Cipher

AES encryption BY nf623 There are two basic types of encryption; asymmetrical and symmetrical. Asymmetrical uses two keys; a public and a private key. The public and the private keys have unique characteristics. In asymmetric encryption you can encrypt with a public key that has a matching private key used for decryption. The other basic type of encryption is called symmetric encryption; the main difference between the two is that symmetrical encryption uses only one key; a private key used for both encryption and decryption.

Asymmetric encryption is used when there are two end points, such as a VPN client communicating with a VPN server. Symmetric encryption is used most commonly when there is only one end point such as a database on a single computer, where you encrypt it before you store it, and you decrypt it to return it. Symmetric is also orders of magnitude fast then Asymmetrical, therefore in database applications where performance is really an issue, symmetrical encryption is most often used. AES is a symmetrical encryption standard. The Advanced Encryption

Standard, or AES is a specification for the encryption of electronic data established by the U. S. National Institute of standards and technology in 2001. It is based on the RiJndael cipher, and was developed by two Belgian cryptographers, Joan Daemen and Vincent RiJmen . AES is based in a design principlae known as a substitution- permutation network, and is fast both in software and hardware (Schneier). Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of RiJndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

By contrast, the RiJndael specification is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4x4 colum major order matrix of bytes, although some versions of RiJndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

The number of cycles of repetition are as follows: 10 cycles of repetition for 128-bit keys. 12 cycles of repetition for 192-bit keys. 14 cycles of repetition for 256-bit keys. Each round consists of several processing steps, each containing five similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. Algorithm used in AES 1 . KeyExpansion” round keys are derived from the cipher key using RiJndael's key chedule.

AES requires a separate 128-bit round key block for each round plus one more. 2. InitialRound 1. AddRoundKey” each byte of the state is combined with a block of the round key using bitwise xor. 3. Rounds 1. SubBytes” a non-linear substitution step where each byte is replaced with another according to a lookup table. 2. ShiftRows” a transposition step where each row ot the state is shitted cyclically a certain number ot steps. 3. MixColumns” a mixing operation, which operates on the columns of the state, combining the four bytes in each column. 4. AddRoundKey .

Final Round (no MixColumns) 1. SubBytes 2. ShiftRows 3. AddRoundKey. (Biryukov) On systems with 32-bits, it is possible to speed up execution of this cipher by combining the SubBytes and ShiftRows steps with the MixColumns step by transforming them into a sequence of table lookups. This requires four 256-entry 32- bit tables, and utilizes a total of four kilobytes (4096 bytes) of memory ” one kilobyte for each table. A round can then be done with 16 table lookups and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations in the

AddRoundKey step. (3) If the resulting four-kilobyte table size is too large for a given target platform, the table lookup operation can be performed with a single 256-entry 32-bit (i. e. 1 kilobyte) table by the use of circular rotates. Using a byte-oriented approach, it is possible to combine the SubBytes, ShiftRows, and MixColumns steps into a single round operation. (4) High speed and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware, from 8-bit smart cards to high-performance computers.