Difference between des and aes

Difference between des and aes

AES has a better encryption standard i. e. it is far more advanced when compared to Des. There are many reasons attributing to this, Firstly the encryption key of an DES standard is just 56 bitsthus having a maximum of 256 combinations, while that of AES is 128, 192 or 259 bits long, with eachof them containing 2128, 2192 and 2256 combinations , thus makes it a tough nut to crack. Secondly, the block size used by DES is just 64 bits long , resulting in the maximum amount of information that can be transmitted with just a single encryption keyof just 32 GB , and beyond this it amounts in in partial leaking, as the information is not encrypted. This doesn’t happened with AES since with a block size of 128 bits, and with a single encryption key a data of 256 billion gigabytes can be transmitted , making it much more safety than the former. Finally, before going through the encryption steps DES uses the Feistel network which divides the block into two halves. AES on the other hand, uses permutation-substitution, which involves a series of substitution and permutation steps to create the encrypted block, thus making it difficult to break the code. [web]

Differences between Asymmetric and symmetric encryption tech

The strength of the encryption lies with the encryption algorithm and key length used by the encryption. To encrypt the data an encryption algorithm is used by both symmetric and asymmetric, a 128-bit key encryption algorithm when implemented has the same strength against being cracked whether it’s used in symmetric or asymmetric encryption program. Hence both symmetric and asymmetric encryption can be compared to the same safe, and so far no one has randomly cracked a 128 bit key length

encryption algorithm, unless the algorithm itself was flawed. Thus, the basic difference lies not in the encryption but the decryption. i. ethe one which cannot be decrypted would be the secure type of safe.

Generally keys can be broken in three ways

1. Simply guessing the password or key.
2. Through interception – Getting the keyby accessing the communication between the sender and recipient or gaining access their computer.
3. Brute Force – until a correct match is made all the random keys are tried using computing power.

Symmetric encryption can be vulnerable to all three methods, reason being the same password that is used to encrypt the data is also used decrypt the data. Asymmetric encryption is only vulnerable to the third method and the second half of the second method. Because the same key is not used to encrypt and decrypt the data but a combination of public and private keys to encrypt and decrypt the information, thus eradicating the need to communicate the password to the other person.

This doesn’t mean that asymmetric encryption is much more efficient when compared to symmetric. It also suffers from certain drawbacks. The biggest drawback being that, it is complicated to use. Certain prerequisites have to be met before using this technique.

1. One needs to make sure that there is appropriate decrypting software at the receiving end.
2. The public key has to be registered on one of the databases that maintain the keys.

For example, if A wants to send B some encrypted information he must first check whether B has the appropriate decrypting software and has registered his public key on one of the databases that maintains these keys or have B send him his public key. If he does already have everything, then great, the process itself is fairly simple as long as A already has the appropriate software for encrypting. If B doesn't have a public key already, or the appropriate software for decrypting, then he must go through this process of installing and registering before the encrypted message can be sent which makes it a time-consuming process.

This is the main reason why people are not using asymmetric encryption in today's fast-paced world.

Difference between Stream cipher and Block cipher

Both Stream cipher and Block Cipher are symmetric ciphers. WhileStream ciphers en one bit or byte at a time by generating an infinite cryptographic key-stream, block ci the other hand work on larger chunks of data at a time, and are often involved in co these blocks for additional security (e. g. AES in CBC mode). And it is this basic prop which makes the stream cipher faster than the latter.

Stream ciphers are generally implemented in scenarios such as embedded devices, firmware, and esp. hardware as they work on only a few bits at a time, consuming v memory requirements, and therefore making it cheaper. On the other hand memory consumed by the block ciphers are more, due to the fact that they work on larger ch data and often have " carry over" from previous blocks, which doesn't make it feasib work in the embedded environments where memory and speed plays a major role. A from this block ciphers are it more susceptible to noise in transmission as they encry whole block at a time. Whereas with stream ciphers are bytes are individually encryp

no connection to other chunks of data (in most ciphers/modes), and often have supp
interruptions on the line, thus making it is less susceptible to noise.

Despite these advantages stream ciphers do suffer from certain drawbacks. Stream
do not provide integrity protection or authentication, whereas some block ciphers (d
on mode) can provide integrity protection, in addition to confidentiality. This is beca
any given instant large blocks of data get processed, thus ensuring that the block of
obtained at the receiving end is free from all the errors. Data loss or a data mismatc
occur in stream ciphers since they work on a bit by bit basis. And apart from this cip
more difficult to implement correctly, and prone to weaknesses based on usage – sir
principles are similar to one-time pad, the key-stream has very strict requirements.
other hand block ciphers are comparatively easier to handle.

Because of all the above mentioned features, stream ciphers are usually best suited
cases where the amount of data is either unknown, or continuous – such as network
and other hardware devices . Block ciphers are more useful when the amount of dat
known – such as a file, data fields, or request/response protocols, such as HTTP whe
length of the total message is known already at the beginning.