers (security summary)
<b>Common algorithms</b>	<span>AES · Blowfish · DES (Internal Mechanics, Triple DES) · Serpent · Twofish</span>
<b>Less common algorithms</b>	<span>Camellia · CAST-128 · <b>IDEA</b> · RC2 · RC5 · SEED · ARIA · Skipjack · TEA · XTEA</span>
<b>Other algorithms</b>	<span>3-Way · Akelarre · Anubis · BaseKing · BassOmatic · BATON · BEAR and LION · CAST-256 · Chiasmus · CIKS-1 · CIPHERUNICORN-A · CIPHERUNICORN-E · CLEFIA · CMEA · Cobra · COCONUT98 · Crab · Cryptomeria/C2 · CRYPTON · CS-Cipher · DEAL · DES-X · DFC · E2 · FEAL · FEA-M · FROG · G-DES · GOST · Grand Cru · Hasty Pudding cipher · Hierocrypt · ICE · IDEANXT · Intel Cascade Cipher · Iraqi · KASUMI · KeeLoq · KHAZAD · Khufu and Khafre · KN-Cipher · Ladder-DES · Libelle · LOKI (97, 89/91) · Lucifer · M6 · M8 · MacGuffin · Madryga · MAGENTA · MARS · Mercy · MESH · MISTY1 · MMB · MULTI2 · MultiSwap · New Data Seal · NewDES · Nimbus · NOEKEON · NUSH · PRESENT · Q · RC6 · REDOC · Red Pike · S-1 · SAFER · SAVILLE · SC2000 · SHACAL · SHARK · Simon · SMS4 · Speck · Spectr-H64 · Square · SXAL/MBAL · Threefish · Treyfer · UES · Xenon · xmx · XXTEA · Zodiac</span>
<b>Design</b>	<span>Feistel network · Keyschedule · Lai-Massey scheme · Product cipher · S-box · P-box · SPN · Avalanche effect · Block size · Key size · Key whitening (Whitening transformation)</span>
<b>Attack (cryptanalysis)</b>	<span>Brute-force (EFF DES cracker) · MITM (Bidiq attack, 3-subset MITM attack) · Linear (Piling-up lemma) · Differential (Impossible · Truncated · Higher-order) · Differential-linear · Integral/Square · Boomerang · Mod <i>n</i> · Related-key · Slide · Rotational · Timing · XSL · Interpolation · Partitioning · Davies' · Rebound · Weak key · Tau · Chi-square · Time/memory/data tradeoff</span>
<b>Standardization</b>	<span>AES process · CRYPTREC · NESSIE</span>
<b>Utilization</b>	<span>Initialization vector · Mode of operation · Padding</span>
<span>v · t · e</span>	Cryptography
	<span>History of cryptography · Cryptanalysis · Cryptography portal · Outline of cryptography</span>
	<span>Symmetric-key algorithm · Block cipher · Stream cipher · Public-key cryptography · Cryptographic hash function · Message authentication code · Random numbers · Steganography</span>

Categories: [Block ciphers](#) | [Broken block ciphers](#)