CHALMERS TEKNISKA HÖGSKOLA
Datavetenskap
Björn von Sydow INN150/TDA350

Tentamen i Kryptoteknik
Exam in Cryptography

Monday December 12, 2005, 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, 24 points is needed for Chalmers students, 28 points for GU students. The exam has 7 problems with a total of 60 points.

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

1. (a) What is the maximal period length of an LFSR of size n? Motivate why the period cannot be longer. You need not prove that this length can be achieved. (3 p)

   (b) The output sequence of an LFSR starts with `100000001`. What is the minimal size of the LFSR? Your answer should exhibit an LFSR of this size that does produce the given sequence and give a motivation why no shorter LFSR will do. (4 p)

2. Alice has been using the Vigenère cipher for encryption, but has become aware that it can be easily broken. She is now considering using double encryption, i.e. sender and receiver will agree on *two* keywords key_1 and key_2 and encrypt message m by first encrypting m with the Vigenère cipher using key key_1 and then encrypting the resulting ciphertext with the Vigenère cipher using key key_2 . Alice is confident that this will be more secure.

   (a) Give a detailed argument that shows that the proposed encryption has in fact the same effect as a single Vigenère encryption using a single keyword key_3 that can be determined from key_1 and key_2. What is the length of key_3? (4 p)

   (b) Do you agree with Alice that the double encryption will be more resistant against e.g. the Kasiski method for discovering the length of the keyword? (3 p)

3. (a) Describe the essential properties we want a cryptographic hash function to have. (2 p)

   (b) Describe briefly some situations where such functions are used. (2 p)

   (c) Explain briefly the birthday attack against a hash function. (2 p)

4. We recall the CBC mode of encryption of a message $M = M_1M_2M_3\ldots M_n$, where M_i is block number i of M. Then the encrypted message is $C_0C_1C_2\ldots C_n$, where

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

   Now we consider the following beginning of a protocol:

   1. $A \longrightarrow B : N_A$

   2. $B \longrightarrow A : \{N_A, K\}_{K_{AB}}$.

   We do not need to know more about the protocol (which may contain further messages) than the following:

   - A and B share a long-term AES key K_{AB}; the notation $\{\ldots\}_{K_{AB}}$ denotes encryption of $\ldots$ using AES in CBC mode (block size 128 bits).
   - N_A is a 128 bit nonce chosen by A and K is a 128 bit session key chosen by B.

   In the second message, B includes N_A to ensure freshness and K as a session key for the session just started. When A receives the second message, she thus concludes that B is alive at the other end and has just chosen a fresh session key K.

   Now consider the following scenario: The adversary C eavesdrops on a run of this protocol between A and B and stores messages sent. Because of an unspecified mistake by A or B (outside the protocol), C gets hold of K and can of course read all subsequent messages in the session. But, the situation is worse than that, as we shall see.

   Let message 2 in the run described above be $C_0C_1C_2$ (three blocks; the IV and two encrypted blocks).

   The next day, A and B initiate a new session. C again eavesdrops and now intercepts the second message $C_0'C_1'C_2'$, changes it to $C_0'C_1'C_2$ and sends the changed message to A, pretending to be B. Show that A will accept the message as the reply to her first message in the new run and that C will know the session key of the new run and thus can continue the session with A, pretending to be B. (10 p)

5. (a) What is, in the context of cryptography, a certificate? In particular, what data does it typically contain, who issues it and what is the purpose of it? (4 p)

   (b) We consider the following protocol for authentication:

   1. $A \longrightarrow B$: n_A
   2. $B \longrightarrow A$: $Cert_B, n_B, S_B\{n_A, n_B\}$
   3. $A \longrightarrow B$: $Cert_A, S_A\{n_B, n_A\}$

   Here n_A and n_B are nonces chosen by A and B, S_A and S_B are the signing operations of A and B, respectively, and $Cert_A$ and $Cert_B$ are certificates, authenticating the public keys of A and B.

   Demonstrate an attack against this protocol, whereby an adversary C can authenticate himself as A to B. (6 p)

   Hint: The attack we have in mind requires that A first initiates a run of the protocol with C.

6. (a) Alice has decided to use RSA for encryption and has generated two large primes p and q and computed $N = pq$. She has also chosen encryption key $e_A = 3$ and computed her private key d_A. When her friend Bob hears about this, he also wants to use RSA. Alice assists him by choosing for him $e_B = 5$ and computing d_B, using the same N. Alice gives Bob his keys (N, e_B) and d_B.

   The next day their common friend Charlie sends message m encrypted to both Alice and Bob, using their respective encryption keys. However, the adversary Deborah eavesdrops and gets hold of the two ciphertexts c_A and c_B. Deborah also notices that Alice and Bob use the same N. Show how she can recover m. You may assume that $\gcd(m, N) = 1$. (8 p)

   (b) Does Deborah's attack generalize to other values of e_A and e_B than 3 and 5? (2 p)

7. In this problem we will consider a signature scheme that once was proposed as a more efficient alternative to RSA. The setting is as follows.

   User Alice chooses two large secret primes p and q. We put $N = pq$ as in RSA. She also chooses an element $g \in \mathbb{Z}_N^*$ that generates a subgroup of prime order r. Alice's public key is (N, g); her private key is r. Here p and q should be big enough to make factoring of N infeasible, i.e. at least 1024 bits. Further, r should be big enough to make the discrete log problem for the subgroup infeasible; hence r could be a 160 bit number.

   The community of users have also agreed on a hash function H. To sign message m, Alice first hashes m and computes x such that $x \cdot H(m) = 1 \bmod r$. The signature is then $s = g^x \bmod N$. The intended advantage of the scheme is that $x < r$, so the exponent is much smaller than for RSA signatures.

(a) How will Bob, after receiving (s,m), verify that s is Alice's signature on m? You must show that a correct signature will be verified. (5 p)

(b) The proposed scheme has several vulnerabilities and is completely broken. We will now demonstrate some of the problems with the scheme.

   i. Show that r is a divisor of at least one of $p-1$ or $q-1$. (2 p)

   ii. Show that, if r is a divisor of $p-1$ but not of $q-1$, then one can factor N, using only the public key. (3 p)
   Hint: Show that $g \bmod q = 1$.