www.wolfssl.com
info@wolfssl.com
phone: +1 425 245 8247

wolfSSL Resource Use

1. RSA Cipher Suites

Math Library	Key Size	Peak Stack Use	Peak RAM (Heap) Use
fast	1024	10k	9k
fast	2048	13k	11k
normal	1024	6k	14k
normal	2048	7k	17k

The above table shows peak stack and heap usage. A description of how these change with different math libraries is described below.

The WOLFSSL object is 1k.

Handshake resources require an additional 8k of dynamic memory, only during the handshake. After the handshake, this memory is freed.

The WOLFSSL object and handshake memory total 9kB, as described above. Depending on key size, RSA takes another 5-8k heap space when using normal math or another 4-6k stack space when using fastmath.

This assumes zero sized input/output buffers that use dynamic memory only when needed. Each buffer can use an additional 17k if using the full SSL record size. If both sides of the SSL connection are under the user's control, the maximum SSL record size can be modified by altering MAX_RECORD_SIZE in ./src/internal.c. Alternatively, if supported on the server side, the application can use the TLS Maximum Fragment Length Extension to request the connection use a smaller maximum record size.

2. ECC Cipher Suites

Math Library	**Key Size**	**Peak Stack Use**	**Peak RAM (Heap) Use**
fast	256	7k	12k
normal	256	6k	15k

The fastmath library only needs an additional 1k of stack when using ECC (as compared to using the normal math library with ECC) because the max bits can be lowered to 512 (256*256) instead of 4096 or 2048 for RSA. Using fastmath with ECC also saves 3k of dynamic memory versus using normal math with ECC.

3. Testing Notes:

The memory usage numbers noted in this document were gathered using a 32-bit instruction set. When using fastmath with 1024-bit keys, FP_MAX_BITS was defined as 2048 (by default, it is set to 4096, to allow for 2048-bit keys).

On desktop systems, stack usage can be higher due to functions such as printf() and gmtime() using a higher amount of stack space than an embedded system would use.