



درس طراحی کامپیوتری سیستم‌های دیجیتال

گزارش شماره‌ی: شش

اعضای گروه: سید احسان سجادی ، کیان جلیلیان

چکیده:

در این پروژه الگوریتم رمز نگاری TinyEncryptionAlgorithm (TEA) در زبان VHDL پیاده سازی شده است.

## فهرست مطالب

### 1- توضیح کد

### 2- نتیجه و جمع بندی

### 1- توضیح کد

پورت ها شامل کلاک، ورودی، کلید و مقدار خروجی رمزنگاری شده میباشند.

در این الگوریتم مقدار ثابت  $\Delta$  را مقدار دهی کرده و سایز ورودی را برابر 32 قرار میدهیم.

سپس در یک حلقه While ، به تعداد 31 بار هر بار مقدار فعلی  $\Delta$  را با مقدار  $\Delta$

جمع کرده و در sum قرار میدهد. و متغیرهای  $y, z$  که دربردارنده دو بخش ورودی ما هستند را به علاوه مساوی حاصل xor ترکیبی از ورودی و کلید قرار میدهد. در نهایت مقادیر  $y, z$  به دست آمده را در مقدار value میریزد.

در کد vhdl ابتدا کلید 32 بیتی را در 4 متغیر 4 بیتی  $k1, k2, k3, k4$  میریزیم. همچنین متغیرهای  $y, y1, y2, y3, yt, z$  و مقدار دهی کرده و متغیرهای  $z1, z2, z3, zt$  را تعریف کرده و طبق الگوریتم مقدار آنها را تعیین میکنیم. مقادیر  $yt, zt$  را با حاصل xor متغیرهای  $y1, y2, y3$  و  $z1, z2, z3$  میباشند. مقدار رمزنگاری شده را از چسباندن  $z, y$  در خروجی (encrypt) میریزیم.

## 2- نتیجه و جمع بندی

در این تمرین الگوریتم tea را در زبان vhdl پیاده سازی کردیم و خروجی را با تست بنچ در مدل سیم تست کردیم که نتایج آن در زیر قابل مشاهده است.

