الگوریتم رمزنگاری AES

الگوریتم AES بر اساس شبکه جانشینی جایگشت طراحی شده است و هم به صورت نرم‌افزاری و هم به صورت سخت‌افزاری کاراست. این الگوریتم بر روی آرایه‌های 4\*4 بایتی با ترتیب ستونی به نام حالت و یا state عمل می‌کند. اندازه‌ی کلید الگوریتم تعداد دورهایی را که طی آن ورودی را به خروجی رمز شده تبدیل می‌شود مشخص می‌کند. تعداد دفعات برای کلید 128 بیت 10 دور، کلید 192 بیتی 12 دور و کلید 256 بیتی 14 دور است.

الگوریتم AES چهار مرحله کلی بسط کلید، چرخه‌ی اولیه، چرخه‌ها و مرحله‌ی نهایی است. در مرحله اول کلیدهای چرخه با استفاده از زمان‌بندی کلید AES به دست می‌آید. در مرحله‌ی بعد با کمک یک XOR بیتی بایت هر حالت با بایت کلید دور ترکیب می‌شود. مرحله سوم خود 4 بخش دارد و بسته به نوع الگوریتم (128، 192 و یا 256 بیتی) 9، 11 و یا 13 بار تکرار خواهد شد. بخش اول این مرحله SubBytes است که در آن بر اساس یک جدول جستجو بایت‌ها به صورت غیر خطی جابه‌جا می‌شوند. شکل زیر این بخش را نشان می‌دهد.

گام SubBytes در الگوریتم AESبخش بعد در مرحله‌ی چرخه‎ها ShiftRows است که در آن حداقل سه سطح از حالت به تعداد گام‌های معینی شیفت پیدا می‌کند.

بخش سوم مرحله‌ی چرخه‌ها بخش MixColumns خواهد بود. در این بخش 4 بایت از هر ستون حالت با یک انتقال خطی ترکیب می‌شوند. این تابع چهار بایت به عنوان ورودی دریافت کرده و 4 بایت خروجی تولید می‌کند. این بخش به همراه بخش قبل پخش شدن رمزنگاری را فراهم می‌کند.

بخش آخر مرحله‌ی سوم گام AddRoundKey است. در این بخش زیر کلید با حالت ترکیب می‌شود. برای هر دور، یک زیرکلید از کلید اصلی با کمک زمان‌بندی کلید ریندال ایجاد شده و هر زیرکلید هم اندازه‌ی حالت خواهد بود. زیرکلید با ترکیب هر بایت از حالت با بایت متناظرش در زیرکلید به کمک xor بیتی جمع می‌شود. شکل زیر این گام را نشان می‌دهد

در مرحله‌ی نهایی، گام‎های SubBytes، ShiftRows و addRoundKey یک دور دیگر اجرا شده و تعداد کل دورهای اجرای الگوریتم را به 10، 12 و یا 14 دور می‌رسانند.