



DES Encryption/Decryption Cipher Modules ¹	Resources		Performance	
	Slices	BRAMs	Spartan 3 (-4)	Virtex 4 (-10)
DES/3DES Standard	~305	0	~500Mbps DES ~170Mbps 3DES	~910Mbps DES ~310Mbps 3DES
DES/3DES Fast	~460	0	~680Mbps DES ~245Mbps 3DES	~1180Mbps DES ~425Mbps 3DES
DES/3DES FastPlus	~675	0	~1,000Mbps DES ~335Mbps 3DES	~1,500Mbps DES ~500Mbps 3DES

¹ DES cipher cores are configurable to support any desired block cipher mode (i.e. ECB, CBC, OFB, CFB, CTR, CBC-MAC)

AES Encryption/Decryption Cipher Modules ^{1,2}	Resources		Performance	
	Slices	BRAMs	Spartan 3 (-4)	Virtex 4 (-10)
AES Tiny En/Decryptor 128	~180	2	~25Mbps	~39Mbps
AES Tiny En/Decryptor 128/192/256	~190	2	~25Mbps	~38Mbps
AES Standard Encryptor 128 w/ offline roundkey	~100	3	~350Mbps	~570Mbps
AES Standard Decryptor 128 w/ offline roundkey	~170	3	~230Mbps	~440Mbps
AES Standard Encryptor 128 w/ h/w roundkey	~250	3	~350Mbps	~570Mbps
AES Standard Decryptor 128 w/ h/w roundkey	~320	3	~230Mbps	~440Mbps
AES Standard En/Decryptor 128 w/ h/w roundkey	~425	6	~230Mbps	~440Mbps
AES Fast Encryptor 128 w/ h/w roundkey	~450	10	~1,300Mbps	~2,200Mbps
AES Fast Decryptor 128 w/ h/w roundkey	~750	10	~1,100Mbps	~2,000Mbps
AES Fast En/Decryptor 128 w/ h/w roundkey	~1020	18	~1,100Mbps	~2,000Mbps
AES Fast Encryptor 256 w/ h/w roundkey	~580	10	~990Mbps	~1600Mbps
AES Fast Decryptor 256 w/ h/w roundkey	~890	10	~850Mbps	~1450Mbps
AES Fast En/Decryptor 256 w/ h/w roundkey	~1150	18	~850Mbps	~1450Mbps
AES GIGA Encryptor 128 w/ h/w roundkey	Available through consulting services, commercial cores under development			
AES GIGA Decryptor 128 w/ h/w roundkey	Available through consulting services, commercial cores under development			
AES GIGA Encryptor/Decryptor 128 w/ h/w roundkey	Available through consulting services, commercial cores under development			
AES GIGA Encryptor 256 w/ h/w roundkey	Available through consulting services, commercial cores under development			
AES GIGA Decryptor 256 w/ h/w roundkey	Available through consulting services, commercial cores under development			
AES GIGA En/Decryptor 256 w/ h/w roundkey	Available through consulting services, commercial cores under development			

¹ AES cipher cores are configurable to support any desired block cipher mode (i.e. CBC, OFB, CFB, CTR)

² All AES cores can be configured to support 128, 192, and/or 256 bit keys