Cryptographic protocols: formal and computational proofs
Mid Term exam

December 2, 2015
Duration 3h. All documents are allowed

Problem

We consider the following (informally described) handshake protocol

$$\begin{array}{ll} A \to B: & \nu n, \nu r, \nu s. \{\langle n, \langle s, A \rangle\rangle\}_k^r \\ B \to A: & \nu n'. \langle n, n' \rangle \\ A \to B: & \nu r'. \{\langle s, n' \rangle\}_k^{r'} \end{array}$$

in which k is a shared key between A, B.

1. Give a reasonable definition of the processes $P_A(a)$ and $P_B(a)$, in which a plays the role A (this is checked by the process P_B)
2. We wish to check the agreement property on the nonce n. Include in the above processes the appropriate events and state formally the agreement property.
3. We consider the scenario $\nu k.(P_A(a) \| P_B(a))$ in a context, in which the initial attacker's knowledge is only $\{a\}$.
   (a) Explain why complete traces of the above process (i.e., traces with 3 input actions and 3 output actions) must correspond to the following sequence of actions: 1. output of P_A 2. input of P_B 3. output of P_B 4. input of P_A 5. output of P_A 6. input of P_B.
   (b) Compute the deducibility constraint representing all possible complete traces.
   (c) Solve the above deducibility constraints.
   (d) List all possible attacks on the agreement property that was stated in the previous question. (Justify that there is no other attack)
   (e) Show that there is no attack on the secrecy of s in this scenario.
   (f) Show an attack on the secrecy of s in the scenario $\nu k.(P_A(a) \| P_B(a) \| P_B(a))$.
4. Give a Horn clause translation $\mathcal{H}$ of $\nu k.(P_A(a) \| P_B(a))$.
5. Show how the attacker clauses, together with $\mathcal{H}$, allow to deduce $\mathtt{Att}(s)$.
6. In the senario $\nu k.(P_A(a) \| P_B(a))$ is there any attack on the agreement on n' ?

7. (**Bonus**) What are the possible attacks on the agreement on n (resp. n') in a scenario $\nu k.(!P_A(a) \parallel !P_B(a))$?

8. (**Bonus**) Assume the encryption scheme is IND-CPA, do we get more attacks in the computational semantics ?

Exercise 2

We assume here that the encryption scheme is IND-CPA. k_1, k_2, k_3, r, r' are arbitrary distinct names. u, v are arbitrary terms.
Which of the following are true ? false (at least for some IND-CPA encryption schemes) ? Justify your answer.

1. $[\![\{k_1\}_{k_2}^r, \{\langle k_1, k_2\rangle\}_{k_3}^{r'}, k_1]\!] \approx [\![\{k_2\}_{k_1}^r, \{\langle k_1, k_2\rangle\}_{k_3}^{r'}, k_1]\!]$
2. $[\![\{k_2\}_{k_1}^r, \{\langle k_1, k_3\rangle\}_{k_2}^{r'}, k_1]\!] \approx [\![\{k_2\}_{k_1}^r, \{\langle k_2, k_3\rangle\}_{k_2}^{r'}, k_1]\!]$
3. $[\![\{k_2\}_{k_1}^r, \{\langle k_1, k_2\rangle\}_{k_1}^{r'}, k_2]\!] \approx [\![\{k_2\}_{k_1}^r, \{\langle k_2, k_3\rangle\}_{k_2}^{r'}, k_3]\!]$
4. $[\![\{\{u\}_{k_1}^r\}_{k_2}^{r'}]\!] \approx [\![\{\{u\}_{k_1}^r\}_{k_1}^{r'}]\!]$

Exercise 3

If a symmetric encryption scheme uses the specific BC mode, we assume that it is possible to compute $\{u\}_k^r$ from $\{\langle v, u\rangle\}_k^r$ (for all u, v, k, r).

Give an example of a protocol, a scenario and a (weak) secrecy property, which is secure in the Dolev-Yao model, but insecure for a symmetric encryption scheme using such a BC mode.

Problem

1. $P_A(a) = \nu n, \nu s, \nu r, \nu r'.\mathtt{out}(\{\langle n, \langle s, a\rangle\rangle\}_k^r).\mathtt{in}(y).\mathsf{if}\ \pi_1(y) = n\ \mathsf{then}\ \mathsf{out}(\{\langle s, \pi_2(y)\rangle\}_k^{r'})$

   $P_B = \nu n'.\mathtt{in}(x).\ \mathsf{let}\ y_n = \pi_1(\mathsf{dec}(x,k))\ \mathsf{in}\ \mathsf{out}(\langle y_n, n'\rangle).\mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK.$

2. $P_A(a) = \nu n, \nu s, \nu r, \nu r'.\mathtt{out}(\{\langle n, \langle s, a\rangle\rangle\}_k^r.\mathtt{in}(y).\mathsf{if}\ \pi_1(y) = n\ \mathsf{then}\ \mathsf{ev}a(n).\mathsf{out}(\{\langle s, \pi_2(y)\rangle\}_k^{r'})$

   $P_B = \nu n'.\mathtt{in}(x).\ \mathsf{let}\ y_n = \pi_1(\mathsf{dec}(x,k))\ \mathsf{in}\ \mathsf{ev}b(y_n).\mathsf{out}(\langle y_n, n'\rangle).\mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK.$

   Agreement: $\mathsf{ev}a(x) \Rightarrow \mathsf{ev}b(x)$.

