CHALMERS TEKNISKA HÖGSKOLA
Datavetenskap
Björn von Sydow INN150/TDA350

Tentamen i Kryptoteknik
Exam in Cryptography

Sunday December 17, 2006, 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 tools: Approved calculator. Other calculators with cleared memory may be used after approval of the responsible teacher.

To pass the exam, 20 points is needed for Chalmers students, 23 points for GU students. The exam has 7 problems with a total of 50 points.

You may answer in English or in Swedish. Motivate all your answers.

We hope to be able to mark the exams and post results on the course web site before Christmas. Visit the site for further information!

1. Alice has decided to use a stream cipher for encryption, i.e.

$$c = m \oplus b(k)$$

where the binary string m is the plaintext, $b(k)$ is the keystream, depending on the secret key k, and c is the ciphertext. As keystream generator she has decided to use an LFSR. Her messages are English text encoded with 8 bits per letter and message lengths are always 25 letters.

   (a) Alice wants the keystream to have the property that the keystream used for each message is shorter than one full period. What is the minimum size of the key k (in bits)? (3 p)

   (b) Alice's messages have the property that they all start with `Alice`. The adversary knows this and has access to one ciphertext c. Will he be able to break the encryption, if Alice chooses the minimum key size from (a)? (3 p)

2. We consider an n round Feistel network with cipher function f:

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus f(K_i, R_i). \end{aligned}$$

We do not specify the function f or how the subkeys K_i are derived from the cipher key.

The plaintext block is $L_0||R_0$ and the ciphertext block is $R_n||L_n$.

   (a) What properties need f satisfy in order for encryption to be invertible? Remember to motivate the answer! (3 p)

   (b) How is decryption performed? You do *not* need to justify that decryption works, i.e. inverts the encryption. (2 p)

3. (a) A web-based auction site uses textbook RSA encryption to maintain the secrecy of bids. The site has public RSA key (N, e). For the sake of this problem we make the completely unrealistic assumption that a bid is sent in a message containing only a single integer, representing the bid value.

   Now, Alice has just made a bid and the adversary Mallory has eavesdropped and heard the ciphertext c. Mallory's main aim is to prevent Alice's bid from winning. Of course, he cannot recover Alice's bid, but makes the guess that her bid is an integer which is a multiple of 10. Show that, if Mallory's guess is right, he can himself make a bid which is 10% higher than Alice's. (6 p)

   (b) To prevent the attack from (a) and other attacks against textbook RSA, messages should be padded using some padding scheme, such as OAEP. Describe some guiding principles in constructing such padding schemes. You do *not* need to describe the actual padding scheme in detail. (2 p)

4. We consider cryptographic hash functions.

   (a) What is meant by collision resistance for a hash function? (3 p)

   (b) What common usage do hash functions have in connection with digital signatures? (2 p)

   (c) What is the difference between a hash function and a message authentication code (MAC)? (2 p)

   (d) Why is it recommended to use a hash function with $2n$ bits of output when it is used as component in a system designed for n bits of security? (3 p)

5. We consider the following protocol intended to allow Alice to authenticate herself to Bob with the help of a trusted third party T. Alice and Bob do not know each other, but each of them shares a symmetric key, K_{AT} and K_{BT}, respectively, with T.

$$\begin{array}{rlcl} 1. & A \longrightarrow B & : & A. \\ 2. & B \longrightarrow A & : & N_B. \\ 3. & A \longrightarrow B & : & \{N_B\}_{K_{AT}}. \\ 4. & B \longrightarrow T & : & \{A, \{N_B\}_{K_{AT}}\}_{K_{BT}}. \\ 5. & T \longrightarrow B & : & \{A, N_B\}_{K_{BT}}. \end{array}$$

After receiving message 5, Bob decrypts it and checks that the encrypted message contains Alice's name and the nonce he created and sent in message 2. If so, he accepts the run and Alice is authenticated.

Now consider the following attack, where the adversary C will manage to get himself authenticated as Alice.

$$\begin{array}{rlcl} 1. & C(A) \longrightarrow B & : & A. \\ 2. & B \longrightarrow C(A) & : & N_B. \\ 3. & C(A) \longrightarrow B & : & N_B. \end{array}$$

Note that in message 3, C deviates from the protocol. Your task is to show how the protocol run is completed by B and C – in fact, C will intercept also message 4 (masquerading as T) and himself send message 5 to B. Finally, you must explain B:s reasoning in accepting the run. (6 p)

6. We recall CBC mode for encryption of a message $M = M_1 M_2 \ldots M_n$:

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

Here E_k is the block cipher encryption function for key k and M is split into blocks of appropriate size. In the variant considered here, the initialization vector IV is agreed upon in advance and hence not sent with the ciphertext. Thus, the ciphertext is $C_1 C_2 \ldots C_n$.

In addition to encryption, this recurrence can be used to produce a message authentication code (MAC): The CBC-MAC of message M is then C_n (previous C_i are discarded). In this usage, the IV is considered to be publicly known and part of the MAC algorithm.

(a) A MAC algorithm is secure against an adaptive chosen-text attack if an efficient adversary cannot win the following game with non-negligible probability:

The adversary is allowed to ask for the MAC for a number of messages of her choice, following which she must produce a pair consisting of a new message and its MAC.

Show that CBC-MAC is not secure in this sense, since the adversary can win the game by only asking for the MAC of two one-block messages: first for an arbitrary block x, and then, after receiving the MAC m for x, for m itself. Which message and corresponding MAC can the adversary then exhibit? (5 p)

(b) A common combination of authentication and encryption is that a sender first computes the MAC m of a message x and then encrypts $x||m$, giving a ciphertext c to be transmitted to the receiver.

Here we consider this practice where the MAC algorithm is CBC-MAC and the encryption method is CBC mode. An ignorant user suggests to use *the same k* and *IV* for both MAC computation and encryption, arguing that this is more efficient, requiring only one pass over the message. Show that this proposal is insecure, by showing that the last block of c is independent of x. Discuss the consequences. (5 p)

7. The Rabin-Miller primality test is based on the following: To test whether an odd number n is prime, first write $n-1$ as $n-1 = 2^s \cdot m$ where m is odd. Then pick a number a with $0 < a < n$ and compute

$$\begin{aligned} x_0 &= a^m \bmod n, \\ x_{k+1} &= x_k^2 \bmod n, \quad \text{for } k = 0, 1, \ldots, s-1. \end{aligned}$$

Prove that if n is actually prime, then either $x_0 = 1$ or $x_k = n-1$ for some $k < s$. (5 p)

(In the actual test, failure in this test reveals that n is not prime. If the test succeeds, it is repeated for several values of a. However, you need *not* consider the full test).