CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

17 January 2020, 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 (12 p)

(a) 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? (5 p)

(b) How do we define IND-CPA security in secret key encryption? (3 p)

(c) Prove that the CBC block cipher with predictable IV is not secure against CPA. (4 p)

Hint: Use in your description a security game and a successful strategy of the attacker in the case the attacker has access to a predictable IV.

2 Public Key Encryption (9 p)

(a) Bob receives two messages and their corresponding cipertexts, m_1, c_1 and m_2, c_2 with El Gamal encryption under the same public key:

$$Enc(m_1) = (g^{r_1}, h^{r_1} \cdot m_1)$$
$$Enc(m_2) = (g^{r_2}, h^{r_2} \cdot m_2)$$

for a cyclic group $G =< g >$ of order q and $h = g^x$, $pk = (G, g, q, h)$ and $sk = (x)$, and $r_1, r_2, x \overset{R}{\leftarrow} \mathbb{Z}_q$.

Bob does not have the secret key x used for the encryption of the messages. Can he generate a new message and the corresponding ciphertext for this message only by having access to m_1, c_1 and m_2, c_2? (3 p)

(b) How is this property called? Does textbook RSA have the same property? Explain and justify your answer. (2 p)

(c) Does this property have an effect on the security of textbook RSA and and El Gamal? Show that one of the two is susceptible to IND-CCA attacks using a security game. (4 p).

3 Data Integrity (17 p)

(a) Explain how textbook RSA can be used for digital signatures, *i.e.,* explain how to sign and how to verify the signature. (3 p)

(b) How do we define an existential forgery in digital signatures? (2 p)

(c) Bob has received from Alice two signed documents (m_1, σ_1) and (m_2, σ_2). Show that Bob can perform an existential forgery attack on textbook RSA signatures, *i.e.,* given messages, m_1, m_2, and the corresponding signatures, σ_1 and σ_2, show how to construct a new message m and a corresponding valid signature σ without having access to the key. (5 p)

Hint: Show this by describing an attacker and his strategy to win the existential forgery game against textbook RSA signatures.

(d) How can we change the way we produce RSA signatures to protect against the above existential forgery attack? Give the construction and show that the attack no longer works. (3 p)

(e) Consider that we employ a hash function (based on the Merkle-Damgård construction) to construct a MAC. More precisely it holds: $MAC(k, m) = H(k||m)$. Is this MAC construction secure against existential forgery? Prove your reasoning.

Hint: Show this by describing an attacker and his strategy to win the existential forgery game against the MAC construction. (4 p)

4 Cryptographic Protocols (12 p)

1. 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? (2 p)

   (b) Discuss how a cheating P, who does not know x, can achieve a probability of 0.5 of passing the test. (2 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. (3 p)

2. Consider that we have three parties P_1, P_2 , P_3 and each of them has a secret value $a = 4$, $b = 3$ and $c = 1$ correspondingly. Show how P_1, P_2 and P_3 using the secure multi party computation protocol for addition (that we have seen in the lectures) based on Shamir's Secret Sharing Scheme with $t = 1$ can compute the sum σ; i.e., fill in the following table. Consider that we are in $\mathbb{Z}_{11}$. (5 p)

	P_1	P_2	P_3
$a = 4$	a_1	a_2	a_3
$b = 3$	b_1	b_2	b_3
$c = 1$	c_1	c_2	c_3
$\sigma = a+b+c$	σ_1	σ_2	σ_3