CHALMERS — GÖTEBORGS UNIVERSITET

EXAM IN CRYPTOGRAPHY

TDA352 (Chalmers) - DIT250 (GU)

12 January 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 plus 6 *bonus points*.
The grades are:

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

Good luck!

1 Symmetric Ciphers (9 p)

(a) Describe in simple words how we may perform encryption and decryption using stream ciphers. (2 p)

Solution: Let $G : \{0,1\}^n \to \{0,1\}^\ell$ with $\ell \gg n$ be a secure pseudorandom generator. Then, in order to encrypt a message m with a key $k \in \{0,1\}^n$ with a stream cipher we perform: $\mathsf{Enc}(m,k) = m \oplus G(k) = c$ and in order to decrypt $\mathsf{Dec}(c,k) = c \oplus G(k) = m$.

(b) Describe how we may get a pseudorandom generator (PRG) from a pseudorandom function (PRF). (2 p)

Solution: Let $F : K \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF. Let us define $G : K \to \{0,1\}^{nt}$ as: $G(k) = F(k,0)||F(k,1)||F(k,2)||...||F(k,t)$ then G is a secure PRG.

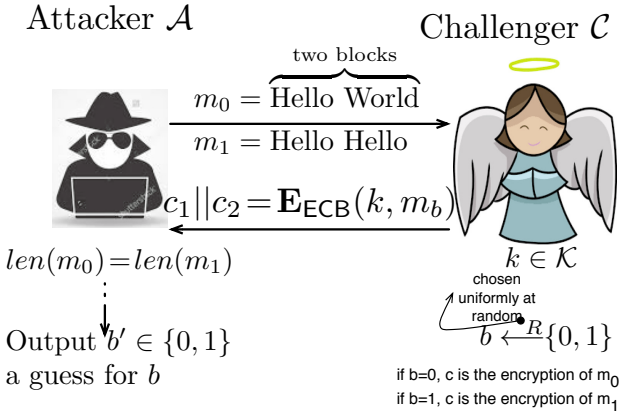
(c) Describe how encryption and decryption works in ECB (Electronic Codebook Block) mode for block ciphers. (1 p)

Solution: In ECB a message is split into blocks. Each plaintext block is encrypted using the encryption algorithm of the block cipher and the same key. To decrypt a message, the message is splitted into blocks and each block is decrypted using the decryption algorithm of the block cipher and the same secret key.

(d) Show that ECB (Electronic Codebook Block) mode for block ciphers works is not semantically secure when a message is longer than one block. (4 p)

Hint: Use in your description a security game and a successful strategy of the attacker in the case the messages used in the security game have length two blocks).

Solution:



Let W_0 be the event that $\mathcal{C}$ chooses $b = 0$, and $\mathcal{A}$ outputs $b' = 0$. Let W_1 be the event that $\mathcal{C}$ chooses $b = 1$, and $\mathcal{A}$ outputs $b' = 0$.

When $\mathcal{C}$ chooses $b = 0$, since $m_0 =$ Hello World it holds $c_1 \neq c_2$ then $b' = 0$

When $\mathcal{C}$ chooses $b = 1$, since $m_1 =$ Hello Hello it holds $c_1 = c_2$ then $b' = 1$.

$\mathcal{A}$ can output $b' = 0$ when $c_1 \neq c_2$ and $b' = 1$ when $c_1 = c_2$.

Then, we have: $|P(W_0) - P(W_1)| = |1 - 0| = 1$

Thus, ECB is not semantically secure since the advantage of the adversary is non-negligible.

2 Public Key Encryption (11 p)

(a) Describe how the El Gamal encryption scheme works. (2 p)

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

Solution:

The El Gamal encryption is composed of the following algorithms.

- $\mathbf{KeyGen}(\lambda) \rightarrow (\mathbf{pk}, \mathbf{sk})$:
  (a) generate a description of a cyclic group $G =< g >$ of order q (that is a λ-bits long integer)
  (b) choose a random value $x \in \{1, 2, \ldots, q-1\}$, and compute $h = g^x$
  (c) set: $\mathbf{pk} = (\mathbf{G}, \mathbf{g}, \mathbf{q}, \mathbf{h})$ and $\mathbf{sk} = (\mathbf{x})$
- $\mathbf{Enc}(\mathbf{pk}, \mathbf{m}) \rightarrow \mathbf{c}$ (function from G to G)
  (a) pick a random $r \in \{1, 2, \ldots, q-1\}$ and compute $\mathbf{c_1} = \mathbf{g^r}$
  (b) compute $\mathbf{c_2} = \mathbf{m} \cdot \mathbf{h^r} \in \mathbf{G}$, the ciphertext is $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2})$
- $\mathbf{Dec}(\mathbf{sk}, \mathbf{c}) \rightarrow \mathbf{m}$ (function from G to G)
  (a) compute $\mathbf{k} = \mathbf{c_1^x}$
  (b) decrypt $\mathbf{m} = \mathbf{c_2 k^{-1}} = \mathbf{c_2 c_1^{-x}}$

