

# 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

### A.1 What happens if a non-prime number incorrectly passes this test during key generation?

If a non-prime number does not pass the primality test, it will be impossible to compute  $e$

### A.2 What would you do when the number of characters to encode is not a multiple of $L$ ?

What we do in our implementation is that we add zeroes (padding) to match  $L$ .

## B Statistics

**Encryption** The time for encryption is clearly affected by how big  $p$  and  $q$  are. The bigger  $p$  and  $q$  are the longer the run-time. *See the encrypt table below*

**Key Generation** We can observe from the table that it takes longer time to generate keys when the key length is 1. We do not know why this is the case. *See the generateKey table below*

**Decryption** From the tables below we can see that for the decrypt function, the longer the key length is the faster it runs. It is easy to see that this is true since it will decrypt more characters at a time, resulting in lesser iterations. *See the decrypt table below*

**Comments on the Statistics** These statistics are not optimal, they do not take into account every case. For example,  $e$  follows  $p$  and  $1$  almost linearly, but it does not take into account when  $p$  and  $q$  are large and  $e$  is small.

encrypt()						
$p$	$q$	$e(bits)$	$d(bits)$	$L$	Text Length	Time(ns)
16	16	26	32	1	23	30566000
16	16	26	31	2	23	26747000
16	16	26	32	3	23	17955000
16	16	26	32	1	23	13987000
16	16	26	31	2	23	44996000
16	16	26	31	3	23	26312000

26	26	44	52	1	23	66164000
26	26	44	51	2	23	84238000
26	26	44	52	3	23	40261000
26	26	44	52	1	23	24422000
26	26	44	52	2	23	49685000
26	26	44	52	3	23	30400000
46	46	62	91	1	23	113200000
46	46	62	92	2	23	80341000
46	46	62	92	3	23	62935000
46	46	62	92	1	23	44744000
46	46	62	92	2	23	43145000
46	46	62	91	3	23	42438000
76	76	80	152	1	23	64651000
76	76	80	150	2	23	63791000
76	76	80	151	3	23	64180000
76	76	80	151	1	23	87176000
76	76	80	152	2	23	168059000
76	76	80	152	3	23	78443000
116	116	98	231	1	23	108000000
116	116	98	232	2	23	181432000
116	116	98	232	3	23	190937000
116	116	98	231	1	23	191400000
116	116	98	231	2	23	89770000
116	116	98	230	3	23	96739000
166	166	116	332	1	23	126413000
166	166	116	332	2	23	385820000
166	166	116	331	3	23	109575000
166	166	116	330	1	23	440746000
166	166	116	332	2	23	399075000
166	166	116	331	3	23	122254000
226	226	134	451	1	23	268837000
226	226	134	450	2	23	184366000
226	226	134	452	3	23	210620000
226	226	134	451	1	23	433959000
226	226	134	452	2	23	417309000
226	226	134	452	3	23	242626000
16	16	26	32	1	53	9096000
16	16	26	32	2	53	9128000
16	16	26	32	3	53	9143000
16	16	26	31	1	53	9314000
16	16	26	32	2	53	10301000
16	16	26	30	3	53	18497000
26	26	44	53	1	53	23994000
26	26	44	51	2	53	23828000
26	26	44	51	3	53	48587000
26	26	44	51	1	53	29346000
26	26	44	52	2	53	32268000
26	26	44	52	3	53	28848000
46	46	62	92	1	53	43191000

