Looking from an overall perspective, we can conclude the blowfish algorithm is more secure than DES, and produces best results for less processing time and rounds. To increase the key size of the blowfish algorithm from 128 to 448, it gives more privacy to the messages and provides high end data security when transmitting over any unsafe medium.

COMPARISON OF BLOWFISH & DES ALGORITHMS
(Both of these algorithms are Symmetric Block Cipher algorithms)

Algorithm	Key size	Block size	Round	Structure	Flexible	Speed of algorithm	Features
DES	64 bits	64 bits	16	Feistel	No	Slow	Not structure, Enough
Blowfish	32-448 bits	64 bits	16	Feistel	Yes	Fast	Excellent Security

==========

Security Development Lifecycle (SDL), developed by Microsoft to answer the issues faced by them during various development projects and hence, mostly caters to the need of their development methodology only. The lifecycle of Microsoft SDL includes Training, Requirements, Design, Implementation, Verification, Release, Response while Owasp has a similar lineup with Requirements & Analysis, Design, Implementation, Testing & Verification, Maintenance in the life cycle model.

CLASP is Comprehensive, Lightweight Application Security Process — is an activity driven, role-based set of process components whose core contains formalized best practices for building security into your existing or new-start software development lifecycles in a structured, repeatable, and measurable way.

CLASP is the outgrowth of years of extensive field work in which system resources of many development lifecycles were methodically decomposed in order to create a comprehensive set of security requirements. These resulting requirements form the basis of CLASP's best practices which allow organizations to systematically address vulnerabilities that, if exploited, can result in the failure of basic security services e.g. confidentiality, authentication, and access control.

CLASP process is composed of
1)CLASP Views
2)CLASP Resources

CLASP Views

These views are broken down into activities which in turn broken into components to provide a brief understanding of the CLASP process.

Activities defined under it explain how they can be easily embedded into software development lifecycle. Views contains following perspectives:

1)Concept view
2)Role-Based view
3)Activity –Assessment view
4)Activity –Implementation view
5)**VulnerabilityView**

CLASP Resources

CLASP provides list of resources which are being required to put in focus while planning implementing and performing activities

Following is the abstracted list of resources which are further categories into organization specific architecture and processes.

Basic principles of application security
Descriptions of core security principles
System assessment worksheet
Network resources
System resources
File system and registry
Sample road maps

	Applicability	Nature	Code Integrity	Suitability
Microsoft SDL	Only SDLC	Heavy	No	Large Organization
OWASP CLASP	Any software development process	Light Weight	Yes	Small and large sized organization

	Nature of Activities	Assessments	Separate Privacy requirement	Application Testing and

			evaluation	assessment
Microsoft SDL	Constructive	SDL can only identify risk assessment. Cannot able to identify vulnerability assessment	Yes	Extensively
OWASP CLASP	Constructive	CLASP can identify vulnerability assessment	No	Through threat modelling, Code Level Review, Security Tests, but No Verification of security attributes of resources