Security M1 – Examen (2h)

Guillaume Scerri, guillaume.scerri@lmf.cnrs.fr

12 January 2026

All paper documents are allowed. Internet connected devices are not allowed. The number of stars after a question roughly denotes difficulty (and thus number of points).

1 A protocol

Consider the following protocol, where a and b are secrets of agents A and B, keys $\mathsf{pk}(a)$ and $\mathsf{pk}(b)$ are public (i.e. initially known to the attacker), and n is a nonce generated by A:

- $A \to B$: $\mathsf{aenc}(n, \mathsf{pk}(b))$
- $B \to A$: $\mathsf{aenc}(n, \mathsf{pk}(a))$

The goal of the protocol is for A to ensure that B has correctly received n (a sort of one way key exchange). The naive idea is that A sends a first message containing a secret n. Upon receipt of a message of the form $\mathsf{aenc}(y, \mathsf{pk}(b))$, B obtains n and sends back the last message to A as an acknowledgment.

Question 1 (*)**.** Provide a pi-calculus process $A(n, a, \mathsf{pk}(b))$ modeling A, and $B(b, \mathsf{pk}(a))$ modelling a version of B that is only willing to talk to A, assuming that both A and B know $\mathsf{pk}(a)$ and $\mathsf{pk}(b)$. You may use pattern matching for binding variables.

In the remainder of this exercise, we model messages as terms built over variables $\mathcal{X}$, and names $\mathcal{N}$ with

- constructors $\mathsf{aenc}/2$, $\langle . , . \rangle/2$, $\mathsf{pk}/1$;
- destructors adec, $\pi_1/1$, $\pi_2/1$;
- rewrite rules $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) \to x$ and $\pi_i(\langle x_1 , x_2 \rangle) \to x_i$.

Question 2 (*)**.** Assume that B binds its internal representation of n to x_n, provide a trace where $x_n \neq n$.

Question 3 (*)**.** Give a security property formalizing the fact that the adversary cannot guess n if B succeeds. You may modify the process from Question 1 in order to add the relevant events.

Question 4 (*)**.** Give a security property formalizing the fact that if B accepts, A and B agree on the value of n. You may modify the process from Question 1 in order to add the relevant events.

Question 5 (*)**.** Give all symbolic executions of the process $A(n, a, \mathsf{pk}(b)) \| B(b, \mathsf{pk}(a))$.

Question 6 (*)**.** Prove that the process $A(n, a, \mathsf{pk}(b)) \| B(b, \mathsf{pk}(a))$ ensures secrecy of n. You may use symbolic execution from the previous question.

Consider now the following modfication of the protocol where B is willing to answer queries from anyone.

- $A \to B$: $\mathsf{aenc}(\langle n\,,\, pk(a)\rangle, \mathsf{pk}(b))$
- $B \to A$: $\mathsf{aenc}(n, \mathsf{pk}(a))$

Question 7 (*)**.** Provide processes $A(n, a, \mathsf{pk}(b))$ and $B(b)$ modelling this new protocol.

Question 8 (**)**.** Prove that the process $A(n, a, \mathsf{pk}(b)) \| B(b)$ ensures secrecy of n. You may use symbolic execution to caracterise all possible traces of these processes.

Question 9 (***)**.** Prove that the process $\|^i A(n, a, \mathsf{pk}(b)) \| \|^j B(b)$ ensures secrecy of n_0.
Hint: You may want to give an invariant on the shape of messages in the knowledge of the adversary that is stable by one action of A of B.

We now assume that the encryption is malleable, i.e., we add to our model the function $\mathsf{mal}/2$ and the rewrite rule $\mathsf{mal}(\mathsf{aenc}(\langle x\,,\, y\rangle, z), t) \to \mathsf{aenc}(\langle x\,,\, t\rangle, z)$.

Question 10 (***)**.** Show that intruder deduction is still decidable in this model.

Question 11 (*)**.** Provide a trace of the process $A(n, a, \mathsf{pk}(b)) \| B(b)$ where n is deducible by the adversary.

2 Computational model

Definition 1. *A function f is* negligible *if for any polynomial p, there exists N such that for all $\eta \geq N$ we have $f(\eta) \leq \frac{1}{p(\eta)}$.*

In this section, we say say that a scheme is secure for a game, is the advantage for the corresponding game is negligible in the security parameter η for any probabilistic polynomial time (in η) adversary.

Definition 2 ($\mathtt{IND-CPA}$ security game)**.** *The attacker must distinguish between two scenarios (the variations between those two scenarios are parametrized by a boolean b).*

- *First, compute pair a key (k) from $\mathcal{K}(\eta)$.*
- *Then, the adversary gets access to an oracle $\mathcal{O}^b_{\mathtt{IND-CPA}}$ and returns a boolean b'. This oracle is defined as such (with r being some fresh randomness at every call)*

$$\mathcal{O}^b_{\mathtt{IND-CPA}}(m_0, m_1) = \begin{cases} \{m_b\}^r_{\mathsf{pk}(k)} & \textit{if } |m_0| = |m_1| \\ \textbf{error} & \textit{otherwise} \end{cases}$$

The advantage of an adversary $\mathcal{A}$ against the $\mathtt{IND-CPA}$ game is

$$\mathbf{Adv}^{\eta}_{\mathtt{IND-CPA}}(\mathcal{A}) = \left| \begin{array}{l} \mathbf{Pr}_r\Big[(k) \leftarrow \mathcal{K}(1^\eta) : \mathcal{A}^{\mathcal{O}^0_{\mathtt{IND-CPA}}}(\mathsf{pk}(k)) = 0\Big] \\ -\mathbf{Pr}_r\Big[(k) \leftarrow \mathcal{K}(1^\eta) : \mathcal{A}^{\mathcal{O}^1_{\mathtt{IND-CPA}}}(\mathsf{pk}(k)) = 0\Big] \end{array} \right|$$

Question 12 (*). Define a cryptographic game ensuring formalizing the fact that an adversary interacting with an encryption oracle is unlikely to guess an encrypted random value $\{n\}^r_{\mathsf{pk}(k)}$ (provided to the adversary at the start of the game).

Question 13 (**). Prove that an $\mathtt{IND} - \mathtt{CPA}$ scheme also satisfies the game defined in Question 12.

Question 14 (*). Prove that if the encryption scheme satisfies $\mathtt{IND} - \mathtt{CPA}$ then the process $A(n, a, \mathsf{pk}(b))$ ensures secrecy of n (you may use the previous question's result).

Question 15 (**). Does the $\mathtt{IND} - \mathtt{CPA}$ assumption ensure that n is secret in $A(n, a, \mathsf{pk}(b)) \| B(b, \mathsf{pk}(a))$? Why?