TECHNISCHE UNIVERSITEIT EINDHOVEN
Department of Mathematics and Computer Science

Examination Cryptographic Algorithms (2WC00),
Tuesday, January 20, 2004, 14.00–17.00

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.
This exam consists of five problems.

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

---

1. Eve intercepts the following ciphertext

   "dcnolcbiwyypzpysrrobrsrqwejvpcdxcbw".

   She knows that is was made with the Vigenère cryptosystem. What is the most likely key length? (Hint: use Kasiski's method.)

2. Let $\{s_i\}_{i\geq 0}$ be a sequence generated by a linear feedback shift register with primitive characteristic polynomial $f(x)$ of degree n.

   (a) Prove that $f(x)$ has an odd number of coefficients equal to 1.

   (b) Show that a full period of the output sequence does contain a block of length n but not of length $n-1$.

   (c) Let $f(x) = x^7 + x + 1$ and let the output sequence start as follows $\{1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, \ldots\}$. Write $S(x) = \sum_{i\geq 0} s_i x^i$ as $u(x)/f^*(x)$, where f^* denotes the reciprocal of f.

3. Use the Pollard-ρ method to solve $3^m \equiv 2 \pmod{23}$. You may but do not have to use Floyd's cycle-finding algorithm.

4. Use $u = 3$ as strong witness to show that $m = 91$ is a composite number (the Miller-Rabin test).

5. How many points lie on the elliptic curve $y^2 = x^3 + x + 1$ over Z_{11}? Check that the point $P = (3, 8)$ lies on the curve. Determine $2P$.