Assignment 2, part 2 by Staffan Lundstrom, roll no 03005201

1. Calculation of Message Digest

Algorithm: MD5

Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Time (millisec):	201	220	230	229	231

Algorithm: SHA-1

Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Time (millisec):	200	221	220	220	221

2. Generation of signatures

Algorithm: DSA (with SHA-1)

Key size: 512

Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Generation time (ms):	0	10	10	5	10

Key size: 1024

Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Generation time (ms):	10	10	20	10	20

Algorithm: RSA (with SHA-1)

Key size: 512

Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Generation time (ms):	160	160	170	171	170

Key size: 1024

Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Generation time (ms):	180	190	191	190	190

3. Verification of signatures

Algorithm: DSA (with SHA-1)

Key size:	512				
Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Verification time (ms):	220	221	220	211	221
Key size:	1024				
Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Verification time (ms):	230	241	240	231	231

Algorithm: RSA (with SHA-1)

Key size:	512				
Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Verification time (ms):	241	250	251	250	240
Key size:	1024				
Message size:	*0K*	*1K*	*2K*	*3K*	*4K*
Verification time (ms):	230	240	241	220	250

In DSA generation of signatures should take longer time than verification.
For RSA it's the opposite. One should be careful when comparing these data for generation and verification because of disturbing factors as different amounts of reading from file etc. Please look in the java files in order to see exactly how the timings have been done.