46	46	62	93	2	53	155413000
46	46	62	91	3	53	87433000
46	46	62	90	1	53	43262000
46	46	62	91	2	53	45150000
46	46	62	91	3	53	44552000
76	76	80	152	1	53	79232000
76	76	80	152	2	53	135914000
76	76	80	150	3	53	63533000
76	76	80	151	1	53	66499000
76	76	80	152	2	53	68944000
76	76	80	152	3	53	145041000
116	116	98	232	1	53	211234000
116	116	98	232	2	53	90313000
116	116	98	231	3	53	190040000
116	116	98	232	1	53	94542000
116	116	98	231	2	53	91585000
116	116	98	232	3	53	379343000
166	166	116	331	1	53	152035000
166	166	116	332	2	53	120064000
166	166	116	331	3	53	141597000
166	166	116	331	1	53	309268000
166	166	116	332	2	53	133441000
166	166	116	331	3	53	328064000
226	226	134	452	1	53	256991000
226	226	134	451	2	53	574725000
226	226	134	452	3	53	259265000
226	226	134	452	1	53	586771000
226	226	134	452	2	53	165634000
226	226	134	452	3	53	163248000
16	16	26	32	1	86	10335000
16	16	26	31	2	86	20433000
16	16	26	31	3	86	10389000
16	16	26	31	1	86	10073000
16	16	26	32	2	86	10766000
16	16	26	32	3	86	9043000
26	26	44	51	1	86	25218000
26	26	44	53	2	86	73870000
26	26	44	51	3	86	48311000
26	26	44	51	1	86	48199000
26	26	44	51	2	86	24959000
26	26	44	52	3	86	48636000
46	46	62	91	1	86	135411000
46	46	62	91	2	86	44097000
46	46	62	92	3	86	139266000
46	46	62	92	1	86	43500000
46	46	62	92	2	86	43734000
46	46	62	92	3	86	43784000
76	76	80	152	1	86	135924000
76	76	80	152	2	86	131926000

76	76	80	153	3	86	73949000
76	76	80	151	1	86	291442000
76	76	80	152	2	86	68806000
76	76	80	151	3	86	69616000
116	116	98	230	1	86	104726000
116	116	98	232	2	86	98733000
116	116	98	230	3	86	196339000
116	116	98	232	1	86	100743000
116	116	98	231	2	86	86078000
116	116	98	233	3	86	99520000
166	166	116	331	1	86	134719000
166	166	116	332	2	86	194134000
166	166	116	331	3	86	120860000
166	166	116	330	1	86	166063000
166	166	116	332	2	86	540384000
166	166	116	331	3	86	150014000
226	226	134	451	1	86	637881000
226	226	134	451	2	86	146389000
226	226	134	451	3	86	465523000
226	226	134	451	1	86	265923000
226	226	134	451	2	86	163422000
226	226	134	451	3	86	188284000

decrypt()						
$p$	$q$	$e(bits)$	$d(bits)$	$L$	$Text\ Length$	$Time(ns)$
16	16	26	32	1	23	840000
16	16	26	31	2	23	280000
16	16	26	32	3	23	179000
16	16	26	32	1	23	340000
16	16	26	31	2	23	249000
16	16	26	31	3	23	76000
26	26	44	52	1	23	1526000
26	26	44	51	2	23	644000
26	26	44	52	3	23	212000
26	26	44	52	1	23	737000
26	26	44	52	2	23	308000
26	26	44	52	3	23	213000
46	46	62	91	1	23	1803000
46	46	62	92	2	23	873000
46	46	62	92	3	23	338000
46	46	62	92	1	23	1008000
46	46	62	92	2	23	473000
46	46	62	91	3	23	317000
76	76	80	152	1	23	1802000
76	76	80	150	2	23	866000
76	76	80	151	3	23	593000
76	76	80	151	1	23	2692000
76	76	80	152	2	23	976000
76	76	80	152	3	23	645000

