

## Re: RSA vs AES

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-08/2342.html>

---

**From:** LVB (*LvB\_at\_sdc.net*)

**Date:** 08/29/03

Date: Fri, 29 Aug 2003 14:52:17 GMT

On Fri, 29 Aug 2003 06:06:45 -0700, Waldyr wrote:

> *Hello !*

>

> *We know that symmetric algorithms are faster than assymmetric ones,*  
> *for the same level of security. I'm interested to know if there is any*  
> *reference where this difference is measured, I mean, about \*how many*  
> *times\* AES-128, for example, is faster than RSA-1024, for the same*  
> *plataform and the same volume of data.*

I have some data for IA64. For the same amount of data (about 128 bytes, which is the most you can do in one go with RSA-1024) AES-128 does it in little more than 8 CPU cycles per byte, whereas a 1024-bit RSA private key operation can do no better than 1980 CPU cycles per bytes. Most RSA implementations are far less efficient than this though.