Skriftlig Eksamen
Kryptologi

Institut for Matematik og Datalogi
Syddansk Universitet - Odense Universitet

Onsdag den 1. juni 2005, kl. 9–13

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

Eksamenssættet består af 7 opgaver på 4 nummererede sider (1–4). Fuld besvarelse er besvarelse af alle 7 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 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 $(S_j, S_{j+1}) = (0, 0)$? (In other words, how many times within one period does the pattern 00 appear?) Why?

Problem 2 (15%)

Suppose a plaintext alphabet, P, and a ciphertext alphabet, C, are both equal to Z_p^*, where p is an odd prime. Consider the following symmetric key cryptosystem. A message $m = m_1 m_2 \dots m_s$, consisting of s symbols from P is encrypted using a shared secret key, $K = k_1 k_2 \dots k_s$, consisting of s values chosen randomly, uniformly and independently from Z_p^*. Symbol m_i from the message is encrypted using k_i, giving the result $c_i = m_i \cdot k_i \pmod{p}$. A key is never used more than once.

a. How is decryption performed?

b. Show that this cryptosystem has perfect secrecy.

c. What advantage or disadvantage does this system have over the one-time pad defined in the textbook?

Problem 3 (5%)

a. When ECB mode is used for encryption with a block cipher, why might it be less secure than CBC mode with the same block cipher?

b. What are two disadvantages of CBC mode over ECB mode?

Problem 4 (20%)

a. What are the elements of the multiplicative group $\mathbb{Z}_{17}^*$?

b. Find a generator of the multiplicative group $\mathbb{Z}_{17}^*$. Show how you check that it is a generator.

c. How many elements of $\mathbb{Z}_{17}^*$ are generators? (Hint: you do not need to check each one to see if it is a generator.)

d. Compute the Jacobi symbol $\left(\frac{23}{243}\right)$, using the standard algorithm (using the four properties of the Jacobi symbol given in the textbook). Show each step.

Problem 5 (15%)

For some of the signature schemes we looked at, it was necessary to find a qth root of 1 modulo p, where p and q were both primes, with q dividing $p-1$. This can be done by choosing a random $g \in Z_p^*$ until finding one where $h \equiv g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$. Then, h can be used.

a. For a given qth root of unity, h, how many $g \in Z_p^*$ are such that $h \equiv g^{\frac{p-1}{q}} \pmod{p}$?

b. Give a value s, expressed as a function of p and/or q, with $2 \leq s \leq p-2$, such that for every $g \in Z_p^*$, $g^{\frac{p-1}{q}} \equiv (g^s)^{\frac{p-1}{q}} \pmod{p}$?

c. What is the expected number of elements one would have to choose randomly from Z_p^* before you would expect to find at least two which gave the same result when raised to the power $\frac{p-1}{q}$ modulo p?

Problem 6 (5%)

What is the unicity distance of the El Gamal Public-key Cryptosystem in Z_p^*. Why?

Problem 7 (30%)

Let n be the product of two large primes, p and q. Suppose that k divides $p-1$ and that $y \equiv x^k \pmod{n}$. Assume the Prover knows the value x and that both the Prover and the Verifier are given the values n, k, and y. To show that $y \equiv x^k \pmod{n}$, one can execute the following protocol $\lceil \log_2 n \rceil$ times.

Prover		Verifier
Choose random $r \in Z_n^*$. Let $z \equiv r^k y \pmod{n}$.		
	$\xrightarrow{z}$	
		Choose a random $b \in \{0,1\}$.
	$\xleftarrow{b}$	
Let $s \equiv r \cdot x^b \pmod{n}$).		
	$\xrightarrow{s}$	
		Check that $s^k \equiv z \cdot y^{b-1} \pmod{n}$). If not, reject and halt.

---

a. Prove that the above protocol is an interactive proof system showing that $y_i \equiv x^k$ for some $x \in Z_n^*$.

b. Suppose that $y = x^k$ for some $x \in Z_n^*$. What distribution do the values for z have when the Prover follows the protocol?

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