AES الگریتم

ساختار بدین صورت است که یک جعبه شامل چندین ماژول وجود دارد. متن اصلی و کلید رمزنگاری با طول رشته های ثابت به صورت بلوک بلوک وارد این جعبه می شوند و پس از گذراندن یک رشته عملیات به صورت رمز شده از جعبه خارج می شوند. در نهایت تمام بلوک ها پس از خروج از جعبه کنار یکدیگر قرار داده شده و متن رمز شده تولید می شود.

حال چه اتفاقی درون این جعبه می افتد؟ در زیر به بررسی این فرآیند می پردازیم.

طول رشته برای متن اصلی 128 بیت و برای کلید نیز 128 بیت است. طول کلید ورودی این ساختار متفاوت است که این بستگی به حالت الگوریتم AES دارد. الگوریتم مذکور در 3 ساختار تولید شده است و حداقل طول رشته برای کلید این الگوریتم 128 بیت است. در مرحله اول یک عملیات XOR وجود دارد. پس از این مرحله 10 مرحله دیگر وجود دارد و در نهایت متن رمز شده تولید می شود. اما وضعیت کلید در این ساختار به چه صورت است؟ کلید در همان آغاز وارد چرخه شده و برای تک تک مراحل موجود توسط ماژول تولید Sub Key اقدام به تولید کلید های جدید می کند. پس از اولین مرحله عملیات XOR متن وارد 10مرحله عملیات به شرح زیر می شود:  
در هر مرحله 4 عملیات انجام می شود. مرحله اول Substitution یا جایگزینی است. در مرحله دوم عملیات Transposition یا جابجایی انجام می شود. در مرحله سوم باز عملیات Substitution و در نهایت عملیات XOR روی 128 بیت رشته انجام می پذیرد. مشخص است که Sub Key تولید شده برای هر مرحله در مرحله چهارم وارد چرخه می شود. شرح هر مرحله :

* 128 بیت به ترکیبی 8 تایی از بایت تبدیل می شود. یعنی 8 رشته 16 بایتی و هر بایت با یک بایت متفاوت دیگر جایگزین می شود و این اطلاعات درون یک جدول ثبت می شود. احتمال جایگزینی در این حالت 2 به توان 8 می باشد. یعنی 256 حالت ممکن برای این جایگزینی ها وجود دارد. یعنی ترکیبات متفاوتی از 0 و 1 ها برای این ساختار.
* جابجایی بیت ها می باشد. براساس یک ساختار مشخص بیت ها با یکدیگر جابجا می شوند.
* در این مرحله از جایگزینی عملیات به صورت 4 بایت 4 بایت انجام می پذیرد. در نتیجه 2 به توان 32 حالت ممکن به وجود می آید. منطقی نیست که برای این تعداد حالت یک جدول تهیه شود، به همین دلیل یک فرمول جایگزین جدول در این مرحله می شود. این فرمول بنا به دلایل امنیتی مشخص نیست.
* یک عملیات XOR با کلید وارد شده در ساختار

