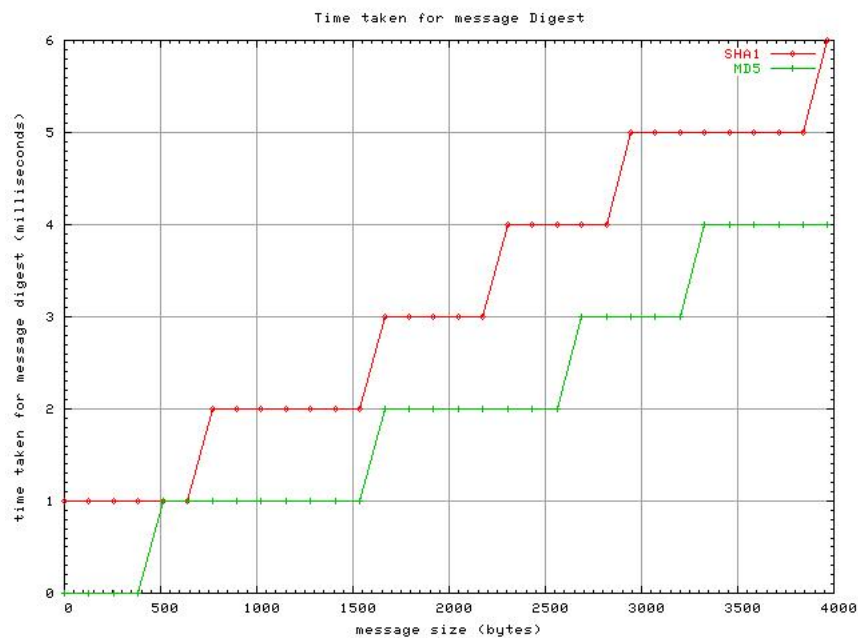


Estimation of time for message digest and signature algorithms

Shweta Agrawal

September 2, 2003

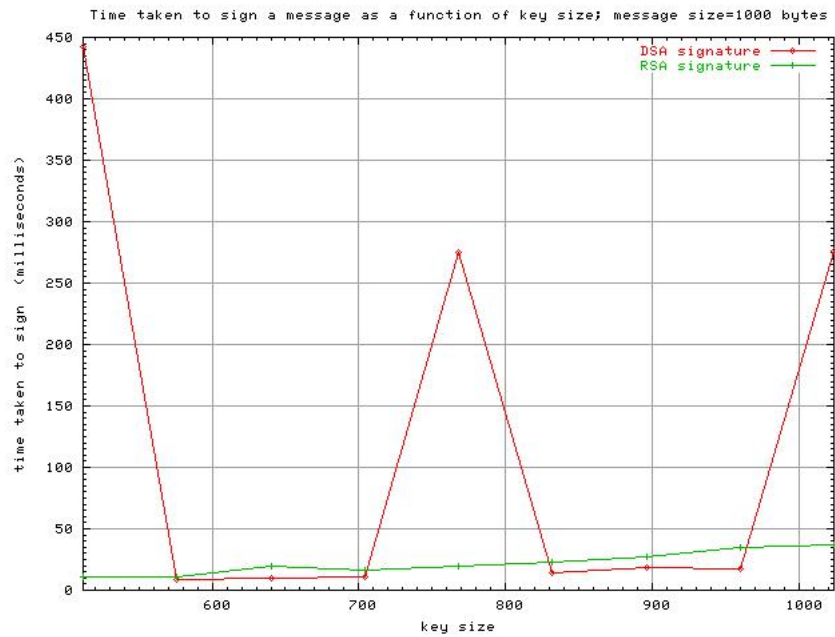
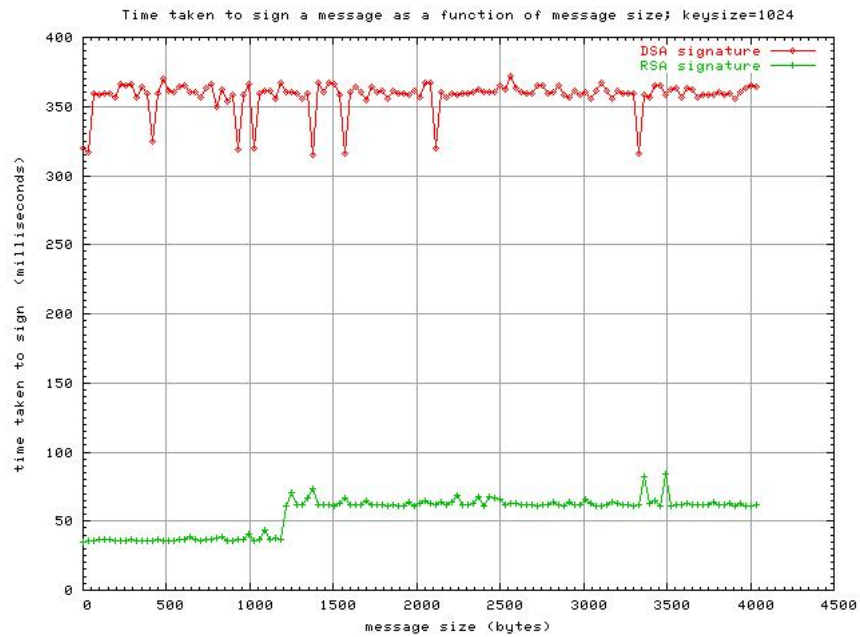
- 1 Estimate the time taken for the message digest as a function of message size (message size varying from 0 to 4K) and the algorithm.



