CHALMERS UNIVERSITY OF TECHNOLOGY
Dept of Computer Science and Engineering DIT250/TDA352

Exam in Cryptography

Friday January 14, 2022, 8.30 – 12.30.
Teacher: Björn von Sydow, phone 0722 39 14 01.

The exam has 7 problems with a total of 50 points. 22/31/40 points are needed for grade 3/4/5 for Chalmers students, 22/40 points for G/VG for GU students.

No aids except an approved calculator may be used. The intention is that a calculator should not be needed. Answers must be given in English and should be clearly justified.

1. We consider cryptographic hash functions.
   (a) What is meant by collision resistance for a hash function? (1 p)
   (b) What common usage do hash functions have in connection with digital signatures? Give also reasons for this usage. (3 p)
   (c) 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? (2 p)

2. We consider the RSA system.
   (a) Describe in detail how a user chooses a key pair for RSA. Illustrate with an example where $p = 5$ and $q = 11$, but do not *only* give the example. (4 p)
   (b) Why is 65537 often recommended as public key (rather than any other number of similar size)? (1 p)
   (c) Which of RSA encryption and decryption is significantly slower than the other and why? (2 p)
   (d) Why does RSA require much longer keys (e.g. 3072 bits) than AES (128 bits)? (2 p)

3. In this problem we consider message authentication codes (MAC's). We recall that the MAC signing algorithm takes a key and an arbitrarily long message as arguments and produces a fixed size *tag* (typically 128 bits).
   (a) What arguments does the verify algorithm take and what result does it produce? (2 p)
   (b) Define informally the notion of a secure MAC (i.e. you do not have to set up a detailed attack game). (2 p)
   (c) Let (E, D) be a block cipher with block size equal to the tag size. Consider the following definition of a MAC for an n-block message $M = M_1 M_2 \dots M_n$:

   $$\mathrm{MAC}(k, M) = E\left(k, E(k, M_1) \oplus E(k, M_2) \oplus \dots \oplus E(k, M_n)\right).$$

   Show that this MAC is not secure. (3 p)

4. Eve has eavesdropped on a communication where Bob sends the password for his *BankID*, six decimal digits encoded in ASCII, to Alice, encrypted with the one-time pad. Eve thinks that, since the ciphertext (and thus the key) is only 48 bits long and she has access to a very powerful computer, she can do a brute force attack and recover the password. Explain why this will not work. Your explanation should include defining what the one-time pad is and what a brute force attack is. (6 p)

5. We consider key establishment using Diffie-Hellman, so we have the usual setting of a cyclic group $\mathcal{G}$ of prime order q with generator g. Alice and Bob have both chosen long-term key pairs $A = g^a$ and $B = g^b$, respectively, and have certificates for these.

   Below, x and y are chosen at random during protocol execution and $X = g^x, Y = g^y$.

   1. Alice $\rightarrow$ Bob : $X, \text{Cert}(\text{"Alice"}, A)$
   2. Bob $\rightarrow$ Alice : $Y, \text{Cert}(\text{"Bob"}, B)$

   After the run, both parties will compute a common session key. Their aim is to achieve both authentication and perfect forward secrecy. So, they use a key derivation function H, computing the key as $H(\mathit{args})$ where *args* is based on data sent in the protocol and keys available to them. Suggest suitable *args* for both Alice and Bob and argue that the resulting key exchange provides both authentication and perfect forward secrecy. As part of the solution, define informally these two notions. (6 p)

6. We recall CBC mode for a block cipher (E, D), here denoted E^{CBC}:

   $$E^{\text{CBC}}(k, M_1 M_2 \dots M_n) = C_0 C_1 C_2 \dots C_n,$$

   where $C_0 = IV$ and $C_i = E(k, M_i \oplus C_{i-1}),$ for $i = 1, 2, \dots n$.

   The Android Keystore is an Android system service that allows apps to store cryptographic keys in a form where integrity and confidentiality is protected using authenticated encryption. Unfortunately, at least until 2016, the encryption method used was a non-standard construction, which, as we will see, does not provide the intended CCA security.

   The encryption method in the Keystore, denoted $\mathbb{E}$, uses also a hash function h, with hash values of the same size as blocks. The encryption of m starts with hashing m; the hash value is added as first block and the resulting extended message $h(m)||m$ is encrypted in CBC mode, i.e. the complete encryption is $\mathbb{E}(k, m) = E^{\text{CBC}}(k, h(m)||m)$.

   (a) Describe how decryption is done. You may use D^{CBC} to denote decryption of CBC mode without further explanation. Note that decryption may fail. (2 p)

   (b) The attack that shows that $\mathbb{E}$ is not CCA secure runs as follows:

   1. The attacker chooses two messages m_0 and m_1 with $h(m_0) \neq h(m_1)$.
   2. He sends $m'_0 = h(m_0)||m_0$ and $m'_1 = h(m_0)||m_1$ to the Challenger.[1]
   3. He receives back a ciphertext c, the encryption with $\mathbb{E}$ of one of m'_0 and m'_1 for some key k.
   4. He strips off the first block of c, giving c', and asks for decryption of c'.
   5. He gets the decryption result r and must now return a bit b, his guess of which of the two messages m'_0 and m'_1 that was encrypted.

   Describe how the attacker uses r to choose b, and explain why he will win the game. (4 p)

   (c) Explain to Android developers how CCA security can be achieved, using a well-known combination of secure primitives. (2 p)

[1] It is *not* a typo that m_0 is hashed in both cases!

7. We consider a variant of ElGamal encryption in the setting of a cyclic group $\mathcal{G}$ of prime order q with generator g. We also assume a symmetric encryption scheme (E, D) where $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$. Finally, we need a hash function $H : \mathcal{G} \to \mathcal{K}$ for key derivation.

   Each user has a private key $x \in \mathbb{Z}_q^*$ and a public key $X = g^x$. To encrypt message $m \in \mathcal{M}$ for this user, the sender chooses a random $y \in \mathbb{Z}_q^*$, computes $Y = g^y$, $k = H(X^y)$ and $c = E(k, m)$. The ciphertext is (Y, c).

   (a) How is a ciphertext (Y, c) decrypted? (3 p)

   (b) We now consider a scenario where a server S stores a private key $x \in \mathbb{Z}_q^*$ and uses it to decrypt incoming ciphertexts. If the server is compromised and the key x leaked to an attacker, he can decrypt all ciphertexts. To avoid this single point of failure, the secret x is divided into n shares (i, x_i) using the (n, t) Shamir secret sharing scheme, and the shares are stored on n distinct servers S_i, $i = 1, \ldots n$. Note that x is no longer stored on S.

   When a ciphertext (Y, c) arrives to S, it forwards Y to all the S_i, which are expected to reply with (i, Y^{x_i}). Describe how S, after having received t replies, completes the decryption. (5 p)