Final exam in

CRYPTOGRAPHY

December 18, 2001, 14–19

Inst. för Informationsteknologi
Lunds Tekniska Högskola
Dept. of Information Technology
Lund University

- You are allowed to use a calculator.
- Each solution should be written on a *separate sheet of paper*.
- You must *clearly* show the line of reasoning.
- If any data is lacking, make reasonable assumptions.

Good luck!

Problem 1

a) Find the shortest LFSR that generates the infinite sequence

$$\mathbf{s} = [1, 0, 2, 0]^{\infty},$$

where $\mathbf{s}$ is defined over $\mathbb{F}_3$.

b Find the shortest LFSR that generates the finite sequence

$$\mathbf{s} = (1, 0, \alpha, \alpha, \alpha)$$

where $\mathbf{s}$ is defined over $\mathbb{F}_9$ using the irreducible polynomial $p(x) = x^2 + x + 2$ and $p(\alpha) = 0$.

(10 points)

Problem 2

Consider the following system for secrecy and authenticity.

		plaintext BV	plaintext SV	
key	0	0	1	ciphertext
	1	2	3	
	2	4	0	
	3	1	2	
	4	3	4	

The keys are equiprobable and the two possible plaintexts "Buy Volvo" (BV) and "Sell Volvo" (SV) have probabilities $P(BV) = 0.89$ and $P(SV) = 0.11$, respectively.

a) Find the probability P_I of success in an impersonation attack.

b) Calculate Simmons' bound $P_I \geq 2^{-I(C;K)}$.

c) Calculate the improved bound $P_I \geq 2^{-\inf I(C;K)}$.

d) Find the probability P_S of success in a substitution attack.

e) What can be said about the secrecy of the system?

(10 points)

Problem 3

The Shamir (k, n)-threshold scheme is a way of distributing a secret key K among n participants such that any k participants can reconstruct K whereas any $k - 1$ or fewer participants get no information about K from their shares.

Shamir's scheme is usually described for $K \in \mathbb{F}_p$, but it work of course over any finite field.

Consider a Shamir $(2, n)$-threshold scheme defined over $\mathbb{F}_{2^8}$, where $p(x) = x^8 + x^6 + x^5 + x^2 + 1$, $p(\alpha) = 0$. The participants receive the public shares $x_i = \alpha^i$.

Assume that P_2 and P_3 want to recover the secret key K by joining their shares. Determine the value of K if the private share of P_2 is $y_2 = \alpha^5 + 1$ and the private share of P_3 is $y_3 = \alpha + 1$.

(10 points)

Problem 4

We wish to encrypt a memoryless source with alphabet $\mathbb{Z}_3$ and $P(M = 0) = 1/2$, $P(M = 1) = 1/4$, $P(M = 2) = 1/4$. Let the key $\mathbf{K} = (K_0, K_1, \ldots, K_{l-1})$ be chosen uniformly from the set of ternary l-tuples ($K_i \in \mathbb{Z}_3$). A sequence of message symbols $\mathbf{M} = (M_1, M_2, \ldots, M_n)$ is encrypted to a sequence of ciphertext symbols $\mathbf{C} = (C_1, C_2, \ldots, C_n)$ by

$$C_i = M_i + K_{i \bmod l} \pmod 3, \quad \forall i, 1 \leq i \leq n.$$

Consider the following statements:

a) When $l = 64$ the unicity distance N_0 ("entydighetslängden") is in the interval $700 < N_0 < 800$.

b) $H(\mathbf{K}|\mathbf{C}) = H(\mathbf{M}|\mathbf{C})$ when $l = n$.

c) When $l = n$ the system has perfect secrecy.

d) When l is fixed, it is possible to have perfect secrecy for any n if the source sequence is compressed to zero redundancy ($D = 0$) before encryption.

e) Let $l = 2$ and $n = 100000$. A ciphertext $\mathbf{C}$ contains 25041 zeros, 50129 ones, and 24830 occurrences of the symbol 2. The most probable key is $\mathbf{K} = (0, 1)$.

Choose for each of the five statements given above one of the following alternatives:

i) Correct — I am uncertain
ii) Wrong — I am uncertain
iii) Correct — I am certain
iv) Wrong — I am certain.

Correct answer according to i) or ii) gives 1 point.
Correct answer according to iii) or iv) gives 2 points.
Erroneous answer according to i) or ii) gives 0 points.
Erroneous answer according to iii) or iv) gives -2 points.

(Only answers are required!)

(10 points)

Problem 5

In an RSA-system the public encryption function is $C = M^e \bmod n$ and the secret decryption function is $M = C^d \bmod n$, where M is the plaintext and C is the ciphertext. Let the public parameters of the RSA-system be denoted by (n, e). It is popular to choose $e = 3$ if possible, since a small value of e gives a fast encryption.

Although RSA is considered to be a secure public-key cryptosystem, there are sometimes errors made when implementing RSA. Such errors can render the implemented RSA system completely insecure. We look at two such cases.

a) Assume that $M \in \mathbb{Z}_{2^{64}}$ is a 64 bit plaintext that is encrypted using a 512 bit RSA number n and the corresponding $e = 3$. Explain why this is completely insecure.

Demonstrate the above by finding the plaintext corresponding to $C = 4921675101$ when $n = 34968844844341$ and $e = 3$.

b) When generating the composite number $n = pq$, care must be taken. For a chosen prime p, let $p - 1$ factor as $p - 1 = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, where the p_i's are distinct primes. Show that if $p_i^{e_i} \leq B$ for $1 \leq i \leq m$, for some B, then n can usually be factored by calculating $\gcd((2^{B!} - 1) \bmod n, n)$. How hard is it to calculate $2^{B!} \bmod n$?

(10 points)