CHALMERS TEKNISKA HÖGSKOLA
Datavetenskap
Björn von Sydow INN150/TDA350/TDA351

Tentamen i Kryptoteknik
Exam in Cryptography

Thursday December 20, 2007, 14.00 – 18.00.
Teacher: Björn von Sydow, phone 1040.

Tillåtna hjälpmedel: Typgodkänd räknare. Annan minnestömd räknare får användas efter godkännande av kursansvarig vid dennes besök i skrivsalen.
Allowed aids: Approved calculator. Other calculators with cleared memory may be used after approval by the responsible teacher.

The exam has 7 problems with a total of 50 points. 22 points are needed to pass.
For the old course TDA350, problem 7(c) is omitted and 19 points are enough to pass.

Answers must be given in English and should be clearly motivated.

1. We consider an LFSR of length n bits.

   (a) Explain why the generated key sequence cannot have a period longer than $2^n - 1$ bits. (3 p)

   (b) Explain why an LFSR that generates maximal period sequences must have an even number of ones in its tap sequence. (2 p)
   Hint: Consider the state with all ones.

2. A variant of CBC mode is *propagating CBC*. The encryption of message $M_0M_1 \ldots M_n$ is $C_0C_1 \ldots C_n$, where

$$\begin{aligned} C_0 &= M_0 \oplus IV \\ C_i &= E_K(M_i \oplus M_{i-1} \oplus C_{i-1}), \quad i = 1,2 \ldots n. \end{aligned}$$

   Here IV is an initialisation vector agreed upon by sender and receiver using other means.

   (a) Describe how decryption is done. (4 p)

   (b) The difference to ordinary CBC (which omits xoring with M_{i-1}) is that bit error propagation is different. How? (2 p)

3. To avoid certain side channel attacks, most implementations of RSA make use of *blinding*, which works as follows for a user with RSA modulus N, public key e and private key d. After receiving a ciphertext c but before decrypting, the receiver multiplies the ciphertext by r^e for a randomly chosen r. Describe how decryption then proceeds. (4 p)

4. We consider a banking application, where messages of the form *fromAccount, toAccount, amount* are sent within the bank network, with the meaning that *amount* dollars should be transferred from *fromAccount* to *toAccount*. Messages are encrypted using AES in Counter mode, i.e.

$$\begin{aligned} K_i &= E_K(IV||i) \\ C_i &= M_i \oplus K_i. \end{aligned}$$

   Each of the three parts of a message is sixteen characters, i.e. one block, so messages consist of three blocks.

   (a) The adversary has an account in the bank and can intercept and change messages. Imagine now that he knows the *toAccount* for a particular message $m = C_1C_2C_3$. Explain how he can modify the message so that the *amount* is transferred to his own account. (4 p)

   (b) Explain how the use of a MAC would prevent this attack. (3 p)

   (c) Above, $E_K(M)$ denotes using block cipher E with key K on message M. It is possible to define a cipher using similar ideas, but using a hash function instead. Describe how to do it, including how to decrypt. (3 p)

5. In this problem we consider the Pohlig-Hellman cryptosystem, which is a *secret key* encryption method based on the difficulty of the discrete log problem. The setting is $\mathbb{Z}_p^*$ for some large prime p, which need not be secret. In order to exchange messages, Alice and Bob agree on a secret key e, which is a positive integer in $\mathbb{Z}_p^*$. Encryption of m is $c = m^e \in \mathbb{Z}_p^*$. Decryption is $m = c^d \in \mathbb{Z}_p^*$ for a suitably chosen d.

   (a) Alice and Bob agree on p and e and they must both compute d in order to be able to decrypt. What condition must e satisfy and how can they compute d? (3 p)

   (b) The only difference between this cryptosystem and RSA is in the modulus; in RSA one works in $\mathbb{Z}_N^*$, where $N = p \cdot q$. Explain why this difference makes it possible to use RSA as a public key system, while the Pohlig-Hellman system could only be used with secret keys. (3 p)

   Remark: Pohlig and Hellman invented this system in 1975; however, they failed to see how to modify it to a public key system.

6. We consider the following protocol, designed to let A and B decide on a fresh, shared session key K'_{AB}. We assume that they already share a long-term key K_{AB}.

$$\begin{array}{lll} 1. & A \longrightarrow B & : \quad A, N_A. \\ 2. & B \longrightarrow A & : \quad \{N_A, K'_{AB}\}_{K_{AB}}. \\ 3. & A \longrightarrow B & : \quad \{N_A\}_{K'_{AB}}. \end{array}$$

   (a) We first try to understand the protocol designer's reasoning:

      i. Why would A and B believe after the protocol run that they share K'_{AB} with the other party?

      ii. Why would they believe that this shared key is fresh?

   In both cases, you should explain both A:s and B:s reasons, so your answer should complete the sentences

   A believes that she shares K'_{AB} with B since ...

   B believes that he shares K'_{AB} with A since ...

   A believes that K'_{AB} is fresh since ...

   B believes that K'_{AB} is fresh since ...

   (4 p)

   (b) Assume now that A starts a run of this protocol with B. However, the connection is intercepted by the adversary C. Show how C can start a new run of the protocol using reflection, causing A to believe that she has agreed on a fresh key with B (in spite of the fact that she has only been communicating with C). Thus, in particular, the belief in (a) is false. (3 p)

   (c) Propose a modification of the protocol that prevents your attack from (b). (2 p)

7. Here we consider the public key encryption scheme DHIES, which makes use of many cryptographic primitives:

   - A subgroup of prime order q of $\mathbb{Z}_p^*$ for some large prime p and a generator g for that subgroup. Typically, q would be a 160 bit and p a 1024 bit prime.
   - A symmetric encryption scheme E with keys of n_1 bits.
   - A MAC function MAC with keys of n_2 bits.
   - A hash function H that produces hash values with $n_1 + n_2$ bits.

   All these choices are public. Each user chooses a private key $x < q$ and a public key $X = g^x$.

   To encrypt a message m for a user with this key pair, one proceeds as follows:

- Choose a random $y < q$ and compute $Y = g^y$.
- Compute $K = X^y$.
- Compute $H(K||Y)$ and parse it as $k_1||k_2$.
- Compute $C = E_{k_1}(m)$.
- Compute $T = MAC_{k_2}(C)$.
- The encrypted message is $Y||C||T$.

Note that here m can be of arbitrary length, so this is a hybrid encryption scheme.

(a) Describe how the receiver decrypts a received ciphertext. (4 p)

(b) DHIES can be shown to be resistant to CCA2 attacks; explain briefly what this means. (3 p)

(c) DHIES can be adapted to work in elliptic curve groups. Describe the changes needed and what advantages this would imply. (3 p)