TECHNISCHE UNIVERSITEIT EINDHOVEN
Department of Mathematics and Computer Science

Examination Cryptology I (2WC12),
OR
Cryptographic Algorithms (2WC00)
OR
Cryptology (2F590)

Thursday, March 22, 2007, 14.00–17.00

All answers should be clearly argued, using a step-by step argumentation.
You are not allowed to use a computer or calculator.
This exam consists of four problems.

---

1. Show that the linear equivalence (complexity) of the binary sequence $(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$ is at least 5. (The linear equivalence of a sequence is the length of the shortest LFSR that can output that sequence.)
   Assume that this sequence is generated by a linear feedback shift register of length 5 with characteristic polynomial $c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + x^5$. Which linear recurrence relation will express state $\underline{s}^{(n)}$ of the register as linear combination of the preceding five states.
   Give this recurrence relation explicitly for this example.

2. Somebody needs to solve $2^m \equiv c \pmod{16139}$ for many different values of c. (The number 16139 is a prime.) He wants every computation of such a discrete logarithm to take no more than 80 calculations. What is the complexity of the precalculation (rounded off to the nearest integer) and the storage requirement when he uses the Baby-step Giant-step method?
   Is this method faster or slower in this case than Pollard-ρ?

3. You are asked to explain and demonstrate Pollard's $p-1$ method for $n = 77$ (without making use of the fact that this number is so small). Assume that the smallest prime factor of n, say p, has the property that $p-1$ is smooth with respect to the $S = 3$. Which exponent R can

you calculate on the basis of n such that $a^R \equiv 1 \pmod{p}$ for all a that are not divisible by p.
Explain and demonstrate for this example how this R can help you to factor n.

4. Show that point $P = (6, 2)$ lies on the elliptic curve $\mathcal{E} : y^2 = x^3 + 2x^2 + 3x + 4$ over Z_{17}.
Determine the tangent l through P to this curve.
Find the point Q different from P that lies on l and $\mathcal{E}$.
Determine $2P$ on $\mathcal{E}$.

All questions count for 25 points.