CHALMERS TEKNISKA HÖGSKOLA
Datavetenskap
Daniel Hedin DIT250/TDA351

Exam in Cryptography

Thursday, April 24, 2014, 8.30 – 12.30.
Teacher: Daniel Hedin, phone 0709 261771.
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 6 problems with a total of 50 points. 22/31/40 points are needed for grade 3/4/5.

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

1. Hash functions. (10p)

a) Describe three important properties we expect cryptographic hash functions to have. (3p)

b) Describe one important use of cryptographic hash functions. (2p)

c) Explain the relation between cryptographic hash functions and message authentication codes (MACs). In particular, how can they be formulated in terms of each other? (5p)

2. Public key. (6p)

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? (3p)

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. (3p)

3. Block Ciphers. (10p)

a) Describe the need for padding in the block cipher setting and how padding can be done. What property is important for a padding schema? (3p)

b) In light of what we have seen in the course — in particular the SSL attack – should you pad before authenticating a message or pad the authenticated message? Be careful to justify your answer - a simple yes/no does not suffice. (2p)

c) Imagine you are designing a block cipher based cryptographic file system. Describe the modes ECB, CBC, and CTR, and discuss their relative merits in this setting. Which mode would you choose? (5p)

4. Protocols: key exchange. (7 p)

a) Explain what a nonce is and how it is used in cryptographic protocols. (2 p)

b) Consider a key exchange protocol using a trusted party T. Assuming that A and B each share a key K_{AT} and K_{BT} with T the suggested protocol is the following:

$$\begin{array}{lll} 1. & A \longrightarrow T: & A, B, \{K\}_{K_{AT}} \\ 2. & T \longrightarrow A: & \{K\}_{K_{BT}} \\ 3. & A \longrightarrow B: & \{K\}_{K_{BT}}, \{M\}_K \end{array}$$

A uses T to encrypt the session key for B and includes this encrypted key in message 3, together with the encrypted message.

Unfortunately, the protocol is vulnerable to an attack by any adversary C, who shares a key K_{CT} with with T. Explain how C, after eavesdropping on the above run, can go on to decrypt the message. Then suggest some modification to the protocol that prevents the attack you found. (5 p)

5. Protocols: authentication. (10p)

We recall the Fiat-Shamir authentication protocol. Let $N = p \cdot q$, where p and q are primes. The prover P wants to convince the verifier V that he knows a square-root of $y \in \mathbb{Z}_N^*$, i.e., a number x such that $y = x^2 \in \mathbb{Z}_N^*$, without revealing x to V. They use the following protocol. All computations are in $\mathbb{Z}_N^*$.

- P generates a random r, computes $R = r^2$ and sends R to V (the commitment).
- V generates a uniformly random bit b and sends it to P (the challenge).
- If $b = 0$, P responds with $z = r$, if $b = 1$ with $z = r \cdot x$ (the response).

a) What computation will V perform to check P's values? (3 p)

b) Discuss how a cheating P, who does not know x, can achieve a probability of 0.5 of passing the test. (3 p)

c) This protocol is used in decoders for Pay-TV access control. The decoder plays the role of the verifer, while the prover is a smart-card bought by the viewer. Here y is the card number, which is publicly known and transmitted to the decoder. The secret x is stored in the smart-card software. The broadcast periodically contains an instruction to check authenticity of the smart-card, together with the random b to be used in the next run of the protocol.

Early uses of this protocol in decoders did not generate the commitment r at random each time but used same r repeatedly (since V did not anyhow have memory enough to check that r was different each time). Explain how this gave opportunities for production of pirate cards. (4 p)

6. Security notions. (7p)

Recall the notion of *indistinguishability under chosen plaintext*, IND-CPA. Let $(\mathcal{K}, E, D)$ be a public key system with key generation algorithm $\mathcal{K}$, encryption algorithm E and decryption algorithm D all known by the adversary. We say that the public key system satisfies IND-CPA if the attacker has *negligible probability* of winning the following game.

$$
\begin{array}{l}
\text{IND-CPA}: \\
\quad (pk, sk) \leftarrow \mathcal{K}() \\
\quad m_0, m_1 \leftarrow \mathcal{A}_1(pk) \\
\quad b \xleftarrow{\$} \{0,1\} \\
\quad c \leftarrow E(pk, m_b) \\
\quad b' \leftarrow \mathcal{A}_2(pk, c)
\end{array}
$$

a) Explain IND-CPA in words. In particular, why is IND-CPA a good security notion? Does IND-CPA limit the amount of information that the adversary can learn about the plaintext from the ciphertext? What about the secret key? (3p)

b) Text-book RSA does not satisfy IND-CPA. Show this by giving an attacker that wins the IND-CPA game against text-book RSA. (2p)

c) Describe in broad terms how text-book RSA can be modified to satisfy IND-CPA. (2p)