Skriftlig Eksamen
Kryptologi

Institut for Matematik og Datalogi
Syddansk Universitet - Odense Universitet

Mandag den 16. juni 2003, kl. 9–13

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

Eksamenssættet består af 5 opgaver på 5 nummererede sider (1–5). Fuld besvarelse er besvarelse af alle 5 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%)

a. 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 triples of positions in S:

$$(S_i, S_{i+1}, S_{i+2}), (S_{i+1}, S_{i+2}, S_{i+3}), ..., (S_{i+2^n-2}, S_{i+2^n-1}, S_{i+2^n}).$$

How many of these triples are such that $(S_j, S_{j+1}, S_{j+2}) = (1, 1, 1)$? (In other words, how many times within one period does the pattern 111 appear?)

Problem 2 (15%)

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

The encryption rules are as follows:

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

Suppose $Pr(K_i) = 1/3$ for $1 \leq i \leq 3$, $Pr(a) = 1/2$, $Pr(b) = 1/4$, $PrP(c) = 1/8$, and $Pr(d) = 1/8$.

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

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

Problem 3 (20%)

a. Suppose two users A and B share a secret n-bit key, k. In order for B to authenticate A, he could check that she has the same key k. Consider the following protocol: B chooses a random bit string r of length n and computes c, the bit-wise exclusive-or of r and k. B sends c to A, who computes d, the bit-wise exclusive-or of c and k. A sends d to B who checks that d and r are the same. Should $d = r$? Is this protocol secure? Why or why not?

b. In the RSA cryptosystem, the public key consists of the modulus n and the exponent b, while the decryption exponent a is kept secret. Suppose a user U leaks his secret key a. Suppose further that when creating a new key pair, for efficiency reasons, he keeps the same modulus, but finds new exponents a' and b'. Is this secure? Why or why not?

c. In the El-Gamal cryptosystem in Z_p^*, the public key consists of the modulus p and the elements α and β, while the discrete logarithm a such that $\beta =$

$\alpha^a \pmod{p}$ is kept secret. Suppose a user U leaks his secret key a. Suppose further that when creating a new key pair, for efficiency reasons he keeps the same modulus, but finds new elements α' and β' and a new secret a' such that $\beta = \alpha^{a'} \pmod{p}$. Is this secure? Why or why not?

d. The known-plaintext attack on the linear feedback shift register stream cipher discussed in the textbook requires n bits of plaintext and n corresponding bits of cipher text where $n = 2m$ (and the recurrence has degree m) to reconstruct the entire key stream. These bits need to be consecutive. Suppose that instead of n consecutive bits, the cryptanalys has m distinct sets of only $m + 1$ consecutive bits. How would this cryptanalyst attempt to reconstruct the entire key stream?

Problem 4 15%

In the RSA cryptosystem, the public key consists of the modulus n and the exponent b, while the decryption exponent a is kept secret. A user can use its own key to create bit commitments as follows: Suppose the user wants to commit to a bit b. It chooses a random number r, with $1 \leq r < n$, subject to the restriction that the low order bit of r is b. Then it encrypts r using its own key to create the commitment B.

a. Under what assumption is this bit commitment scheme "hiding", i.e. for any constant ϵ and any probabilistic distinguisher, the probability that the distinguisher correctly determines b from B is less than $\frac{1}{2} + \epsilon$? Give as weak an assumption as you can.

b. How can the user open a commitment?

c. How can the user give a zero-knowledge proof that it knows the value b?

Problem 5 (40%)

Let n be the product of two large primes, and let $y_i \equiv x_i^2 \pmod{n}$ for $1 \le i \le k$ be quadratic residues in the group Z_n^*. Assume the Prover knows the values $x_1, x_2, ..., x_k$ and that both the Prover and the Verifier are given the values n and $y_1, y_2, ..., y_k$. To show that $y_1, y_2, ..., y_k$ are all quadratic residues, one can execute the following protocol $\lceil \log_2 n \rceil$ times.

Prover		Verifier
		Choose random subset R of $\{1, ..., k\}$.
	$\xleftarrow{R}$	
Choose random $r \in Z_n^*$. Let $z \equiv r^2 \cdot \prod_{i \in R} y_i \pmod{n}$.		
	$\xrightarrow{z}$	
		Choose a random $b \in \{0, 1\}$.
	$\xleftarrow{b}$	
Let $s \equiv r \cdot (\prod_{i \in R} x_i \pmod{n})^b$.		
	$\xrightarrow{s}$	
		Check that $s^2 \equiv z \cdot (\prod_{i \in R} y_i \pmod{n})^{b-1}$ and $s \in Z_n^*$. If not, reject and halt.

You may use the following fact:

Fact: Let $S = A \cup B$, where A and B are disjoint sets. Suppose R is a randomly chosen subset of S, i.e. each element of S is chosen with probability $\frac{1}{2}$, independently of all other choices. Then, if $A \neq \emptyset$, the probability that an an odd number of elements from A is chosen is $\frac{1}{2}$.

a. Suppose that at least one of the y_i is a quadratic nonresidue. What distribution do the values for z have when the Prover follows the protocol?

b. Prove that the above protocol is an interactive proof system showing that all of the y_i are quadratic residues.

c. Suppose that all of the y_i are quadratic residues. What distribution do the values for z have when the Prover follows the protocol?

d. Prove that the above protocol is perfect zero-knowledge.