Symmetric Key Encryption

It only requires a single key for both encryption and decryption.
The size of cipher text is same or smaller than the original plain text.
The encryption process is very fast.
It is used when a large amount of data is required to transfer.

It only provides confidentiality.

Examples: 3DES, AES, DES and RC4

In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.

Asymmetric Key Encryption

It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or larger than the original plain text.
The encryption process is slow.
It is used to transfer small amount of data.
It provides confidentiality, authenticity and non-repudiation.
Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA
In asymmetric key encryption, resource utilization is high.

AES

AES stands for Advanced Encryption Standard

The date of creation is 1999.

Key length can be 128-bits, 192-bits, and 256-bits.

Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)
The structure is based on a substitution-permutation network.
The design rational for AES is open.
The selection process for this is secret but accepted open public comment.

AES is more secure than the DES cipher and is the de facto world standard.

The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition

AES can encrypt 128 bits of plaintext.

AES cipher is derived from square cipher.

AES was designed by Vincent Rijmen and Joan Daemen.
No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible.
Biclique attack have better complexity than brute-force but still ineffective.

DES

DES stands for Data Encryption Standard
The date of creation is 1976.
The keyThe number length is 56 bits in DES.
DES involves 16 rounds of identical operations
The structure is based on a feistal network.
The design rational for DES is closed.

The selection process for this is secret.

DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation
DES can encrypt 64 bits of plaintext.
DES cipher is derived from Lucifer cipher.

DES was designed by IBM.

Known attacks against DES include : Brute-force, Linear crypt-analysis and Differential crypt-analysis.