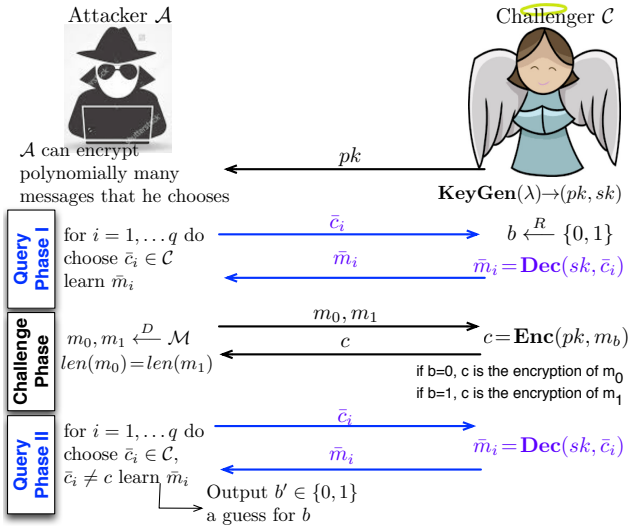
(b) What does the discrete log problem state? (2 p)

Solution: Given a cyclic group G, with generator g ($G =< g >$) and a random element $h \in G$, compute $x \in \{0, 1, \ldots, ord(G)\}$ such that $g^x = h$.

In simpler words:

Consider the function: $x \rightarrow g^x$.
The discrete log is the inverse function: $g^x \rightarrow x$. It can be denoted as: $Dlog_g(g^x) = x$

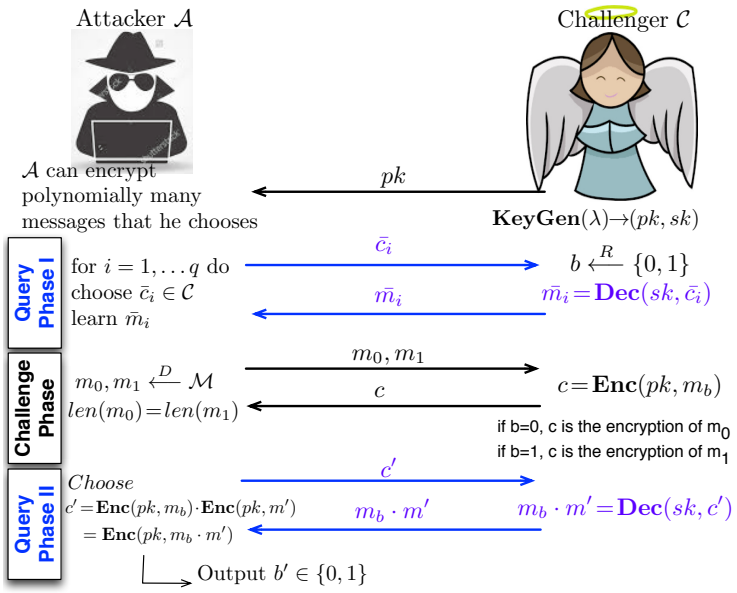
(c) *Bonus points: Give the definition of chosen-chiphertext attacks (IND-CCA) for public key encryption using a security game. (3 p)*



A public key cipher ($\mathbf{KeyGen}, \mathbf{Enc}, \mathbf{Dec}$) is secure under CCA if for any 'efficient' adversary it holds: $P(b' = b) < \frac{1}{2} + \text{negligible}$

(d) Show that El Gamal encryption is not secure against chosen chiphertext attacks (IND-CCA) (4 p)

Solution:



The attacker knows m' so he can get $\frac{m_b \cdot m'}{m'} = m_b$!

Let W_0 be the event that $\mathcal{C}$ chooses $b = 0$ and $\mathcal{A}$ outputs $b' = 0$.

Let W_1 be the event that $\mathcal{C}$ chooses $b = 1$ and $\mathcal{A}$ outputs $b' = 0$.

Then we have: $|\mathbf{P(W_0)} - \mathbf{P(W_1)}| = |\mathbf{1} - \mathbf{0}| = \mathbf{1}$.

