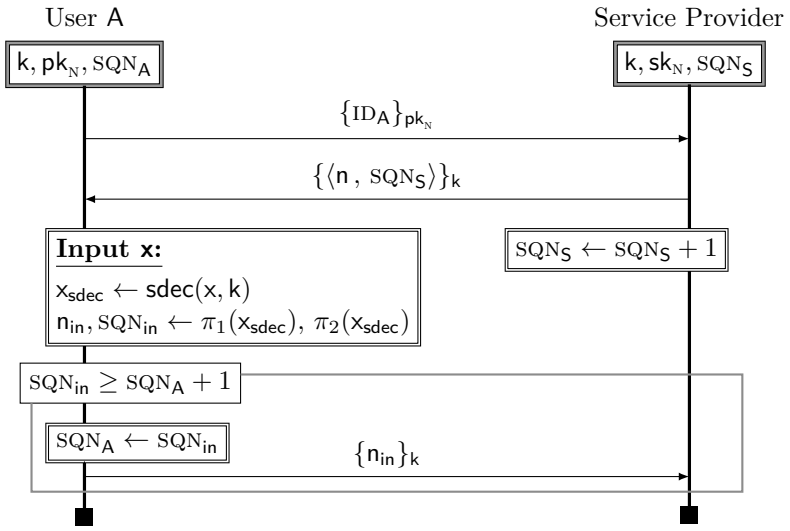
TD 3: Deduction system for the symbolic setting

Margot Catinaud margot.catinaud@lmf.cnrs.fr

Exercise 1 (AKA-)

Consider the following protocol :



1. Give a set of function symbols, rewriting rules and equational theory that captures all primitives needed for this protocol.
2. Write it down formally all the agents in the process calculus in the case where there is only one user and one session by user.
3. Write it down formally all the agents in the process calculus in the case where there is multiple users and one session by user.
4. Add **store**$(cell, t)$ and **get**$(x, cell)$ constructs to your process calculus and propose a semantics capturing the intuitive meaning of this constructs for manipulating global states.
5. Write it down formally all the agents in the process calculus in the case where there is multiple users and multiple sessions by user.
6. Express the following security properties:
   (a) If the Service Provider S accepts then A and S agree on $\mathsf{n_{in}}$;
   (b) If the Service Provider S accepts then there is exactly one matching session of user A ;
   (c) We always have $\mathrm{SQN}_\mathsf{S} \geqslant \mathrm{SQN}_\mathsf{A}$;
   (d) The user A never accepts the same token $\{\langle \mathsf{n}\,,\, \mathrm{SQN}_\mathsf{S}\rangle\}_\mathsf{k}$ twice.

Exercise 2 (Unification)

For each pair of terms, check if those are unifiable or not (find a most general unifier if possible).
Here, b and a are function symbols.

1. $\langle x\,,\, \mathsf{b}\rangle$ and $\langle \mathsf{a}\,,\, x\rangle$
2. $\langle \mathsf{b}\,,\, x\rangle$ and $\langle \mathsf{a}\,,\, y\rangle$
3. $\{x\}_\mathsf{a}$ and $\{\mathsf{b}\}_x$
4. $\langle x\,,\, y\rangle$ and $\langle\langle y\,,\, y\rangle\,,\, x\rangle$
5. $\langle \mathsf{a}\,,\, y\rangle$ and $\langle\langle y\,,\, y\rangle\,,\, \mathsf{a}\rangle$
6. z and $\langle x\,,\, y\rangle$

Exercise 3 (A first deduction system)

Consider the following deduction system:

$$\frac{x \quad y}{\langle x\,,\,y\rangle} \qquad \frac{\langle x\,,\,y\rangle}{x} \qquad \frac{\langle x\,,\,y\rangle}{y}$$

$$\frac{x \quad y}{\{x\}_y} \qquad\qquad \frac{\{x\}_y \quad y}{x}$$

1. Give the signature used by this deduction system? Is the encryption symmetric or asymmetric?

Consider the set of terms:

$$\mathsf{T} = \left\{\{\mathsf{s}\}_{\langle \mathsf{k}_1\,,\,\mathsf{k}_2\rangle},\ \{\mathsf{k}_1\}_{\mathsf{k}_3},\ \mathsf{k}_3,\ \mathsf{k}_2\right\}$$

2. Enumerate all the subterms of T
3. the term s is deducible from T. Give a derivation witnessing this fact.
4. Among the subterms of T, give those that are deducible.
5. Give a term u that is not a subterm of T and such that $\mathsf{T} \vdash \mathsf{u}$

Exercise 4 (Various Primitives)

For each primitive, give a set of deduction rules that represent the primitive. (You can assume that you have the pair and booleans in your signature if you wish)

1. *Symmetric encryption:* the corresponding signature is $\{\mathsf{senc}/2,\ \mathsf{sdec}/2\}$.
2. *Asymmetric encryption:* the corresponding signature is $\{\mathsf{aenc}/2,\ \mathsf{adec}/2,\ \mathsf{pk}/1\}$.
3. *Signature:* the corresponding signature is $\{\mathsf{sign}/2, \mathsf{verify}/3, \mathsf{signkey}/1\}$.
4. *Authenticated Encryption with Associated Data:* the corresponding signature is $\{\ \mathsf{enc}_{\mathsf{aead}}/3, \mathsf{dec}_{\mathsf{aead}}/3\}$.

Exercise 5 (Bonus exercise – Strong secrecy)

Consider a protocol between two parties A and B exchanging some name s. In this exercise, we will propose a statement for the strong secrecy of s viewed as a trace property. Intuitively, the *strong secrecy of s* property means that no adversarial test, *i.e.* adversarial computation on the frame with a boolean output, can be true on s and false on a fresh new value.

Hint: You will need a helper process that will perform the test and your term algebra need to be able to represent all adversarial tests.