TECHNISCHE UNIVERSITEIT EINDHOVEN
Department of Mathematics and Computer Science

Examination Cryptographic Algorithms (2WC00 & 2F590),
Tuesday, January 18, 2005, 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.

This exam consists of five problems, each worth 10 points.

---

1. Consider a language over an alphabet of just the three symbols $0, 1, 2$, occurring with probabilities $p_0 = 0.5, p_1 = 0.3$, and $p_2 = 0.2$. The ciphertext

   001000221012102020100211101000

   of length 30 is the result of a Vigenère encryption (the calculations are mod 3 now, of course). The Vigenère encryption consists of r Caesar ciphers.

   (a) If one compares the first u letters in the ciphertext with the last u letters what is the probability of seeing the same letter on the same place if r divides $30 - u$ and if r does not divide $30 - u$.

   (b) Use this method (called the "incidence of coincidences" method) to determine the most probable value of r. (Only test the values $u = 29, 28, 27$ and 26.)

   (c) What is the most likely key?

2. Consider an LFSR with feedback polynomial $f(x) = x^5 + x + 1$. Let $\{s_i\}_{i \geq 0}$ be the output sequence of this register, when the initial state is given by $(s_0, s_1, s_2, s_3, s_4) = (1, 1, 1, 0, 1)$.

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

   (b) What would the period of $\{s_i\}_{i \geq 0}$ have been if $f(x)$ had been irreducible?

   (c) Give a shorter LFSR that can generate the same sequence $\{s_i\}_{i \geq 0}$.

3. Bob uses the Rabin variant (so $e = 2$) of RSA with modulus $n = 25217$. Eve discovers by accident that the plaintext $m_1 = 5331$ leads to the ciphertext 2 and that the plaintext $m_2 = 6808$ leads to the ciphertext $18 = 2 \times 3^2$. Use this information to find that $n = 151 \times 167$.

4. We continue with Problem 3, so Bob knows that $n = 151 \times 167$. Suppose that Bob receives $m^2 \equiv c \equiv 19 \pmod{25217}$. Show why he can find $m_1 \equiv m \pmod{p}$ with the formula $m_1 \equiv c^{(p+1)/4} \pmod{p}$ (and similarly $m_2 \equiv m \pmod{q}$ with the formula $m_2 \equiv c^{(q+1)/4} \pmod{q}$). Suppose that Bob gets $m_p = 64$ and $m_q = 112$. Describe a method to find all solutions m. (You do not have to find these solutions.) How many solutions are there?

5. Use the Pohlig-Hellman method to solve $2^m \equiv 12 \pmod{19}$.