116	116	98	231	1	23	3783000
116	116	98	232	2	23	1698000
116	116	98	232	3	23	1100000
116	116	98	231	1	23	3405000
116	116	98	231	2	23	1614000
116	116	98	230	3	23	1068000
166	166	116	332	1	23	6197000
166	166	116	332	2	23	2869000
166	166	116	331	3	23	1704000
166	166	116	330	1	23	6525000
166	166	116	332	2	23	3075000
166	166	116	331	3	23	2014000
226	226	134	451	1	23	9948000
226	226	134	450	2	23	4751000
226	226	134	452	3	23	3536000
226	226	134	451	1	23	10942000
226	226	134	452	2	23	5616000
226	226	134	452	3	23	3344000
16	16	26	32	1	53	423000
16	16	26	32	2	53	197000
16	16	26	32	3	53	154000
16	16	26	31	1	53	402000
16	16	26	32	2	53	206000
16	16	26	30	3	53	134000
26	26	44	53	1	53	1341000
26	26	44	51	2	53	665000
26	26	44	51	3	53	438000
26	26	44	51	1	53	2103000
26	26	44	52	2	53	1173000
26	26	44	52	3	53	448000
46	46	62	92	1	53	2165000
46	46	62	93	2	53	1090000
46	46	62	91	3	53	782000
46	46	62	90	1	53	2230000
46	46	62	91	2	53	1188000
46	46	62	91	3	53	734000
76	76	80	152	1	53	5199000
76	76	80	152	2	53	2177000
76	76	80	150	3	53	1410000
76	76	80	151	1	53	4213000
76	76	80	152	2	53	2057000
76	76	80	152	3	53	1990000
116	116	98	232	1	53	7803000
116	116	98	232	2	53	4251000
116	116	98	231	3	53	2528000
116	116	98	232	1	53	7963000
116	116	98	231	2	53	3731000
116	116	98	232	3	53	2568000
166	166	116	331	1	53	14501000

166	166	116	332	2	53	7050000
166	166	116	331	3	53	4497000
166	166	116	331	1	53	14718000
166	166	116	332	2	53	7070000
166	166	116	331	3	53	7936000
226	226	134	452	1	53	27658000
226	226	134	451	2	53	14583000
226	226	134	452	3	53	7870000
226	226	134	452	1	53	24451000
226	226	134	452	2	53	11982000
226	226	134	452	3	53	7906000
16	16	26	32	1	86	1666000
16	16	26	31	2	86	461000
16	16	26	31	3	86	218000
16	16	26	31	1	86	677000
16	16	26	32	2	86	385000
16	16	26	32	3	86	236000
26	26	44	51	1	86	2205000
26	26	44	53	2	86	1110000
26	26	44	51	3	86	865000
26	26	44	51	1	86	2061000
26	26	44	51	2	86	1045000
26	26	44	52	3	86	738000
46	46	62	91	1	86	3895000
46	46	62	91	2	86	1820000
46	46	62	92	3	86	1334000
46	46	62	92	1	86	3745000
46	46	62	92	2	86	1894000
46	46	62	92	3	86	1222000
76	76	80	152	1	86	7150000
76	76	80	152	2	86	3551000
76	76	80	153	3	86	2218000
76	76	80	151	1	86	6639000
76	76	80	152	2	86	3622000
76	76	80	151	3	86	2438000
116	116	98	230	1	86	13080000
116	116	98	232	2	86	7145000
116	116	98	230	3	86	4331000
116	116	98	232	1	86	14201000
116	116	98	231	2	86	6329000
116	116	98	233	3	86	4146000
166	166	116	331	1	86	25230000
166	166	116	332	2	86	11497000
166	166	116	331	3	86	7712000
166	166	116	330	1	86	21766000
166	166	116	332	2	86	11018000
166	166	116	331	3	86	7481000
226	226	134	451	1	86	37573000
226	226	134	451	2	86	19137000

226	226	134	451	3	86	13309000
226	226	134	451	1	86	43840000
226	226	134	451	2	86	19809000
226	226	134	451	3	86	13489000

generateKey()						
$p$	$q$	$e(bits)$	$d(bits)$	$L$	$Text\ Length$	$Time(ns)$
16	16	26	32	1	23	1225000
16	16	26	31	2	23	490000
16	16	26	32	3	23	220000
16	16	26	32	1	23	624000
16	16	26	31	2	23	359000
16	16	26	31	3	23	154000
26	26	44	52	1	23	1883000
26	26	44	51	2	23	882000
26	26	44	52	3	23	310000
26	26	44	52	1	23	992000
26	26	44	52	2	23	748000
26	26	44	52	3	23	394000
46	46	62	91	1	23	3791000
46	46	62	92	2	23	1371000
46	46	62	92	3	23	843000
46	46	62	92	1	23	1905000
46	46	62	92	2	23	950000
46	46	62	91	3	23	621000
76	76	80	152	1	23	3845000
76	76	80	150	2	23	2084000
76	76	80	151	3	23	1222000
76	76	80	151	1	23	5549000
76	76	80	152	2	23	2045000
76	76	80	152	3	23	1335000
116	116	98	231	1	23	9885000
116	116	98	232	2	23	4498000
116	116	98	232	3	23	2849000
116	116	98	231	1	23	9688000
116	116	98	231	2	23	4709000
116	116	98	230	3	23	3189000
166	166	116	332	1	23	22208000
166	166	116	332	2	23	9133000
166	166	116	331	3	23	5992000
166	166	116	330	1	23	19336000
166	166	116	332	2	23	9159000
166	166	116	331	3	23	6318000
226	226	134	451	1	23	37514000
226	226	134	450	2	23	19450000
226	226	134	452	3	23	13161000
226	226	134	451	1	23	48881000
226	226	134	452	2	23	19580000
226	226	134	452	3	23	18718000