3 Data Integrity (18 p)

(a) Describe the textbook RSA signature scheme. (2 p)

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

Solution: The RSA signature scheme is composed of three algorithms KeyGen, Sign, Verify. More precisely, it holds:

- $\mathbf{KeyGen}(\lambda) \rightarrow (\mathbf{pk}, \mathbf{sk})$
  (a) generate two distinct λ-bit primes p and q, compute $N = pq$ and $\Phi(N)$, where $\Phi(N) = (p-1)(q-1)$.
  (b) choose an integer $e \xleftarrow{R} \mathbb{Z}_{\Phi(N)}$ such that $GCD(e, \Phi(N)) = 1$ and compute its (modular) inverse $d = e^{-1} \mod \Phi(N)$.
  (c) set: $\mathbf{pk} = (N, e)$ and $\mathbf{sk} = (N, d)$
- $\mathbf{Sign}(\mathbf{sk}, \mathbf{m}) \rightarrow \sigma$: *compute* $\mathbf{m^d} \pmod{\mathbf{N}} = \sigma$
- $\mathbf{Verify}(\mathbf{pk}, \mathbf{m}) \rightarrow \mathbf{1/0}$: outputs 1 if and only if $\sigma^{\mathbf{e}} \pmod{\mathbf{N}} \stackrel{?}{=} \mathbf{m}$

(b) Show that textbook RSA signatures have the homomorphic property. (2 p)

Solution:

Let us sign two messages, m_1 and m_2 with textbook RSA (and the same key):

$$Sign(sk, m_1) = m_1^d \pmod{N}$$
$$Sign(sk, m_2) = m_2^d \pmod{N}$$

where p, q, primes $N = pq$ and $e \stackrel{?}{\leftarrow} \mathbb{Z}_{\Phi(N)}$, $GCD(e, \Phi(N)) = 1$, $d = e^{-1} \pmod{Phi(N)}$

Then it holds:

$$Sign(sk,m_1)\cdot Sign(sk,m_2) = (m_1^d \pmod N)(m_2^d \pmod N)$$
$$= (m_1\cdot m_2)^d \pmod N = Sign(sk, m_1\cdot m_2).$$

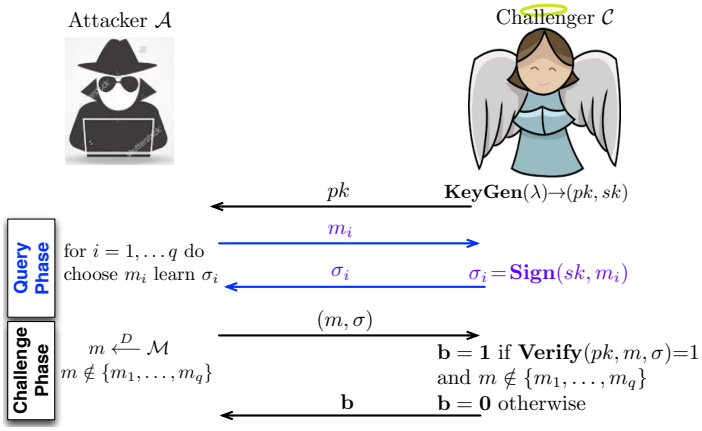
We have shown that RSA signatures have the homomorphic property *i.e.,* having the signature of two messages you can get the signature of their product **without the secret key**!

(c) *Bonus points: How do we define an existential forgery in digital signatures? (3 p)*

Hint: give the security game and formal definition.

Solution:

Let us consider the following security game.

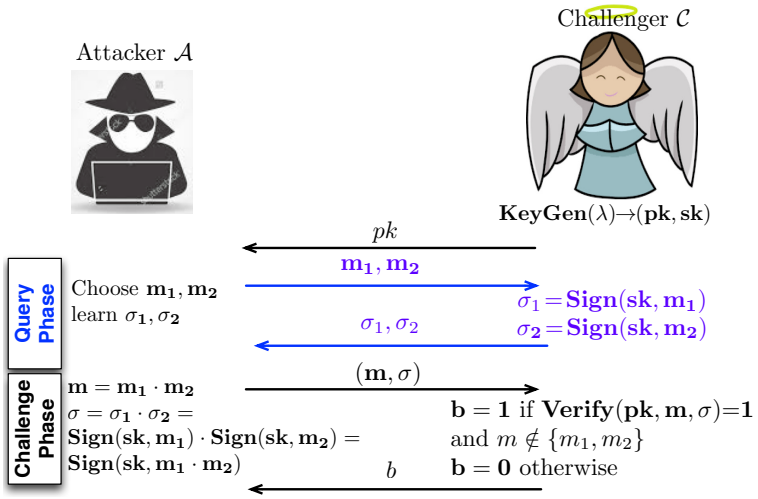


A public signature scheme (**KeyGen, Sign, Verify**) is secure, if for any efficient adversary $\mathcal{A}$ it holds: P(Challenger outputs 1) is negligible

(d) Describe an existential forgery against RSA signatures. (5 p)

Hint: an existential forgery that relies on their homomorphic property.

