

Question Number 2**Block Ciphers**

Search for five Feistel five SPN block ciphers with following details

- Name
- Block-length
- Supported Key-sizes
- Any other additional info (in one line only)

Solution.**Block Ciphers**

Below are two tables that provide details about five Feistel and five SPN block ciphers, including their block length, supported key sizes, and additional information.

Feistel Block Ciphers

Name	Block-length	Supported Key-sizes	Additional Info
DES	64 bits	56 bits	16-round Feistel structure
Blowfish	64 bits	32 to 448 bits	Key-dependent S-boxes
Camellia	128 bits	128, 192, 256 bits	Used in both software and hardware implementations
CAST-128	64 bits	40 to 128 bits	Uses eight S-boxes; 12 or 16 rounds depending on key size
TEA	64 bits	128 bits	Simple structure, susceptible to certain attacks

SPN Block Ciphers

Name	Block-length	Supported Key-sizes	Additional Info
AES	128 bits	128, 192, 256 bits	Widely used; operates in 10, 12, or 14 rounds
Rijndael	128, 192, 256 bits	128, 192, 256 bits	AES finalist; supports variable block sizes
ANUBIS	128 bits	128 to 320 bits	Designed by Vincent Rijmen, co-designer of AES
PRESENT	64 bits	80 or 128 bits	Lightweight blockcipher for constrained environments
Noekeon	128 bits	128 bits	Simple structure, efficient in both hardware and software