Skriftlig Eksamen
Kryptologi

Institut for Matematik og Datalogi
Syddansk Universitet - Odense Universitet

Torsdag den 15. juni 2000, kl. 9–13

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

Eksamenssættet består af 4 opgaver på 4 nummererede sider (1–4). 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 (15%)

Suppose that a keystream S is produced by a linear feedback shift register with n stages (by a linear recurrence relation of degree n). Suppose the period is $2^n - 1$. Consider any positive integer i and the following pairs of positions in S: $(S_i, S_{i+1}), (S_{i+1}, S_{i+2}), ..., (S_{i+2^n-3}, S_{i+2^n-2})), (S_{i+2^n-2}, S_{i+2^n-1}))$. How many of these pairs are such that $(S_j, S_{j+1}) = (1, 1)$? (In other words, how many times within one period does the pattern 11 appear?)

Prove that your answer is correct.

Problem 2 20%

Throughout this problem, suppose it is known that $n = p \cdot q$, where p and q are distinct primes, though the factorization of n is unknown to the Verifier. Let $x, y \in Z_n^*$ both have Jacobi symbol $+1$.

a. Prove that $x \cdot y \pmod{n}$ is a quadratic residue modulo n if and only if either

1. x and y are both quadratic residues, or
2. x and y are both quadratic nonresidues.

b. Prove that $x^3 \cdot y^5 \pmod{n}$ is a quadratic residue modulo n if and only if either

1. x and y are both quadratic residues, or
2. x and y are both quadratic nonresidues.

c. Give a perfect zero-knowledge proof showing that x and y satisfy one of the following two conditions modulo n:

1. x and y are both quadratic residues, or
2. x and y are both quadratic nonresidues.

Problem 3 (15%)

a. In one of the homework problems this semester, you showed that using RSA in the following way was insecure: Use a large modulus n for which it is unlikely that anyone can factor n in a reasonable amount of time. Represent each alphabetic character (from English) as an integer between 0 and 25. Encrypt each character of a message separately using the number which represents it.

Suppose instead of using a large composite n and RSA, a large prime p and the El-Gamal public-key cryptosystem is used. Is this also insecure? Why or why not?

b. Are there any advantages or disadvantages of using El Gamal this way, other than those related to security that you discussed above?

Problem 4 (50%)

Let $p = 4k+3$ be a prime, and let g and h be quadratic residues modulo p. Assume that h is in the subgroup generated by g and that the Prover knows an x such that $g^x = h \pmod p$. Suppose that p, g, and h are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated $\log_2 p$ times:

Prover		Verifier
Choose a random $k \in \{1, ..., \frac{p-1}{2}\}$. Let $z = h \cdot g^{2k} \pmod p$.	$\xrightarrow{z}$	
		Choose a random $b \in \{0,1\}$.
	$\xleftarrow{b}$	
Let $r = 2k + b \cdot x \pmod{p-1}$.	$\xrightarrow{r}$	
		Check that r is even, $z = g^r h^{1-b} \pmod p$, $p \pmod 4 = 3$, and $g^{\frac{p-1}{2}} = 1 \pmod p$. If not, reject and halt.

(Actually, the last two checks only need to be done once and could be done before the first round of the protocol. Don't let their placement here confuse you.)

a. Prove that the above protocol is an interactive proof system showing that $h = g^{2y} \pmod p$ for some integer y.

b. Suppose that $h = g^{2y} \pmod p$ for some integer y. What is the probability distribution of the values (z, r) sent by a Prover following the protocol?

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

d. Suppose $p = 4k + 3$. Note that any quadratic residue g modulo p has odd order. Use this fact to show that if h is in the subgroup generated by a quadratic residue g, then it is always possible to write h as $h = g^{2y} \pmod p$ for some integer y. (Thus, the above protocol is an alternative zero-knowledge proof of subgroup membership for this special case.)

e. Suppose $p = 4k + 3$, $g \neq 1$ is a quadratic residue modulo p, and $q = \frac{p-1}{2} = 2k + 1$ is a prime. Then, there is a more efficient secure way, than using the above protocol, to convince the Verifier that $h = g^y \pmod p$ for some integer y. What is it? (Hint: no Prover is necessary.)