An existential forgery against RSA signatures can be described with the following game.



The attacker $\mathcal{A}$ is able to create a valid pair of a message m and a corresponding signature σ, using the homomorphic property of the RSA signature scheme and thus successfully create a forgery, i.e., $\mathbf{P}$(Challenger outputs 1) $= \mathbf{1}$

(e) How may we avoid this forgery? Describe a solution and explain why in this case the forgery is not possible. (3 p)

In order to avoid this forgery, insead of signing a message $\mathbf{m}$, we sign the hash of the message $\mathbf{H}(\mathbf{m})$.

Below we show why by signing the hash of the message the homomorphic property of the RSA signature does not work any more and thus we cannot perform the existential forgery.

$$\mathbf{Sign}(\mathbf{sk},\mathbf{H}(\mathbf{m_1}))\cdot\mathbf{Sign}(\mathbf{sk},\mathbf{H}(\mathbf{m_2})) = H(m_1)^d\cdot H(m_2)^d = \Big(H(m_1)\cdot H(m_2)\Big)^d$$
$$\neq \Big(H(m_1\cdot m_2)\Big)^d = \mathbf{Sign}(\mathbf{sk},\mathbf{H}(\mathbf{m_1}\cdot\mathbf{m_2}))$$

(f) Give two advantages of digital signatures in comparison to MACs (message authentication codes). (3 p)

Solution: Below we describe the main advantages of digital signatures in comparison to MACs. Any two are sufficient to get three points:

- Simpler key-distribution & key management.
- Alice needs to sign a message only once to guarantee integrity if she sends a message to multiple recipients!
- Signatures are publicly verifiable!
- Transferable signatures: Bob can convince a third party that Alice has signed a message!
- Non-repudiation: If Alice signs a message she cannot deny she has signed it.

4 Cryptographic Protocols (18 p)

(a) Let $\langle g\rangle$ be a group of order q, where q is a large prime. Let x selected uniformly at random from $\mathbb{Z}_q$ be a prover's private key, and let $X = g^x$ be the prover's public key (the verifier has the prover's public key). Peggy (the prover) and Victor (the verifier) run the following zero-knowledge protocol:

Verifier $\mathcal{V}$		**Prover $\mathcal{P}$**
		x secret key
X		$X = g^x$
		$r \in \{1,2,\ldots,q-1\}$
	$\xleftarrow{R}$	$R = g^r$
$c \in \{1,2,\ldots,q-1\}$	$\xrightarrow{c}$	
$R \stackrel{?}{=} g^s \cdot X^{-c}$	$\xleftarrow{s}$	$s = (r + c\cdot x) \bmod q$

i. Show that a true Peggy, following the protocol will be identified correctly by Victor. (2 p)
Solution: It holds:

$$g^s \cdot X^{-c} = g^{(r+c\cdot x)}\cdot (g^x)^{-c} = g^r = R.$$

So a true Peggy that follows the protocol will be identified correctly by Victor.

ii. Can Victor transfer his knowledge, that indeed Peggy has the secret x, to someone else? Explain why. (2 p)
Solution:
No! $\mathcal{V}$ could have produced (R,c,s) by generating c and s at random and computing $R = g^s X^{-c}$.

iii. Peggy (the prover) happens to use the same R in two different executions of the protocol. Can Victor (the verifier) learn anything about x? If yes, show how. (3 p)
Solution: Yes, by using the equation: $R = g^s \cdot X^{-c} = g^{s'} \cdot X^{-c'}$
Indeed it holds:
$R = g^s \cdot X^{-c} = g^{s'} \cdot X^{-c'} \Leftrightarrow$
$g^s \cdot (g^x)^{-c} = g^{s'} \cdot (g^{x\prime})^{-c'} \Leftrightarrow$
$s + x(-c) = s' + x(-c') \bmod q \Leftrightarrow x = \frac{s-s'}{c-c'} \bmod q$

(b) Consider that we have three parties P_1, P_2, P_3 and each of them has a secret value $a = 3$, $b = 5$ and $c = 2$ correspondingly. We are using the secure multi party computation (SMPC) protocol for addition (that we have seen in the lectures) based on Shamir's Secret Sharing Scheme with $t = 1$.

