Written Exam
Cryptology

Department of Mathematics and Computer Science
University of Southern Denmark

Friday, June 6, 2008, 9:00–13:00

You are allowed to use the textbook and any notes you have for this course, along with a pocket calculator.

The exam consists of 7 problems on 5 numbered pages (1–5). All parts of all seven questions should be answered. The weight assigned to each problem in grading is given in parentheses at the start of each problem.

You may refer to algorithms and results from the textbook, course notes (those included in the official syllabus) or problems which have been assigned during the course. In particular, you may give as a reason for a claim holding that it follows from a result in the textbook or official course notes (assuming this is true). References to other books than the textbook will not be accepted.

Note that if there is a question in a problem which you cannot answer, you may continue with the following questions, assuming the result from the question you could not answer.

Problem 1 (10%)

Suppose that a keystream S is produced by a linear feedback shift register with m stages (by a linear recurrence relation of degree m).

a. Assume that S does not end with an infinite string consisting entirely of alternating zeros and ones (where every one is followed immediately by a zero, and every zero is followed immediately by a one). What is the longest string of alternating zeros and ones which could appear in S? Prove that it is not possible for S to contain a longer string of alternating zeros and ones.

b. How long can S be and still give perfect secrecy if it is to be used to encrypt a bit string using bitwise exclusive-or (as with a one-time pad)?

Problem 2 (10%)

Consider the following cryptosystem for plaintexts consisting of English text, using only the 26 characters $\{a, b, c, ..., y, z\}$:

The ith character in the set is represented using the binary representation of i. Thus, each character is represented by a 5-bit binary string, with a represented by 00001, b by 00010, c by 00011, d by 00100, etc., and z by 11010. The key for encrypting a string of n characters is a string random string of n characters (each one a letter between a and z). The characters in both the original string and the key are replaced by their representations as bit strings, and the results are exclusive-ored together bitwise (as with a one-time pad).

a. How does the receiver decrypt the resulting ciphertext?

b. Prove that this system does not have perfect secrecy.

Problem 3 (10%)

The Rabin Cryptosystem has the disadvantage that the encryption function $e_K(x) = x^2 \pmod{n}$ is not an injection, so decryption is not necessarily unique. Consider the following restriction where $p = 2p' + 1$, $q = 2q' + 1$, and p, p', q, q' are all primes. Restrict messages to be encrypted to be values between 1 and $\min\{p', q'\}$. Now use the same encryption function as for the Rabin Cryptosystem.

a. Is this encryption function an injection (1-1)? Why or why not?

b. Is this cryptosystem secure? Why or why not?

Problem 4 (10%)

Describe two problems with the following proposal for a bit commitment scheme using quantum cryptography, with photons sent either in the rectilinear or circular basis.

To commit to a bit, Alice randomly chooses a basis and sends Bob a photon in that basis (with whichever polarization is correct for the bit being committed to). To open the bit, she tells Bob which basis it was sent in. Bob verifies the commitment by observing it in the basis she tells him.

Problem 5 (10%)

Consider using the counter mode for a block encryption scheme with encryption function $e_K(x)$ and decryption function $d_K(c)$:

A random bitstring of length m (the length of a plaintext and of a ciphertext block) is chosen for the initial value of the counter, *ctr*. The sequence $T_1, T_2, ...,$ is defined by $T_i = \text{ctr} + i - 1 \pmod{2^m}$ for all $i \geq 1$. Encryption of the plaintext blocks $x_1, x_2, ...$ is performed by computing $y_i = x_i \oplus e_K(T_i)$ for all i.

a. How is decryption performed?

b. Suppose one ciphertext block is transmitted incorrectly. How many blocks will be decrypted incorrectly?

Problem 6 (40%)

Let n be the product of two large primes, $p \equiv q \equiv 3 \pmod 4$. Suppose the Prover knows s pairs, $(x_1, y_1), (x_2, y_2), ..., (x_s, y_s)$, such that $y_i \equiv x_i^2 \pmod n$, for $1 \leq i \leq s$. All of these values are in Z_n^*. The Verifier knows the y_i values, but not the x_i values. The Prover convinces the Verifier that all of the y_i are quadratic residues modulo n by repeating the following protocol $\lceil \log_2 n \rceil$ times:

Prover		Verifier
Choose random $v_1, v_2, ..., v_s \in Z_n^*$. Let $u_i \equiv v_i^2 \pmod{n}$, $1 \leq i \leq s$.		
	$u_1, u_2, ..., u_s \longrightarrow$	
		Choose a random $c \in \{0, 1\}$. Choose random $(b_1, b_2, ..., b_s) \in \{0, 1\}^s$.
	$c, (b_1, b_2, ..., b_s) \longleftarrow$	
If $c = 0$, let $z = \prod_{i=1}^{s} v_i^{b_i} \pmod{n}$.		
	$z \longrightarrow$	
If $c = 1$, let $z_i \equiv x_i \cdot v_i \pmod{n}$.		
	$(z_1, z_2, ..., z_s) \longrightarrow$	
		If $c = 0$, check that $z^2 \equiv \prod_{i=1}^{s} u_i^{b_i} \pmod{n}$ for $1 \leq i \leq s$. If $c = 1$, check that $u_i \cdot y_i \equiv z_i^2 \pmod{n}$ for $1 \leq i \leq s$. If so, accept. Otherwise, reject.

a. Prove completeness for the above protocol, showing that (assuming that both the Prover and Verifier follow the protocol) the Verifier will accept if all of the y_is are quadratic residues modulo n.

b. Assume that at least one of the u_i is not a quadratic residue modulo n and the Verifier chooses the b_i randomly. What is the probability that the product $\prod_{i=1}^{s} u_i^{b_i}$ is not a quadratic residue modulo n?

c. Prove soundness for the above protocol.

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

Problem 7 (10%)

Consider Shamir's (t, w) threshold scheme for secret sharing. Suppose that the two secrets, K_1 and K_2 have been shared between w users, so user i has share $y_{1,i}$ for K_1 and $y_{2,i}$ for K_2. Let user i's x-coordinate be x_i in both cases, and let p be the public modulus used. Each of the w users can compute their shares for the secret $K = K_1 + K_2 \pmod{p}$ without any additional help from the dealer by computing $y_i = y_{1,i} + y_{2,i} \pmod{p}$.

Prove that this works.