16	16	26	32	1	53	564000
16	16	26	32	2	53	280000
16	16	26	32	3	53	183000
16	16	26	31	1	53	578000
16	16	26	32	2	53	281000
16	16	26	30	3	53	187000
26	26	44	53	1	53	1655000
26	26	44	51	2	53	867000
26	26	44	51	3	53	549000
26	26	44	51	1	53	2093000
26	26	44	52	2	53	1332000
26	26	44	52	3	53	595000
46	46	62	92	1	53	3452000
46	46	62	93	2	53	1809000
46	46	62	91	3	53	1281000
46	46	62	90	1	53	3774000
46	46	62	91	2	53	2199000
46	46	62	91	3	53	1317000
76	76	80	152	1	53	8925000
76	76	80	152	2	53	4228000
76	76	80	150	3	53	2962000
76	76	80	151	1	53	8624000
76	76	80	152	2	53	4341000
76	76	80	152	3	53	3243000
116	116	98	232	1	53	21660000
116	116	98	232	2	53	10581000
116	116	98	231	3	53	6700000
116	116	98	232	1	53	21085000
116	116	98	231	2	53	10259000
116	116	98	232	3	53	7017000
166	166	116	331	1	53	45365000
166	166	116	332	2	53	21884000
166	166	116	331	3	53	14813000
166	166	116	331	1	53	43636000
166	166	116	332	2	53	22540000
166	166	116	331	3	53	19414000
226	226	134	452	1	53	95089000
226	226	134	451	2	53	59388000
226	226	134	452	3	53	28871000
226	226	134	452	1	53	91809000
226	226	134	452	2	53	48347000
226	226	134	452	3	53	29955000
16	16	26	32	1	86	815000
16	16	26	31	2	86	564000
16	16	26	31	3	86	305000
16	16	26	31	1	86	1126000
16	16	26	32	2	86	470000
16	16	26	32	3	86	286000
26	26	44	51	1	86	2728000



26	26	44	53	2	86	1345000
26	26	44	51	3	86	965000
26	26	44	51	1	86	2690000
26	26	44	51	2	86	1449000
26	26	44	52	3	86	936000
46	46	62	91	1	86	7753000
46	46	62	91	2	86	3085000
46	46	62	92	3	86	1919000
46	46	62	92	1	86	6097000
46	46	62	92	2	86	3187000
46	46	62	92	3	86	2124000
76	76	80	152	1	86	14951000
76	76	80	152	2	86	9654000
76	76	80	153	3	86	8355000
76	76	80	151	1	86	13584000
76	76	80	152	2	86	7484000
76	76	80	151	3	86	5391000
116	116	98	230	1	86	33168000
116	116	98	232	2	86	16886000
116	116	98	230	3	86	11038000
116	116	98	232	1	86	35991000
116	116	98	231	2	86	17257000
116	116	98	233	3	86	11467000
166	166	116	331	1	86	71211000
166	166	116	332	2	86	41007000
166	166	116	331	3	86	23660000
166	166	116	330	1	86	70215000
166	166	116	332	2	86	34861000
166	166	116	331	3	86	22704000
226	226	134	451	1	86	153625000
226	226	134	451	2	86	74205000
226	226	134	451	3	86	53393000
226	226	134	451	1	86	152752000
226	226	134	451	2	86	73950000
226	226	134	451	3	86	53442000