Skriftlig Eksamen
Kryptologi

Institut for Matematik og Datalogi
Syddansk Universitet - Odense Universitet

Tirsdag den 26. januar 1999, kl. 9–13

Alle sædvanlige hjælpemidler (lærebøger, notater, etc.) samt brug af lommeregner er tilladt.

Eksamenssættet består af 4 opgaver på 3 nummererede sider (1–3). Fuld besvarelse er besvarelse af alle 4 opgaver. Opgavernes vægt ved bedømmelsen er angivet i parenteser ved starten af hver opgave.

Der må gerne refereres til algoritmer og resultater fra lærebogen inklusive øvelsesopgaverne. Specielt må man gerne begrunde en påstand med at henvise til, at det umiddelbart følger fra et resultat i lærebogen (hvis dette altså er sandt!). Henvisninger til andre bøger (udover lærebogen) accepteres ikke som besvarelse af et spørgsmål.

Bemærk, at hvis der er et spørgsmål i en opgave, man ikke kan besvare, kan man godt besvare de efterfølgende spørgsmål og blot antage at man har en løsning til de foregående spørgsmål.

Problem 1 (10%)

Suppose that a keystream is produced by a linear feedback shift register with $m = 2s$ stages. Suppose the first $m + 2$ bits of the sequence are $(01)^{s+1}$, i.e. 01 repeated $s+1$ times. Is it possible for bit $m+3$ to be a 1? Explain your answer.

Problem 2 20%

Suppose a cryptosystem has $P = \{a, b, c\}$, $C = \{1, 2, 3, 4\}$ and $K = \{K_1, K_2, K_3\}$.

The encryption rules are as follows:

	a	b	c
K_1	1	2	3
K_2	4	3	2
K_3	3	4	1

Suppose $p_K(K_i) = 1/3$ for $1 \leq i \leq 3$, $p_P(a) = 1/2$, $p_P(b) = 1/3$, and $p_P(c) = 1/6$.

a. Compute the probabilities $p_C(y)$ for all $y \in \{1, 2, 3, 4\}$.

b. Does this cryptosystem achieve perfect secrecy? Explain your answer.

Problem 3 (30%)

Suppose that RSA is implemented using the public keys, $N = 221$ and $e = 77$.

a. While encrypting the plaintext 160, repeated squaring was used, and the following results were obtained:

$$\begin{array}{rlcr}
160^2 & \bmod 221 & = & 185 \\
160^4 & \bmod 221 & = & 191 \\
160^8 & \bmod 221 & = & 16 \\
160^{16} & \bmod 221 & = & 35 \\
160^{32} & \bmod 221 & = & 120 \\
160^{64} & \bmod 221 & = & 35 \\
160^{72} & \bmod 221 & = & 118 \\
160^{76} & \bmod 221 & = & 217 \\
160^{77} & \bmod 221 & = & 23
\end{array}$$

The intermediate results which were obtained give a cryptanalyst some very useful information for factoring the modulus. What was so interesting? (Hint: Look at the results of the different squarings.) Show how to use this information to factor 221.

b. What is the decryption exponent d?

Problem 4 (40%)

Let n be an integer with unknown factorization $n = pq$, where p and q are prime, and let $x_0, x_1 \in Z_n^*$ be such that at least one of x_0 and x_1 is a quadratic residue modulo n. Assume that both x_0 and x_1 have Jacobi symbol $+1$ modulo n. (Assume that it is x_b and $u^2 \equiv x_b \pmod{n}$). Suppose that x_0, x_1, and n are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated $\log_2 n$ times:

Prover		Verifier
Choose random $i \in \{0,1\}$ and random $v_b, v_{1-b} \in Z_n^*$. Compute $y_b = v_b^2 \pmod{n}$ and $y_{1-b} = v_{1-b}^2 (x_{1-b}^i)^{-1} \pmod{n}$.	$\xrightarrow{y_0, y_1}$	
		Choose a random $c \in \{1, 0\}$.
	$\xleftarrow{c}$	
Compute $z_b = u^{i \oplus c} v_b \pmod{n}$, $z_{1-b} = v_{1-b}$.	$\xrightarrow{z_0, z_1}$	
		Check that either ($z_0^2 \equiv y_0 \pmod{n}$ and $z_1^2 \equiv x_1^c y_1 \pmod{n}$) or ($z_0^2 \equiv x_0 y_0 \pmod{n}$ and $z_1^2 \equiv (x_1)^{1-c} y_1 \pmod{n}$). If not, reject and halt.

Note that $\oplus$ is addition modulo 2.

a. Prove that the above protocol is an interactive proof system showing that at least one of x_0 and x_1 is a quadratic residue modulo n.

b. Suppose that x_{1-b} is also a quadratic residue. What is the distribution of the values y_0, y_1, z_0, z_1 sent by a Prover following the protocol?

c. Suppose that x_{1-b} is a quadratic nonresidue. What is the distribution of the values y_0, y_1, z_0, z_1 sent by a Prover following the protocol?

d. Prove that the above protocol is perfect zero-knowledge (use definition 13.2 in the textbook).