TECHNISCHE UNIVERSITEIT EINDHOVEN
Department of Mathematics and Computer Science

Examination Cryptographic Algorithms (2WC00 & 2F590),
Friday, November 18, 2005, 12.00–17.00

All answers should be clearly argued, using a step-by step argumentation resp. description (for algorithms). In particular in Problems 3 and 4 you have to demonstrate your knowledge of general techniques; "direct" solutions that work because the parameters are small are not allowed. 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. A plaintext source generates independent, identically distributed letters from the alphabet $\{\alpha, \beta, \gamma, \delta\}$, where the distribution is given by $Pr(\alpha) = 1/2$, $Pr(\beta) = 1/4$, $Pr(\gamma) = Pr(\delta) = 1/8$.

   (a) What is the redundancy per symbol of a word over this alphabet of length n?

   (b) Suppose that this word is encrypted with the Caesar cipher under a randomly selected key (all four possibilities are equally likely). What is the uncertainty of the key given the first letter of the ciphertext?

   (c) What is the unicity distance of this cipher?

2. Consider the sequence $\{w_i\}_{i\geq 0} = \{s_i \oplus t_i\}_{i\geq 0}$, where $\{s_i\}_{i\geq 0}$ is generated by the LFSR with characteristic polynomial $1 + x + x^2$ and $\{t_i\}_{i\geq 0}$ is generated by the LFSR with characteristic polynomial $1 + x + x^3$.

   (a) What is the period of $\{s_i\}_{i\geq 0}$ and of $\{t_i\}_{i\geq 0}$?

   (b) What are the possible periods of the sequence $\{w_i\}_{i\geq 0}$ and why?

   (c) Consider a particular initial state $(s_0, s_1; t_0, t_1, t_2)$ and suppose that $\{w_i\}_{i\geq 0}$ has period 3. Prove that $t_0 = t_1 = t_2 = 0$. (Hint: consider $w_0, w_3, w_6, \ldots$.)

(d) Why does $(s_0, s_1; t_0, t_1, t_2) = (1, 0; 1, 0, 0)$ generate a sequence $\{w_i\}_{i\geq 0}$ of maximal length.

3. This problem is about the discrete logarithm problem.

   (a) Show that the multiplicative order of 2 modulo 37 is 36.

   (b) To solve $2^m \equiv 27 \pmod{37}$ show how the Pohlig-Hellman algorithm reduces this problem to two smaller problems.

   (c) Set up all preliminary work to solve $2^m \equiv c \pmod{37}$ in general.

   (d) Now solve $2^m \equiv 27 \pmod{37}$ in this way.

4. Of the "large" integer $n = 119$ it is known that its smallest prime factor p has the additional property that $p-1$ is smooth with respect to $\{2, 3\}$, so $p - 1 = 2^a 3^b,\ a, b \geq 0$. Demonstrate Pollard's $p - 1$ factorization method by means of the following questions.

   (a) Give an upperbound on a and on b. Call these bounds A resp. B.

   (b) Let $R = 2^A 3^B$ and let u be randomly selected from $\{1, 2, \ldots, p-1\}$. Prove that $u^R \equiv 1 \pmod{p}$.

   (c) Now select a random $u,\ 1 \leq u < n$. Prove that almost always $\gcd(u^R - 1, n) = p$.

   (d) When does this method fail?

   (e) Demonstrate this method with $u = 5$.

5. Let $p = 13$.

   (a) How many points lie on the elliptic curve $y^2 = x^3 + 2x + 1$ over Z_p?

   (b) Verify that $P = (8, 3)$ and $Q = (1, 2)$ lie on this curve.

   (c) Determine $P + Q$.