

BitSpeed™ Velocity Encryption implements two algorithms to encrypt data while in-flight during transmission. Each algorithm provides enhanced data security without the normally crippling overhead associated with encryption functions, and each algorithm is seamlessly integrated with BitSpeed's compression and MD5 checksum features.



### BitSpeed™ Velocity ASC (Advanced Symmetric Cipher)

ASC performs at up to 3 gigabytes per second with extremely low CPU utilization.

BitSpeed's proprietary key generation system enables Velocity to change encryption keys every 64-bits (8 bytes), with sufficient keys generated on each initiation of a Velocity transfer to encrypt approximately 500 PB (Petabytes) of data.

BitSpeed's Advanced Symmetric Cipher (ASC) technology supports key lengths of 128-, 192-, 256-, and 512-bits.

### Standard AES

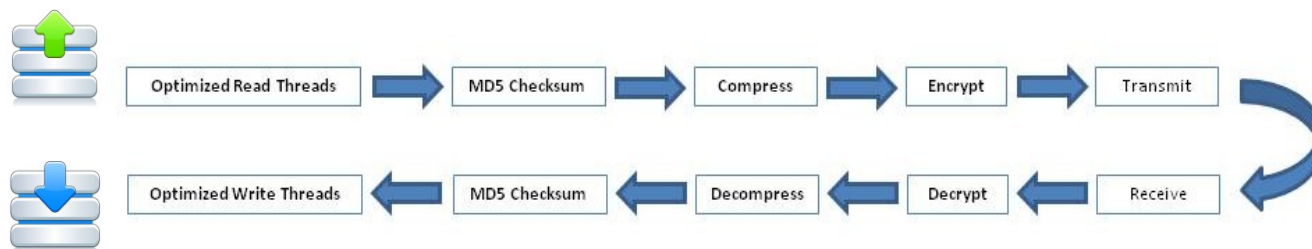
BitSpeed's implementation is a highly optimized version of the worldwide standard AES encryption, which performs at up to 200 megabytes per second available for use with both 128- and 256-bit keys, with very low CPU utilization.

### Summary

BitSpeed Velocity encryption offers world-class security of in-flight data while never impacting the performance of file transfers below the maximum available bandwidth limits.

Key generation is completely automated and requires no additional software, databases, or user interactivity.

Below is a diagram of the data transfer path of Velocity with encryption enabled:



Contact us at:

**BitSpeed LLC**  
1601 N. Sepulveda Blvd.  
Manhattan Beach, CA 90266 USA  
Phone +1 562.735.0660  
[www.bitspeed.com](http://www.bitspeed.com), [info@bitspeed.com](mailto:info@bitspeed.com)