TECHNISCHE UNIVERSITEIT EINDHOVEN
Department of Mathematics and Computer Science

Examination Cryptographic Algorithms (2WC00), Friday, November 21, 2003, 9.00 – 12.00.

All answers should be clearly argued, using a step-by step argumentation resp. description (for algorithms).
You are not allowed to use a computer or calculator.
A Vigenère table and the grading points are given at the end.
This exam consists of five problems.

Distribution of points for the problems: 50 in total, 10 per problem.

---

1. Alice is using the Vigenère cryptosystem (see table at the end). To generate a key she flips a fair coin. If head comes up she picks at random the name of one of the four cities where she has lived, while if tail comes up she selects at random the first name of one her eight friends. Eve knows this key generation process and the names of these cities and friends as well.

   (a) Encrypt the plaintext "thanks"with the key "rome".

   (b) What is the uncertainty of Eve about the key?

   (c) What is the unicity distance of this system, when you may assume that the redundancy of the text is 3.2 bits per letter?

   (d) Demonstrate the notion of unicity distance by using as few letters as possible to choose between key "hank" and "boris" when "sepdbrr" is the intercepted ciphertext.

2. Consider a feedback shift register of length n with feedback polynomial $f(x_0, x_1, \ldots, x_{n-1})$, so $x_{k+n} = f(x_k, x_{k+1}, \ldots, x_{k+n-1})$ for all $k \geq 0$. Show that each state of the register has a unique predecessor if and only $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + g(x_1, x_2, \ldots, x_{n-1})$ for some function $g(x_1, x_2, \ldots, x_{n-1})$.

3. Let m be the solution of $2^m \equiv 17 \pmod{37}$. What is the multiplicative order of 2 modulo 37? Determine the value of m modulo 9 by means of the Pohlig-Hellman method. Do this as efficiently as possible.

4. Demonstrate the Pollard-ρ method for factoring numbers on $n = 91$. You may but do not have to use Floyd's cycle-finding algorithm.

5. How many points lie on the elliptic curve $y^2 = x^3 + 6x + 3$ over Z_{11}? Check that the points $(4, 5)$ and $(5, 9)$ lie on the curve. What is their sum?

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y