<u>TECHNISCHE UNIVERSITEIT EINDHOVEN</u>
Department of Mathematics and Computer Science

Examination Cryptographic Algorithms (2WC00 & 2F590),
Friday, November 19, 2004, 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.

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

---

1. The Hill cipher (1929) operates on pairs of letters from $\{a, b, \ldots, z\}$, which are in the standard way identified with the elements from the set $Z_{26} = \{0, 1, \ldots, 25\}$. The Hill cipher maps the pair of plaintext letters (p_1, p_2) to the ciphertext pair (c_1, c_2) by means of:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \equiv K \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \pmod{26}, \qquad \text{with key } K = \begin{pmatrix} k_{1,1} & k_{1,2} \\ k_{2,1} & k_{2,2} \end{pmatrix},$$

where the $k_{i,j}$ are also in Z_{26}.

(a) What is a necessary and sufficient condition *Cond* on K to make this into a cryptosystem?

(b) Assuming that *Cond* holds, how does one perform a decryption?

(c) Let $K = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. Show that *Cond* holds and check that $\begin{pmatrix} 25 & 2 \\ 1 & 25 \end{pmatrix}$ can be used for decryption.

(d) Suppose that you have intercepted the ciphertext"pqcfku" and know that it originated from the plaintext "friday". Determine the key K. (Tip: start with the first two pairs of letters.)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

2. Consider the binary sequence $\underline{s} = (s_0, s_1, \ldots, s_{n-1})$ of length n and let L be its linear complexity. Show that L is minimal with respect to the property that $(s_L, s_{L+1}, \ldots, s_{n-1})^T$ is in the linear span of the columns of

$$\begin{pmatrix} s_0 & s_1, & \cdots & \cdots & s_{L-1} \\ s_1 & s_2, & \cdots & \cdots & s_L \\ \vdots & & & & \vdots \\ s_{n-L-1} & s_{n-L}, & \cdots & \cdots & s_{n-2} \end{pmatrix}.$$

Show that the linear equivalence (complexity) of $(0, 0, 1, 1, 0, 1, 1, 1, 0)$ is 5 and give a LFSR of length 5 that can output this sequence.

3. Alice and Bob make use of the Diffie-Hellman key exchange algorithm to agree on 10 common bits. They work with binary polynomials modulo $1 + x^7 + x^{10}$. Bob makes public the bit-string 1010011000 which stands for the polynomial $1 + x^2 + x^5 + x^6$. The secret key of Alice is 2. On which secret will they agree?

4. Alice sends ciphertext $c = 40$ to Bob. The public parameters of Bob are $n = 437$ and $e = 233$. Find the factorization of n with "brute force", determine the decryption exponent of Bob and find the plaintext corresponding to message c.

5. Show that the points $P = (2, 9)$ and $Q = (11, 6)$ lie on the elliptic curve $\mathcal{E} : y^2 = x^3 + x + 3$ over Z_{17}. Determine the line l through P and Q and find the third point of intersection of l with $\mathcal{E}$. Determine $P + Q$ on $\mathcal{E}$.