TECHNISCHE UNIVERSITEIT EINDHOVEN
Department of Mathematics and Computer Science

Examination Cryptographic Algorithms (2WC00 & 2F590),
Wednesday, January 18, 2006, 9.00–12.00

All answers should be clearly argued, using a step-by-step argumentation resp. description (for algorithms). In particular in Problems 2, 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. Consider a language with only the letters a, b, c and let these letters occur with respective probabilities $0.7, 0.2$, and 0.1. The ciphertext "a b c b a b b b a c" was made by using the Vigenère cryptosystem, where the letters a, b, c are identified with resp. $0, 1, 2$ and the addition is modulo 3.

   (a) Suppose that the key length is either $1, 2$ or 3. What is the most probable key length?

   (b) Determine the most probable key.

2. Consider the binary sequences $\{s_i\}_{i\geq 0}$, $\{t_i\}_{i\geq 0}$, and $\{u_i\}_{i\geq 0}$ generated by the LFSR's with resp. characteristic polynomial $1+x+x^2$, $1+x+x^3$, resp. $1+x+x^4$. Let $\{w_i\}_{i\geq 0}$ be defined by $w_i = s_i t_i \oplus u_i,\ i \geq 0$.

   (a) What are the possible periods of $\{s_i\}_{i\geq 0}$, $\{t_i\}_{i\geq 0}$, and $\{u_i\}_{i\geq 0}$?

   (b) Give an initial state $(s_0, s_1; t_0, t_1, t_2; u_0, u_1, u_2, u_3)$ of the three LFSR's that leads to an output sequence $\{w_i\}_{i\geq 0}$ of period 21.

   (c) Compute $(w_0, w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8)$ for the initial state

   $$(s_0, s_1; t_0, t_1, t_2; u_0, u_1, u_2, u_3) = (1, 0; 1, 0, 0; 1, 0, 0, 0).$$

   Show that the linear complexity of these 9 terms is 4.

3. Demonstrate the Baby-Step Giant-Step method in full detail to solve the discrete logarithm problem $2^m \equiv 18 \pmod{37}$ (assume that you can store only 6 numbers).

4. The RSA system is being used on a smartcard to sign documents. Its public parameters are $n = 55$ and $e = 17$.

   (a) Determine the secret exponent d.

   (b) The smart card makes use of the Chinese Remainder Theorem to sign documents. Show the precalculations to set this up.

   (c) Evaluate the signature c of the message $m = 9$ in this way.

   (d) Suppose that the smartcard makes a mistake in the calculation of c_p which is the value of c modulo $p = 5$ and produces $\hat{c}_p = 2$. What will the output $\hat{c}$ be?

   (e) How can one find the factorization of n from the values c and $\hat{c}$?

5. Let $p = 11$.

   (a) How many points lie on the elliptic curve $y^2 = x^3 + 3x + 4$ over Z_p?

   (b) Verify that $P = (4, 6)$ lies on the curve.

   (c) Determine $2P$.