Stream Cipher And Block Cipher

Block cipher mode of operation A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block. In cryptography, a block cipher mode of operation is an algorithm that uses a block cipher to provide information security such as confidentiality or In cryptography, a block cipher mode of operation is an algorithm that uses a block cipher to provide information security such as confidentiality or authenticity. A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block a0aec451fb

Iraqi block cipher cryptography, the Iraqi block cipher was a block cipher published in C source code form by anonymous FTP upload around July 1999, and widely distributed on In cryptography, the Iraqi block cipher was a block cipher published in C source code form by anonymous FTP upload around July 1999, and widely distributed on Usenet. It is a five round unbalanced Feistel cipher operating on a 256 bit block with a 160 bit key a0aec451fb

Speck (cipher) Speck is part of a family of lightweight block ciphers publicly released by the National Security Agency (NSA) in June 2013. Speck has been optimized a0aec451fb

A block cipher uses blocks as an unvarying transformation. Even a secure block cipher is suitable for the encryption of only a single block of data at a time, using a fixed key. A multitude of modes of operation have been designed to allow their repeated use in a secure way to achieve the other security goals of confidentiality and authenticity. However, block ciphers may also feature as building blocks in other cryptographic protocols, such as universal hash functions and pseudorandom number generators. a0aec451fb The pseudorandom keystream is typically generated serially from a random seed value using digital shift registers. The seed value serves as the cryptographic key for decrypting the ciphertext stream. Stream ciphers represent a different approach to symmetric encryption from block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. This distinction is not always clear-cut: in some modes of operation, a block cipher primitive is used in such a way that it acts effectively as a stream cipher. Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity. However, stream ciphers can be susceptible to security breaches... a0aec451fb The source code shows that the algorithm operates on blocks of 32 bytes (or 256 bits). That's four times larger than DES or 3DES (8 bytes) and twice as big as Twofish or AES (16 bytes). It also shows that the key size can vary from 160 to 2048 bits. a0aec451fb == History == a0aec451fb == Table color key == a0aec451fb

Cipher An alternative, less common term is encipherment. By whether the same In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. In common parlance, "cipher" is synonymous with "code", as they are both a set of steps that encrypt a message; however, the concepts are distinct in cryptography, especially classical cryptography. whether they work on blocks of symbols usually of a fixed size (block ciphers), or on a continuous stream of symbols (stream ciphers). To encipher or encode is to convert information into cipher or code a0aec451fb

Codes generally substitute different length strings of characters in the output, while ciphers generally substitute the same number of characters as are input. A code maps one meaning with another. Words and phrases can be coded as letters or numbers. Codes typically have direct meaning from input to key. Codes primarily function to save time. Ciphers are algorithmic. The given input must follow the cipher's process to be solved. Ciphers are commonly used to encrypt written information. a0aec451fb

Block cipher Block ciphers are the elementary In cryptography, a block cipher is a deterministic algorithm that operates on fixed-length groups of bits, called blocks. cryptography, a block cipher is a deterministic algorithm that operates on fixed-length groups of bits, called blocks. They are ubiquitous in the storage and exchange of data, where such data is secured and authenticated via encryption. Block ciphers are the elementary building blocks of many cryptographic protocols a0aec451fb

== References == a0aec451fb

BEAR and LION ciphers Both are 3-round generalized (alternating) Feistel ciphers, using the hash function and the stream cipher as round functions. The inventors proved that an attack on either BEAR or LION that recovers the key would break both the stream cipher and the hash. The BEAR and LION block ciphers were invented by Ross Anderson and Eli Biham by combining a stream cipher and a cryptographic hash function. The algorithms The BEAR and LION block ciphers were invented by Ross Anderson and Eli Biham by combining a stream cipher and a cryptographic hash function. LION uses the stream cipher twice and the hash function once. The algorithms use a very large variable block size, on the order of 213 to 223 bits or more. BEAR uses the hash function twice with independent keys, and the stream cipher once a0aec451fb

Cryptomeria cipher It is the successor to CSS algorithm (used. The Cryptomeria cipher, also called C2, is a proprietary block cipher defined and licensed by the 4C Entity a0aec451fb

Stream cipher stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. In practice, a digit is typically a bit and the combining operation is an exclusive-or (XOR). In a stream cipher, A stream cipher is a

symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher a0aec451fb

Cipher security summary Note that there are perhaps attacks that are not publicly known, and not all entries may be up This article summarizes publicly known attacks against block ciphers and stream ciphers. publicly known attacks against block ciphers and stream ciphers. Note that there are perhaps attacks that are not publicly known, and not all entries may be up to date a0aec451fb

A comment suggests that it is of Iraqi origin. However, like the S-1 block cipher, it is generally regarded as a hoax, although of lesser quality than S-1. Although the comment suggests that it is Iraqi in origin, all... a0aec451fb

Feistel cipher cryptography, a Feistel cipher (also known as Luby–Rackoff block cipher) is a symmetric structure used in the construction of block ciphers, named after the In cryptography, a Feistel cipher (also known as Luby–Rackoff block cipher) is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel, who did pioneering research while working for IBM; it is also commonly known as a Feistel network. A large number of block ciphers use the scheme, including the US Data Encryption Standard, the Soviet/Russian GOST (aka Magma) and the more recent Blowfish and Twofish ciphers. In a Feistel cipher, encryption and decryption are very similar operations, and both consist of iteratively running a function called a "round function" a fixed number of times a0aec451fb

Many modern symmetric block ciphers are based on Feistel networks. Feistel networks were first seen commercially in IBM's Lucifer cipher, designed by Horst Feistel and Don Coppersmith in 1973. Feistel networks gained respectability when the U.S. Federal Government adopted the DES (a cipher based on Lucifer, with changes made by the NSA) in 1976. Like other components of the DES, the iterative nature of the Feistel construction makes implementing the cryptosystem in hardware easier (particularly on the hardware available... a0aec451fb Codes operated by substituting according to a large codebook which linked a random string of characters or numbers to a word or phrase. For example, "UQJHSE" could be the code for "Proceed to the following coordinates.". When using... a0aec451fb Most modes require a unique binary sequence, often called an initialization vector (IV), for each encryption operation. The IV must be non-repeating, and for some modes must also be random. The initialization vector is used to ensure that distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key. Block ciphers may be capable of operating on more than one block size, but during transformation the block size is always fixed. Block cipher modes operate on whole blocks and require that the final data fragment be padded to a full block if it is smaller than the current block size. There are, however, modes that do not require padding because they effectively... a0aec451fb A detailed analysis of the source code of the algorithm shows that it uses a 256-byte S-Box that is key-dependant (as on Blowfish, it uses a first fixed S table that will generate, with the key, the second S-Box used for encryption/decryption). The algorithm also uses a 16-column x 16-row P-Box, which is also key-dependent and also initialized from a fixed P table. Each round uses one row from P-Box and 16 columns, which means that the algorithm can use up to 16 rounds. a0aec451fb == Definition == a0aec451fb