Analysis The message digest algorithms, MD5 and SHA1 takes as input a message of arbitrary length ($max2^{32}$ in case of MD5) and produce an output of fixed length. The input is processed in 512-bit blocks. That is why we can see a rise in the time taken for calculating digest as the message size increases by 512 bytes. An increase in 512 bytes results in increase in number of blocks and hence the time to calculate digest.

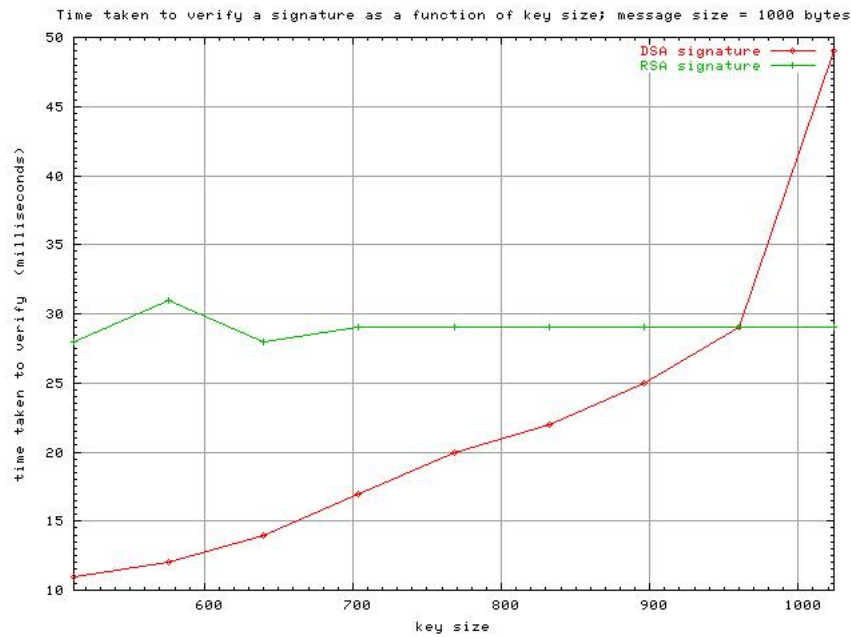
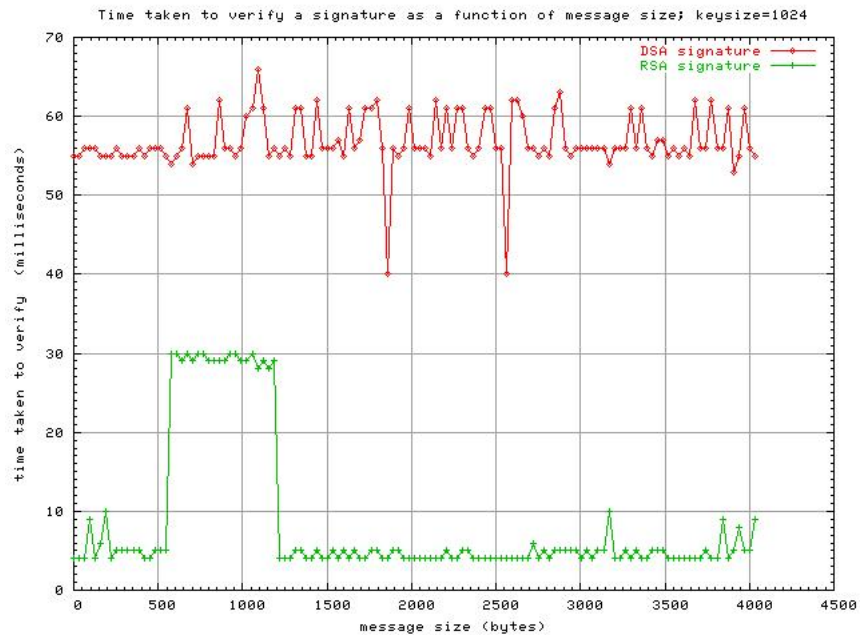
Secondly, SHA1 involves more steps (80) as compared to MD5(64). Also SHA1 produces 160-bit message digest, and hence has to process a 160-bit buffer as compared to MD5's 128-bit buffer. Thus SHA1 executes slowly, and takes more time than MD5 for the same message size.

2 Estimate the time taken for generating the signatures as a function of message size, key-size and algorithm.



Analysis RSA algorithm takes more time for signing than DSA normally, except for the cases when keysize is 512, 768, 1024. For these keysizes, DSA takes more time as compared to RSA, as can be seen in time vs. message size graph plotted for keysize = 1024.

3 Estimate the time taken for verifying the signatures as a function of message size, keysize and algorithm.



Analysis RSA takes less time to verify as compared to DSA.