Memorial University of Newfoundland **Fall Semester 2018**
Yorck Sommerhäuser **MATH 3370: Sheet 9**

Introductory Number Theory

Problem: You have intercepted a message to a person with public key (e, n), where

$$e = 3199957 \qquad \text{and} \qquad n = 3832716017551$$

The message consists of six blocks:

0182002821959

3092737753574

3397137880489

2339619796630

2916903963593

1986692232044

You know that each block corresponds to a number that encodes four characters of the standard keyboard according to the tables

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

p	q	r	s	t	u	v	w	x	y	z	A	B	C	D
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45

T	U	V	W	X	Y	Z	‘	1	2	3	4	5	6	7
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

8	9	0	−	=	∼	!	@	#	$	%	ˆ	&	*	(
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75

)	-	+		,	.	/	<	>	?	;	’	:	”	[
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

]	{	}	|											
91	92	93	94											

which follow in principle the method described in Paragraph 7.2 on page 87 and page 88 of the course notes. Note that the blank has number 79 and the period has number 81. Using computer algebra, decrypt the message by breaking the code. (100 points)

Due date: Monday, November 19, 2018. Submit the decrypted message and a qualitative description how you broke the code. You do not have to write down all numbers explicitly. Normally, your solution should fit on one or two handwritten pages.