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

Exam in Cryptography

Thursday December 18, 2008, 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. Construct an LFSR (linear feedback shift register) of minimal length that produces the output $(1001110)^\infty$. (3 p)

2. 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) A particular hash function produces n bit hash values. We generate messages at random in some unspecified way and hash them. Approximately how many messages would you expect that we have to generate before we get a collision? (2 p)

3. As you know, DES is insecure because of its short key length (56 bits). An improvement, proposed by Rivest, is DESX. DESX has key length 120 bits, seen as a pair (k_1, k_2), where k_1 is 56 bits and k_2 64 bits. The encryption of a one-block message m is
$$DESX_{(k_1,k_2)}(m) = DES_{k_1}(m \oplus k_2) \oplus k_2.$$
   (a) Explain how decryption is done. (3 p)
   (b) Explain why the inner xor is necessary, i.e. explain an attack against
$$DESX'_{(k_1,k_2)}(m) = DES_{k_1}(m) \oplus k_2$$
   that is much better than brute force. (5 p)

4. (a) Can a user of RSA choose the encryption exponent e to be even, e.g. $e = 4$? (2 p)

   (b) Alice wants to send an encrypted message to Bob using RSA, but doesn't know his public key. So, she sends Bob an email asking for the key. Bob replies with his RSA public key (e,N). However, the active adversary intercepts the message and changes one bit in e from 0 to 1, so Alice receives an email claiming that Bob's public key is (e',N), where e' differs from e in one bit. Alice encrypts m with this key and sends it to Bob. Of course, Bob cannot decrypt, since the message was encrypted with the wrong key. So he resends his key and asks Alice to send the encrypted message again, which she does. The adversary eavesdrops to the whole communication without interfering further. Describe how he can now recover m.
   (5 p)

5. Alice and Bob share a long term key K_{AB} and want to use it for authentication, employing protocol ISO 9798-2, which is as follows:

$$\begin{array}{lcl} 1. & A \rightarrow B & : \quad A, N_A \\ 2. & B \rightarrow A & : \quad \{A, N_A, N_B\}_{K_{AB}} \\ 3. & A \rightarrow B & : \quad \{N_B, N_A\}_{K_{AB}} \end{array}$$

   We assume that a block cipher is used for encryption, that nonces and names are each one block and that CBC mode is used. Recall that CBC mode uses the recurrence

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

   (a) Explain why the change of order between the nonces is necessary in message 3. (3 p)

   (b) The adversary is planning an attack against Alice, in a completely unrelated protocol, where he will need to send the message A,B encrypted with K_{AB}. Describe how he may (mis-)use the above protocol to get this service from Bob. (3 p)

6. We consider an identification protocol based on the discrete log problem. The setting is some cyclic group G of prime order q with generator g. Peggy chooses a private key $x < q$ and has as public key $X = g^x$. The purpose of the following protocol is to convince Victor that Peggy knows x:

   1. Peggy chooses $r < q$ at random and computes $R = g^r$ and $S = g^{x-r}$. She sends R and S to Victor.
   2. Victor chooses a random bit b and sends to Peggy.
   3. If $b = 0$, Peggy sends $z = r$ to Victor; if $b = 1$ she sends $z = x - r$.

(a) What computations will Victor now do to check Peggy's values? (3 p)

(b) Show that a false Peggy (i.e. someone who does not know x) can participate in this protocol and have probability 0.5 to pass Victor's check. (3 p)

(c) How would you extend the protocol so that Victor can be reasonably convinced that if Peggy passes, she really knows x? (2 p)

7. We consider an encryption scheme proposed by Zheng and Seberry, which combines ideas from Diffie-Hellman and stream ciphers. The setting is a subgroup G of $\mathbb{Z}_p^*$ for a large prime p. G has prime order q and generator g. The users have also agreed on a hash function H which produces n bits digests and a pseudorandom bit generator b which, when given a seed in the subgroup, produces a random-looking bitstream.

   Each user chooses private key $x \in G$ and public key $X = g^x$. Encryption of message m proceeds as follows. The sender

   - computes $t = H(m)$.
   - chooses a random integer $y < q$.
   - computes $Y = g^y$.
   - computes $k = b(X^y)$, where the length of k is length$(m) + n$ bits.
   - computes $c = k \oplus (m||t)$.

   The ciphertext is (Y, c).

   (a) Describe how decryption is done. Note: Not all pairs of bitstrings of the correct length are valid ciphertexts, so decryption may fail. (4 p)

   (b) In a CCA2 attack, the adversary picks two messages m_0 and m_1 and sends them to Alice. Alice picks one of these at random and encrypts it, producing ciphertext c, which is sent to the adversary, who may then ask Alice to decrypt a number of ciphertexts (except c) before he guesses whether m_0 or m_1 was encrypted.

   Demonstrate that the Zheng-Seberry scheme is not CCA2 secure; in fact, show that the adversary can construct one single ciphertext, the decryption of which will tell him whether c is the encryption of m_0 or m_1. (4 p)

   (c) Give a brief description of how this encryption scheme could be adapted to elliptic curve cryptography and why one might want to do that. (3 p)