Cryptology (course 1DT075)
Uppsala University – Spring 2013
Report for part 1 of lab 2

Simon YOUNG Li MI Hans KOBERG

May 7, 2013

A Reflection

B Statistics

encrypt()						
p	q	e	d	L	*Text Length*	*Time(ns)*
16	8	175	4015087	1	23	70853000
16	8	173	11645861	2	23	10009000
16	8	229	5763117	3	23	24401000
39	31	179	$5.5298620 * 10^{20}$	1	23	12858000
62	54	251	$2.6628073 * 10^{34}$	2	23	19046000
85	77	227	$6.3118817 * 10^{48}$	3	23	15151000
131	123	227	$1.0273761 * 10^{76}$	1	23	23883000
177	169	229	$7.0571036 * 10^{104}$	2	23	130990000
223	215	139	$7.5669375 * 10^{131}$	3	23	202935000
16	8	145	3832657	1	53	8761000
16	8	253	8173417	2	53	17784000
16	8	253	9651517	3	53	9131000
39	31	191	$8.6802261 * 10^{20}$	1	53	9412000
62	54	149	$3.3223155 * 10^{34}$	2	53	15075000
85	77	131	$3.5485491 * 10^{48}$	3	53	7788000
131	123	153	$3.5322089 * 10^{76}$	1	53	39715000
177	169	215	$5.6082680 * 10^{104}$	2	53	40994000
223	215	227	$4.9663907 * 10^{131}$	3	53	224722000
16	8	211	17601391	1	86	17933000
16	8	211	17101891	2	86	8636000
16	8	241	11501401	3	86	27810000
39	31	217	$3.7576331 * 10^{20}$	1	86	20844000
62	54	251	$4.1917540 * 10^{34}$	2	86	29359000
85	77	251	$2.8594169 * 10^{48}$	3	86	12591000
131	123	251	$9.8765183 * 10^{76}$	1	86	29287000
177	169	221	$7.2295576 * 10^{104}$	2	86	22908000
223	215	215	$5.1382213 * 10^{131}$	3	86	95712000

Table 1: *Benchmark* for the encrypt function

decrypt()						
p	q	e	d	L	*Text Length*	*Time(ns)*
16	8	175	4015087	1	23	643000
16	8	173	11645861	2	23	134000
16	8	229	5763117	3	23	181000
39	31	179	$5.5298620 * 10^{20}$	1	23	753000
62	54	251	$2.6628073 * 10^{31}$	2	23	145000
85	77	227	$6.3118817 * 10^{48}$	3	23	178000
131	123	227	$1.0273761 * 10^{76}$	1	23	369000
177	169	229	$7.0571036 * 10^{104}$	2	23	138000
223	215	139	$7.5669375 * 10^{131}$	3	23	124000
16	8	145	3832657	1	53	402000
16	8	253	8173417	2	53	224000
16	8	253	9651517	3	53	148000
39	31	191	$8.6802261 * 10^{20}$	1	53	346000
62	54	149	$3.3223155 * 10^{31}$	2	53	153000
85	77	131	$3.5485491 * 10^{48}$	3	53	115000
131	123	153	$3.5322089 * 10^{76}$	1	53	313000
177	169	215	$5.6082680 * 10^{104}$	2	53	267000
223	215	227	$4.9663907 * 10^{131}$	3	53	321000
16	8	211	17601391	1	86	561000
16	8	211	17101891	2	86	285000
16	8	241	11501401	3	86	191000
39	31	217	$3.7576331 * 10^{20}$	1	86	752000
62	54	251	$4.1917540 * 10^{31}$	2	86	312000
85	77	251	$2.8594169 * 10^{48}$	3	86	426000
131	123	251	$9.8765183 * 10^{76}$	1	86	694000
177	169	221	$7.2295576 * 10^{104}$	2	86	430000
223	215	215	$5.1382213 * 10^{131}$	3	86	391000

Table 2: *Benchmark* for the decrypt function

generateKey()						
p	q	e	d	L	*Text Length*	*Time(ns)*
16	8	175	4015087	1	23	1323000
16	8	173	11645861	2	23	315000
16	8	229	5763117	3	23	273000
39	31	179	$5.5298620 * 10^{20}$	1	23	4624000
62	54	251	$2.6628073 * 10^{31}$	2	23	1986000
85	77	227	$6.3118817 * 10^{48}$	3	23	3570000
131	123	227	$1.0273761 * 10^{76}$	1	23	19929000
177	169	229	$7.0571036 * 10^{104}$	2	23	9599000
223	215	139	$7.5669375 * 10^{131}$	3	23	12260000
16	8	145	3832657	1	53	1087000
16	8	253	8173417	2	53	682000
16	8	253	9651517	3	53	366000
39	31	191	$8.6802261 * 10^{20}$	1	53	2947000
62	54	149	$3.3223155 * 10^{31}$	2	53	2643000
85	77	131	$3.5485491 * 10^{48}$	3	53	3361000
131	123	153	$3.5322089 * 10^{76}$	1	53	24107000
177	169	215	$5.6082680 * 10^{104}$	2	53	20832000
223	215	227	$4.9663907 * 10^{131}$	3	53	30100000
16	8	211	17601391	1	86	1548000
16	8	211	17101891	2	86	914000
16	8	241	11501401	3	86	564000
39	31	217	$3.7576331 * 10^{20}$	1	86	7150000
62	54	251	$4.1917540 * 10^{31}$	2	86	4862000
85	77	251	$2.8594169 * 10^{48}$	3	86	6422000
131	123	251	$9.8765183 * 10^{76}$	1	86	38114000
177	169	221	$7.2295576 * 10^{104}$	2	86	35639000
223	215	215	$5.1382213 * 10^{131}$	3	86	39416000

Table 3: *Benchmark* for the generateKey function