CRYPTOGRAPHY and SECURITY, exam Feb 2023, preparation tasks

Problem 1 Smart-ID: assume the Estonian citizen Helger. His public key is $n = n_1 \cdot n_2$. The private key is d_1', n_1 on the side of Helger's signing device, and d_1'', n_1, d_2, n_2 on the side of the authority (so $d_1 = d_1' + d_1''$ is the secret exponent corresponding to n_1).

Assume that the same RSA number n_1 has been chosen for Erika (due to some wrong setting of PRNG). In this situation, can Helger forge signatures of Erika?

Problem 2 Recall the concept of differential privacy and consider a database with salaries of employees. The algorithm A simply returns a median salary (with no name of the employee).

Does it satisfy the condition of differential privacy?

Problem 3 Modify slightly the definition of TOR. Establishing a shared key between the sender and an intermediate node A on the path is in with Diffie-Hellman key exchange protocol but with Static DH protocol.

Evaluate security consequences of this decision.

Problem 4 Consider the first padding attack we have discussed during the lecture. We have used the fact that padding bytes are added on the end of the message.

What about moving the padding to front of the message? Does it help to resist the attack?

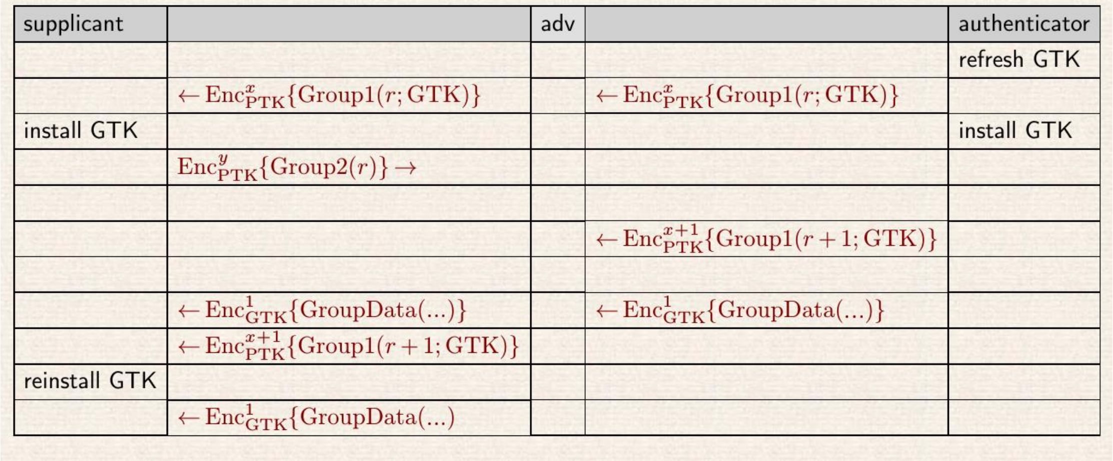
Problem 5 Recall the LINUX access rights system for the files (for each file we have an owner, access right are r(ead), w(rite), (e)x(ecute), there are defined groups and a group containing all users).

Express a concrete situation in terms of NGAC policy.

Problem 6 If a new member joins the group of an Access Point, it is necessary to renew the group key (otherwise the new member would be able to understand the old broadcast messages of the AP, and this is not that we want).

AP has to inform all group member about the change and the new group key GTK must be given to them. But what is the moment to **install** GTK? As in the problem of Byzantine generals – we do not know whether the message informing about the change of the group key has been received by each group member.

The following picture shows an attack for the case where the new group key GTK is installed immediately by the authenticator (AP) and the supplicant (user device). What is the problem in this scenario and why are the messages accepted?



supplicant		adv		authenticator
				refresh GTK
	$\leftarrow \mathrm{Enc}^{x}_{\mathrm{PTK}}\{\mathrm{Group1}(r;\mathrm{GTK})\}$		$\leftarrow \mathrm{Enc}^{x}_{\mathrm{PTK}}\{\mathrm{Group1}(r;\mathrm{GTK})\}$	
install GTK				install GTK
	$\mathrm{Enc}^{y}_{\mathrm{PTK}}\{\mathrm{Group2}(r)\} \rightarrow$			
			$\leftarrow \mathrm{Enc}^{x+1}_{\mathrm{PTK}}\{\mathrm{Group1}(r+1;\mathrm{GTK})\}$	
	$\leftarrow \mathrm{Enc}^{1}_{\mathrm{GTK}}\{\mathrm{GroupData}(\ldots)\}$		$\leftarrow \mathrm{Enc}^{1}_{\mathrm{GTK}}\{\mathrm{GroupData}(\ldots)\}$	
	$\leftarrow \mathrm{Enc}^{x+1}_{\mathrm{PTK}}\{\mathrm{Group1}(r+1;\mathrm{GTK})\}$			
reinstall GTK				
	$\leftarrow \mathrm{Enc}^{1}_{\mathrm{GTK}}\{\mathrm{GroupData}(\ldots)$			