CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

05 April 2018, 08:30 – 12.30

Tillåtna hjälpmedel: Typgodkänd räknare. Annan minnestömd räknare får användas efter godkännande av kursansvarig vid dennes besök i skrivsalen.
No extra material is allowed during the exam except of pens and a simple calculator (with cleared memory). No smartphones or other electronic devices are allowed.
Answers must be given in *English* and should be clearly justified.

Teacher/Examiner: Katerina Mitrokotsa
Questions during exam: Katerina Mitrokotsa, phone 031 772 1040

The exam is divided in four main topics and the total number of points is 50.
The grades are:

CTH Grades:	22-30 → 3	31-39 → 4	40-50→5
GU Grades:	22-39 → G	40-50 → VG	

Good luck!

1 Symmetric Ciphers (14 p)

(a) Suppose $\mathcal{G} : \mathcal{K} \rightarrow \{0,1\}^n$ is a pseudorandom generator (PRG). Let us denote for $k \in \mathcal{K}$ $G(k) = g_1, g_2, g_3, \ldots, g_n$ where g_i denotes the $i-th$ bit of $G(k)$ for $k \in \mathcal{K}$. We know that for this PRG it holds: $g_1 \oplus g_2 \oplus \ldots \oplus g_n = 1$ for all $k \in \mathcal{K}$. Is $\mathcal{G}$ predicable? If yes show why. (2 p)

(b) Let us consider that $\mathcal{G} : \mathcal{K} \rightarrow \{0,1\}^n$ is a predictable PRG. Describe an attack that can be performed against a stream cipher that uses the predictable PRG $\mathcal{G}$. (3 p)

(c) Let us consider the following symmetric cipher:

$$E(k, m_0) = E(k, m_{00}||m_{01}) = m_{00}||E(k \oplus m_{01})$$

where m_{00} and m_{01} denote the first and second bit of a message m_0. Prove that this symmetric cipher is not semantically secure. (5 p)

Hint: Use a security game and describe a successful strategy of the attacker.

(d) Prove that the One Time Pad (OTP) is semantically secure (for one time key). (4 p)

Hint: use the standard game between a challenger and an adversary.

2 Public Key Encryption (12 p)

(a) Let $G = \mathbb{Z}_{13}^*$ and $g \in G$. Show that g=6 is a generator of the group G. (2 p)

(b) Suppose that Alice has a secret value $a = 3$ and Bob has a secret value $b = 6$. Describe how Alice and Bob may establish a secret key using the Diffie-Hellman protocol using the group $G = \mathbb{Z}_{13}^*$ and the generator $g = 6$. (2 p)

(c) Describe how Eve may perform a man-in-the-middle attack against the Diffie-Hellman exchange protocol used above. (2 p)

(d) Describe how the RSA encryption works (2 p)

Hint: Describe the algorithms with their corresponding input and output.

(e) Define the IND-CPA security game (indistinguishability chosen plaintext attacks) and show that the RSA encryption scheme is not secure under IND-CPA. (4 p)

3 Data Integrity (15 p)

(a) How can we sign and how can we verify a signed message using textbook RSA? (2 p)

(b) Bob has received from Alice two documents signed with textbook RSA (m1; s1) and (m2; s2). What problem does this cause and how it can be avoided? (2 p)

Hint: Can Bob generate a new signed message?

(c) Explain what a cryptographic hash function is and the notion of collision resistance. (2 p)

(d) Describe the birthday paradox and its impact on the security of hash functions. (3 p)

(e) Suppose H_1 and H_2 are collision resistant hash functions mapping inputs in a set $\mathcal{M}$ to $\{0,1\}^{256}$. Show that the function $H_2(H_1(m))$ for $m \in \mathcal{M}$ is also collision resistant. (3 p)

Hint: Prove the contra-positive.

(f) We consider the possibility of using SHA-1 or MD5 for authentication as follows. Bob authenticates message m for Alice by computing $h(K\|m\|p)$ where h is the hash function, K is the secret key shared between Alice and Bob, and p is padding. Show that this system has the (unwanted) property that the Adversary can authenticate certain messages not sent by Bob. (3 p)

4 Cryptographic Protocols (9 p)

1. Let p, q two large prime numbers such that $N = p \cdot q$. Let $s \in \mathbb{Z}_N$ such that $gcd(s, N) = 1$ and it holds $v = s^2 \pmod N$.

   Peggy (the prover) and Victor (the verifier) run the following zero-knowledge protocol:

Verifier (Victor) $\mathcal{V}$		**Prover** (Peggy) $\mathcal{P}$
(N, v)		(N, s, v) s secret key pick a random $r \in \{1, 2, \ldots, N-1\}$
pick a random	$\xleftarrow{\quad w \quad}$	$w = r^2 \pmod N$
$c \in \{0, 1\}$	$\xrightarrow{\quad c \quad}$	compute
check	$\xleftarrow{\quad z \quad}$	$z = rs^c \pmod N$
$z^2 = wv^c \pmod N$		

   (a) Show that a true Peggy, following the protocol will be identified correctly by Victor. (1 p)

   (b) What is the probability that a fake Peggy (not having the secret s) to be identified correctly. Justify your answer and explain how we may decrease the success probability of a fake Peggy. (2 p)

   (c) Peggy (the prover) happens to use the same w in two different executions of the protocol. Can Victor (the verifier) learn anything about s? If yes show how. (2 p)

2. Assume that we have five parties $P_1, \cdots, P_5$ and that we tolerate $t = 2$ corrupted parties in a Shamir threshold secret sharing scheme.
   Assume that we work in $\mathbb{Z}_{11}$ and want to share the secret value $s = 6$.

   - Show how we can distribute s among five parties, *i.e.,* compute the shares $s_1, \cdots, s_5$. Each of the shares s_i is sent to the party P_i ($i \in \{1, \cdots, 5\}$) (2 p)
   - Assume that someone is given the shares s_3, s_4, s_5. Is it possible for her to compute the secret s? Show how. (2 p)