Institut for Matematik og Datalogi
Syddansk Universitet

December 14, 2006
JFB

Cryptology – E06 – Week 12

Lecture, November 23

We covered chapter 9.

Lecture, November 30

We will finish chapter 8 and cover sections 10.1, 10.2, and 10.5.4 of chapter 10. We will cover section 11.2.

Lecture, December 7

We will cover up through section 13.2.1 of chapter 13 and begin on chapter 14.

Problem session December 4

1. What group would you use for Diffie-Hellman Key Predistribution?
2. How might you remove the possibility of a Man-in-the-Middle attack in the Diffie-Hellman Key Agreement Scheme?
3. Do problem 10.1 d.
4. Do problem 10.7.
5. Do problem 10.8.

Assignment due Monday, December 21, 14:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in January, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become the assignment you redo). You may work in groups of two or three. You may write in either English or Danish.

1. Suppose a user A uses the same secret random number k in the Digital Signature Algorithm for two different signatures. Show how a cryptanalyst can then find A's secret key.

2. Let n be an integer with unknown factorization $n = pq$, where p and q are prime. Let e and d be such that e is relatively prime to $\phi(n)$ and $ed \equiv 1 \pmod{\phi(n)}$. Suppose that Alice knows n, e, and d, and she publishes n and e, but keeps d secret. Let H be a public collision reistant hash function. Consider the following digital signature scheme:

   To sign a message m of length $2k$, Alice considers it as two concatenated messages m_1, m_2, each of lengh k. Then she computes $sig = (H(< 1 > ||m_1) \cdot H(< 2 > ||m_2))^d \pmod{n}$. Note that $< i >$ is a bit string of length 2 representing the integer i, and $||$ denotes concatenation.

   a. How would a verifier check such a signature?

   b. How would a cryptanalyst create a signature on an arbitirary message m of length $2k$, using a chosen plaintext attack, requesting signatures on at most 3 different messages?

3. Do problem 9.14 in the textbook.

4. Let n be an integer with unknown factorization $n = pq$, where p and q are prime, and let $x \in \mathbb{Z}_n^*$ be a quadratic residue modulo n. Suppose a Prover knows a square root u of x modulo n and wants to prove to a Verifier that she knows this. Consider the interactive protocol in which the following is repeated $\log_2 n$ times:

Prover		Verifier
Choose random $v \in \mathbb{Z}_n^*$. Compute $y = xv^2 \pmod{n}$.	$\xrightarrow{y}$	
		Choose a random $c \in \{1, 0\}$.
	$\xleftarrow{c}$	
Compute $z = u^c v \pmod{n}$.	$\xrightarrow{z}$	
		Check that $z^2 \equiv yx^{c-1}$ (mod n). If not, reject and halt.

a. Prove completeness of this protocol.

b. Prove soundness of this protocol, assuming that finding a square root of v is hard. What is the probability of the Prover getting the Verifier to accept if she does not know a square root of u?

c. What is the distribution of the values y, z sent (in each round) by a Prover following the protocol when both the Prover and Verifier are honest?

d. Prove that the above protocol is honest verifier zero-knowledge. (Actually, one does not need the qualifier "honest", but don't worry about that.)