i. Show how P_1, P_2 and P_3 can distribute shares of their secrets a, b, c to each other and compute the shares of the sum $\sigma = a + b + c$ *i.e.,* fill in the following table. (3 p)

	P_1	P_2	P_3
$a = 3$	a_1	a_2	a_3
$b = 5$	b_1	b_2	b_3
$c = 2$	c_1	c_2	c_3
$\sigma = a+b+c$	σ_1	σ_2	σ_3

Solution: Since $t = 1$ each of the P_1, P_2, P_3 selects a polynomial of degree 1, the only restrictions is that each if $p_1(x)$ is the polynomial by the party P_1 then it should hold $p_1(0) = 3$. Similarly for the other two polynomials it should hold: $p_2(0) = 5$ and $p_3(0) = 2$.
More precisely, lets assume that P_1 selects the polynomial: $p_1(x) = 3 + 2x$. Then, we we have:

$$p_1(1) = 3 + 2 \cdot 1 = 5 = a_1$$
$$p_1(2) = 3 + 2 \cdot 2 = 7 = a_2$$
$$p_1(3) = 3 + 2 \cdot 3 = 9 = a_3$$

Lets assume that P_2 selects the polynomial $p_2(x) = 5 - x$. Then, we have:

$$p_2(1) = 5 - 1 = 4 = b_1$$
$$p_2(2) = 5 - 2 = 3 = b_2$$
$$p_2(3) = 5 - 3 = 2 = b_3$$

Lets assume that $\mathrm{P}_3 selects the polynomial \mathrm{p}_3(x) = 2 + x$. Then, we have:

$$p_3(1) = 2 + 1 = 3 = c_1$$
$$p_3(2) = 2 + 2 = 4 = c_2$$
$$p_3(3) = 2 + 3 = 5 = c_3$$

Then, the shares of the sum σ_1, σ_2 and σ_3 can be calculated as follows:

$$\sigma_1 = a_1 + b_1 + c_1 = 12$$
$$\sigma_2 = a_2 + b_2 + c_2 = 14$$
$$\sigma_3 = a_3 + b_3 + c_3 = 16$$

Thus, the table filled in looks as follows:

	P_1	P_2	P_3
$a = 3$	5	7	9
$b = 5$	4	3	2
$c = 2$	3	4	5
$\sigma = a+b+c$	12	14	16

ii. Show how P_1, P_2, P_3 using the shares σ_1, σ_2 and σ_3, can compute the sum σ. (4 p)
Solution: First, we show how to compute

$$\delta_i(0) = \prod_{j=\{1,2,3\}\setminus\{i\}} \frac{j}{j-i} \text{ for } i = \{1,2,3\}$$

It holds:

$$\delta_1(0) = \frac{2}{2-1} \cdot \frac{3}{3-1} = 2 \cdot \frac{3}{2} = 3$$

$$\delta_2(0) = \frac{1}{1-2} \cdot \frac{3}{3-2} = -3$$

$$\delta_3(0) = \frac{1}{1-3} \cdot \frac{2}{2-3} = \frac{1}{-2} \cdot \frac{2}{-1} = 1$$

Thus, we have:

$$\begin{aligned}\sigma &= \delta_1(0) \cdot \sigma_1 + \delta_2(0) \cdot \sigma_2 + \delta_3(0) \cdot \sigma_3 \\ &= 3 \cdot 12 - 3 \cdot 14 + 1 \cdot 16 = 36 - 42 + 16 = 10\end{aligned}$$

Indeed this is correct since $\sigma = a + b + c = 10$.

iii. Consider that P_3 decides not to announce his share σ_3 and thus P_1 and P_2 collaborate announcing σ_1 and σ_2. Is it still possible to compute the sum σ? If yes, justify why and show how. (4 p)
Solution: Indeed since $t = 1$ two parties are sufficient in order to compute σ.
Since only P_1 and P_2 collaborate we compute

$$\delta_i(0) = \prod_{j=\{1,2\}\setminus\{i\}} \frac{j}{j-i} \text{ for } i = \{1,2\}$$

.
It holds:

$$\delta_1(0) = \frac{2}{2-1} = 2$$

$$\delta_2(0) = \frac{1}{1-2} = -1$$

Thus, we have: $\sigma = \delta_1(0) \cdot \sigma_1 + \delta_2(0) \cdot \sigma_2 = 2 \cdot 12 - 1 \cdot 14 = 10$
Indeed this is correct since $\sigma = a + b + c = 10$.