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

Simon YOUNG Li MI Hans KOBERG

May 16, 2013

Part I
Statistics

In this part, we present the runtimes of the diffrent ciphertexts as well as the resulting plaintext. We also investigate how big r must be to get anything of value. We break the ciphertext three times, each time with a different r. We chose r to be in the intervall $L * 8 - 3 \leq r \geq L * 8$.

A Group 1

Plaintext for L = 1 We call a a witness for the compositeness of n (sometimes mislead

Plaintext for L = 2

Group 1		
r	L	*Time(s)*
6	1	1.0
7	1	1.0
8	1	3.0
14	2	120.0
15	2	240.0
16	2	480.0

Table 1: Statistics for Group 1 cryptotext

Group 2		
r	L	*Time(s)*
6	1	13.0
7	1	26.0
8	1	52.0
14	2	1489.0
15	2	2989.0
16	2	5953.0

Table 2: Statistics for group 2 cryptotext

Group 3		
r	L	*Time(s)*
6	1	10.0
7	1	20.0
8	1	41.0
14	2	520.0
15	2	1046.0
16	2	2100.0

Table 3: Statistics for group 3 cryptotext

Group 4		
r	L	*Time(s)*
6	1	0.0
7	1	0.0
8	1	0.0
14	2	32.0
15	2	65.0
16	2	130.0

Table 4: Statistics for group 4 cryptotext

Group 6		
r	L	*Time(s)*
6	1	7.0
7	1	15.0
8	1	31.0
14	2	844.0
15	2	1687.0
16	2	3388.0

Table 5: Statistics for group 6 cryptotext

Group 8		
r	L	*Time(s)*
6	1	1.0
7	1	2.0
8	1	4.0
14	2	168.0
15	2	338.0
16	2	676.0

Table 6: Statistics for group 8 cryptotext

Group 9		
r	L	*Time(s)*
6	1	0.0
7	1	0.0
8	1	0.0
14	2	18.0
15	2	37.0
16	2	75.0

Table 7: Statistics for group 9 cryptotext

B Group 2

C Group 3

D Group 4

E Group 6

F Group 8

G Group 9

Part II
Reflection

H Describe what you think is missing in your implementation of the RSA algorithm (of part 1) to make it a usable product one can rely on. In particular, what are the potential sources of insecurity?

I Explain how and why the attack you implemented works. Explain also why it works even if you don't know what is the language/structure of the plain text.

J The attack you have used is only possible for small L. A usual way to attack RSA is to try to factor n into its two prime factors. Look at the public key files of the submitted ciphers. Are there some that you think are insecure (because too small) from this point of view? Specify what you consider