Written Exam
Cryptology

Department of Mathematics and Computer Science
University of Southern Denmark

Thursday, June 9, 2011, 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 6 problems on 5 numbered pages (1–5). All parts of all six 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 (20%)

Consider a linear feedback shift register with 4 stages (a linear recurrence of degree 4), where the tap sequence is $c_0 = c_3 = 1, c_1 = c_2 = 0$. Suppose a sequence of $4n$ random bits $b_1, b_2, ..., b_{4n}$ is partitioned into consecutive substrings of length 4. For each substring, the linear feedback shift register is applied in such a way that the first output bit (which is also the first bit of the input to the linear feedback shift register) is ignored and the next four output bits are placed in a new sequence. For example, if the original random sequence is 10100111, then the new sequence is 01011111, where the 4th and 8th bits were computed by the linear feedback shift register and the others are just rotates to the left.

a. Suppose the original sequence is 11001001. What is the new sequence produced?

Suppose that a plaintext alphabet $P = \{0, 1\}$, so that a message m is a sequence of bits $(m_1, m_2, ..., m_s)$. Suppose that encryption of a message is bitwise XOR with the new sequence produced from a random original sequence (as with a one-time pad, but the bits for encryption are from the new sequence, not the random original sequence).

b. Suppose the sender and receiver of the encrypted message share the random original sequence and both know the tap sequence. How does the receiver decrypt?

c. Show that this cryptosystem has perfect secrecy.

d. Suppose that the tap sequence is changed so that $c_0 = c_2 = c_3 = 0$ and $c_1 = 1$. Explain why the cryptosystem now does not have perfect secrecy.

Problem 2 (10%)

Consider the ElGamal Public-key Cryptosystem in Z_p^*.

a. Suppose that Bob encrypted several messages, $x_1, x_2, ..., x_n$, to send to Alice using Alice's public key, but used the same value k in every encryption. Thus, the encryptions are

$$(\alpha^k, x_1\beta^k), (\alpha^k, x_2\beta^k), ..., (\alpha^k, x_n\beta^k),$$

where all operations are performed modulo p. Suppose that x_5 was also sent to the eavesdropper, Eve. How can Eve determine the other x_i's?

b. Suppose that, instead of using the same value k, Bob used consecutive values of k. Thus, for some k the encryptions are

$$(\alpha^k, x_1\beta^k), (\alpha^{k+1}, x_2\beta^{k+1}), ..., (\alpha^{k+n-1}, x_n\beta^{k+n-1}),$$

where all operations are performed modulo p. How can Eve still determine the other x_i's if she is sent x_5?

Problem 3 (15%)

Consider a hash function, h, defined as follows:

```
proc $h(x, K)$
    denote $x = x_1||x_2||...||x_n$
    IV $\leftarrow$ 00...0
    $y_0 \leftarrow$ IV
    for $i \leftarrow 1$ to $n$ do
        $y_i \leftarrow y_{i-1} \oplus \mathrm{AES}(x_i, K)$
    return($y_n$)
```

Suppose x_i consists of 128 bits for $1 \leq i \leq n$ (x_n is padded if necessary). Suppose that K also has 128 bits and is public.

a. For each of the following problems explain how easy or hard they are for h. Give the best algorithm you can for solving these problems and analyze them. (i) Preimage, (ii) Second Preimage, (iii) Collision.

b. Would you recommend using this hash functions in connection with a signature scheme, such as El Gamal? Why or why not?

Problem 4 (30%)

Suppose that a Prover wants to convince a Verifier that it knows the factorization of a number n, which is the product of two primes p and q. Consider the following protocol repeated $\lceil \log_2 n \rceil$ times:

Prover		Verifier
		Choose random $v \in Z_n^*$. Let $u \equiv v^4 \pmod{n}$.
	$\xleftarrow{u}$	
Compute a square root x of u such that x is a quadratic residue.		
	$\xrightarrow{x}$	
		Check that $x = v^2 \pmod{n}$. If so, continue. Otherwise, reject.

The Verifier accepts if it has not rejected in any round.

a. Given that u is computed as $v^4 \pmod{n}$ for some $v \in Z_n^*$, how many of its four square roots are also quadratic residues? Consider three cases separately:

- $p \equiv q \equiv 3 \pmod{4}$.
- Exactly one of p and q is congruent to $1 \pmod{4}$, and the other is congruent to $3 \pmod{4}$.
- $p \equiv q \equiv 1 \pmod{4}$.

For the following subproblems, assume that $p \equiv q \equiv 3 \pmod{4}$.

b. Suppose both the Prover and the Verifier follow the protocol. Can the Prover who knows the factorization of n, but otherwise can only compute using probabilistic polynomial time, efficiently find an x which is a square root of v and is a quadratic residue? If so, how? If not, why not?

c. Why do we believe that the Verifier will reject if the Prover cannot factor n? (Give a brief answer.)

d. Is this protocol zero-knowledge? Explain your answer.

Problem 5 (20%)

Let n be the product of two large primes, p and q, where $p \equiv 1 \pmod{3}$, and let $y \in Z_n^*$. Suppose the Prover knows x such that $x^3 \equiv y \pmod{n}$. The Prover convinces the Verifier that there exists an x satisfying $x^3 \equiv y \pmod{n}$ by repeating the following protocol $\lceil \log_2 n \rceil$ times:

Prover		Verifier
Choose random $u \in Z_n^*$. Let $v \equiv u^3 \pmod{n}$.		
	$\xrightarrow{v}$	
		Choose a random $c \in \{0, 1\}$.
	$\xleftarrow{c}$	
Let $z = u \cdot x^c \pmod{n}$.		
	$\xrightarrow{z}$	
		Check that $z^3 \equiv v \cdot y^c \pmod{n}$. If so, continue. Otherwise, reject.

The Verifier accepts if it has not rejected in any round.

a. Prove that the above protocol is an interactive proof system.

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

Problem 6 (5%)

In the quantum cryptography protocol discussed in this course, in order to remove bits where Alice and Bob disagree, they compute parities of randomly chosen subsets of their bits. Since an eavesdropper could get information about the original bits from these parity bits, Alice and Bob jointly discard the last bit of each set where the parity has been revealed (and they have not discarded an incorrect bit). Would it be just as good to remove the first bit in each such set? Why or why not?