Symmetric-key algorithm

From Wikipedia, the free encyclopedia
(Redirected from Symmetric key algorithm)

Symmetric-key algorithms[1] are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.[2] This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.[3]

Types of symmetric-key algorithms [edit]

Symmetric-key encryption can use either stream ciphers or block ciphers.[4]

- Stream ciphers encrypt the digits (typically bytes) of a message one at a time.
- Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks.

Implementations [edit]

Examples of popular symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, 3DES, Skipjack, Safer+/++ (Bluetooth), and IDEA.[*citation needed*]

Cryptographic primitives based on symmetric ciphers [edit]

Symmetric ciphers are commonly used to achieve other cryptographic primitives than just encryption.[*citation needed*]

Encrypting a message does not guarantee that this message is not changed while encrypted. Hence often a message authentication code is added to a ciphertext to ensure that changes to the ciphertext will be noted by the receiver. Message authentication codes can be constructed from symmetric ciphers (e.g. CBC-MAC).[*citation needed*]

However, symmetric ciphers cannot be used for non-repudiation purposes except by involving additional parties. See the ISO/IEC 13888-2 standard.[*citation needed*]

Another application is to build hash functions from block ciphers. See one-way compression function for descriptions of several such methods.[*citation needed*]

Construction of symmetric ciphers [edit]

Main article: Feistel cipher

Many modern block ciphers are based on a construction proposed by Horst Feistel. Feistel's construction makes it possible to build invertible functions from other functions that are themselves not invertible.[*citation needed*]

Security of symmetric ciphers [edit]

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
العربية
Català
Čeština
Deutsch
Ελληνικά
Español
Esperanto
Euskara
فارسی
Français
한국어
Հայերեն
Italiano
עברית
ქართული
Lietuvių
Magyar
Nederlands
日本語
Norsk bokmål
Polski
Português
Русский
Simple English
Slovenčina
Suomi
Svenska
Türkçe
Українська

Symmetric ciphers have historically been susceptible to known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis and linear cryptanalysis. Careful construction of the functions for each round can greatly reduce the chances of a successful attack.[*citation needed*]

Key generation [edit]

When used with asymmetric ciphers for key transfer, pseudorandom key generators are nearly always used to generate the symmetric cipher session keys. However, lack of randomness in those generators or in their initialization vectors is disastrous and has led to cryptanalytic breaks in the past. Therefore, it is essential that an implementation uses a source of high entropy for its initialization.[5][6][7]

Notes [edit]

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed. *(April 2012)*

1. ^ Other terms for symmetric-key encryption are **secret-key**, **single-key**, **shared-key**, **one-key**, and **private-key** encryption. Use of the last and first terms can create ambiguity with similar terminology used in public-key cryptography. Symmetric-key cryptography is to be contrasted with asymmetric-key cryptography.
2. ^ Delfs, Hans & Knebl, Helmut (2007). "Symmetric-key encryption". *Introduction to cryptography: principles and applications*. Springer. ISBN 9783540492436.
3. ^ Mullen, Gary & Mummert, Carl (2007). *Finite fields and applications*. American Mathematical Society. p. 112. ISBN 9780821844182.
4. ^ Pelzl & Paar (2010). *Understanding Cryptography.* Berlin: Springer-Verlag. p. 30.
5. ^ Ian Goldberg and David Wagner. "Randomness and the Netscape Browser". January 1996 Dr. Dobb's Journal. quote: "it is vital that the secret keys be generated from an unpredictable random-number source."
6. ^ Thomas Ristenpart , Scott Yilek. "When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography (2010)" CiteSeerX: 10.1.1.183.3583 quote from abstract: "Random number generators (RNGs) are consistently a weak link in the secure use of cryptography."
7. ^ "Symmetric Cryptography". James. 2006-03-11.

v · t · e	**Block ciphers (security summary)**
Common algorithms	AES · Blowfish · DES (Internal Mechanics, Triple DES) · Serpent · Twofish
Less common algorithms	Camellia · CAST-128 · IDEA · RC2 · RC5 · SEED · ARIA · Skipjack · TEA · XTEA
Other algorithms	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 · IDEA NXT · 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
Design	Feistel network · Key schedule · Lai-Massey scheme · Product cipher · S-box · P-box · SPN · Avalanche effect · Block size · Key size · Key whitening (Whitening transformation)
Attack (cryptanalysis)	Brute-force (EFF DES cracker) · MITM (Biclique attack, 3-subset MITM attack) · Linear (Piling-up lemma) · Differential (Impossible · Truncated · Higher-order) · Differential-linear · Integral/Square · Boomerang · Mod *n* · Related-key · Slide · Rotational · Timing · XSL · Interpolation · Partitioning · Davies' · Rebound · Weak key · Tau · Chi-square · Time/memory/data tradeoff
Standardization	AES process · CRYPTREC · NESSIE
Utilization	Initialization vector · Mode of operation · Padding

v · t · e	**Stream ciphers**	
Widely used ciphers	RC4 · Block ciphers in stream mode	
eSTREAM Portfolio	**Software**	HC-256 · Rabbit · Salsa20 · SOSEMANUK
	Hardware	Grain · MICKEY · Trivium
Other ciphers	A5/1 · A5/2 · Achterbahn · E0 · F-FCSR · FISH · ISAAC · MUGI · Panama · Phelix · Pike · Py · QUAD · Scream · SEAL · SNOW · SOBER · SOBER-128 · VEST · WAKE	
Theory	Shift register · LFSR · NLFSR · Shrinking generator · T-function · IV	
Attacks	Correlation attack · Correlation immunity	

v · t · e **Cryptography**

History of cryptography · Cryptanalysis · Cryptography portal · Outline of cryptography

Symmetric-key algorithm · Block cipher · Stream cipher · Public-key cryptography · Cryptographic hash function · Message authentication code · Random numbers · Steganography

Authority control GND: 4317451-6

Categories: Cryptographic algorithms