AES شامل سه رمز بلوک است: AES-128 ، AES-192 و AES-256.

AES-128 برای رمزگذاری و رمزگشایی یک پیام از طول کلید 128 بیتی استفاده می کند ، در حالی که AES-192 از طول کلید 192 بیتی و AES-256 از طول کلید 256 بیتی برای رمزگذاری و رمزگشایی پیام ها استفاده می کند. هر رمزگذار با استفاده از کلیدهای رمزنگاری به ترتیب 128 ، 192 و 256 بیت ، داده ها را در بلوک های 128 بیتی رمزگذاری و رمزگشایی می کند.

متقارن ، که به آن کلید مخفی نیز گفته می شود ، رمزها از همان کلید برای رمزگذاری و رمزگشایی استفاده می کنند ، بنابراین فرستنده و گیرنده باید هر دو کلید مخفی را بشناسند و از آن استفاده کنند. دولت اطلاعات را در سه دسته محرمانه ، مخفی یا فوق سری طبقه بندی می کند. از تمام طول کلیدها می توان برای محافظت از سطح محرمانه و محرمانه استفاده کرد. اطلاعات فوق سری به طول کلیدهای 192 یا 256 بیتی نیاز دارد.

برای کلیدهای 128 بیتی 10 دور ، برای کلیدهای 192 بیتی 12 دور و برای کلیدهای 256 بیتی 14 دور وجود دارد. یک دور شاملچندین مرحله پردازش است که شامل جایگزینی ، جابجایی و مخلوط کردن متن ساده ورودی برای تبدیل آن به خروجی نهایی متن رمز است