   Comment: in the student's answers, the events are often misplaced, yielding either a trivially unsatisfiable security property (the attacker may always cheat) or a very strong agreement property, because the agreement is required, even when a has not checked n in B's reply.

3. (a) Let $P = P_A(a) \parallel P_B$. Consider $(\phi_0, P, \emptyset)$ be the initial configuration.
   First observe that, if ϕ is a frame that does not contain the key k, then, for every u, $\phi \not\vdash \{u\}_k^r$. Therefore, if $\phi \vdash m$, then $\mathsf{dec}(m,k)$ is irreducible.
   There are, a priori, two possible transitions from the initial configuration (output of A or input of B). Let us show that the latter yields a dead-end.

$$\begin{array}{lll}(\phi_0, P, \emptyset) & \to & (\nu n'.\phi_0, \quad P_A(a) \| \ \mathsf{let}\ y_n = \pi_1(\mathsf{dec}(m,k))\ \mathsf{in}\ \mathsf{out}(\langle y_n, n'\rangle). \\ & & \qquad \mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK.\end{array}$$

where $\phi_0 \vdash m$. Then y_n is bound to $\pi_1(\mathsf{dec}(m,k))$. There are again two possible moves:

$$\begin{array}{lll}(\phi_0, P, \emptyset) & \to & (\nu n'.\phi_0, \quad P_A(a) \| \ \mathsf{let}\ y_n = \pi_1(\mathsf{dec}(m,k))\ \mathsf{in}\ \mathsf{out}(\langle y_n, n'\rangle). \\ & & \qquad \mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK. \\ & \to & (\nu n'.\phi_0, \langle \pi_1(dec(m,k)), n'\rangle, P_A(a) \| \\ & & \qquad \mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK.\end{array}$$

and

$$\begin{array}{lll}(\phi_0, P, \emptyset) & \to & (\nu n'.\phi_0, \quad P_A(a) \| \ \mathsf{let}\ y_n = \pi_1(\mathsf{dec}(m,k))\ \mathsf{in}\ \mathsf{out}(\langle y_n, n'\rangle). \\ & & \qquad \mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK. \\ & \to & (\nu n'.\phi_0, \langle \pi_1(dec(m,k)), n'\rangle, \quad P_1 \| \\ & & \qquad \mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK.\end{array}$$

where $P_1 = \mathtt{in}(y).\mathsf{if}\ \pi_1(y) = n\ \mathsf{then}\ \mathsf{ev}a(n).\mathsf{out}(\{\langle s, \pi_2(y)\rangle\}_k^{r'})$
In order to complete one of these traces, we need to deduce a message m' such that $\pi_1(\mathsf{dec}(m',k)) = \pi_1(\pi_2(\mathsf{dec}(m,k)))$ or such that $\pi_1(m'') = n$. In both cases, the frames are contained in $\phi = \phi_0, \langle \pi_1(dec(m,k)), n'\rangle, \{\langle n, \langle s, a\rangle\rangle\}_k^r$. However, $\phi \not\vdash n$, hence, for every m'' such that $\pi_1(m'')$, $\phi \not\vdash m''$. Furthermore, the only message m' that can be computer from ϕ and decrypted with k is $\{\langle n, \langle s, a\rangle\rangle\}_k^r$, for wich $\pi_1(\mathsf{dec}(m',k)) = n \neq \pi_1(\pi_2(\mathsf{dec}(m,k)))$. Finally, if m' cannot be decrypted by k,

the two messages $\pi_1(\mathsf{dec}(m', k))$, $\pi_1(\pi_2(\mathsf{dec}(m, k)))$ are irreducible and distinct. In all cases the process is stuck.

It follows that the first action in a complete trace is an output of A. The second action cannot be an input of A because $a, \{\langle n, \langle s, a\rangle\rangle\}_k^r \not\vdash n$. It is therefore an input of B, followed by an output of B (for the same reason, the input of A is not possible before the output of B).

Now, we got out A; in B; out B. Remains two choices: in A or in B. in B requires a message, which is encrypted by k and whose plaintext contains n'. The frame does not contain any such message and there is not way to construct new encryptions with k.

Therefore, the next action must be an input of A, followed by an output of A: we have the desired sequence of actions.

Comments: I did not require such a detailed explanation. A 10-15 lines explanation providing with the correct arguments was OK. However, many explanations were incorrect or too short.

(b) For the only sequence of actions that we have:

$$\left\{\begin{array}{rcl} a, \{\langle n, a\rangle\}_k^r & \overset{?}{\vdash} & \{\langle y_n, a\rangle\}_k^{z'} \\ \phi_0, \{\langle n, a\rangle\}_k^r, \langle y_n, n'\rangle & \overset{?}{\vdash} & \langle n, y'\rangle \\ \phi_0, \{\langle n, a\rangle\}_k^r, \langle y_n, n'\rangle, \{\langle s, y'\rangle\}_k^{z''} & \overset{?}{\vdash} & \{\langle s, n'\rangle\}_k^{z'''} \end{array}\right.$$

(c) We may focus on the first constraint first, for which there are only two possible rule applications, yielding respectively:

$$\left\{\begin{array}{rcl} & y_n = n \wedge z' = r & \\ a, \{\langle n, a\rangle\}_k^r, \langle n, n'\rangle & \overset{?}{\vdash} & \langle n, y'\rangle \\ a, \{\langle n, a\rangle\}_k^r, \langle n, n'\rangle, \{\langle s, y'\rangle\}_k^{z''} & \overset{?}{\vdash} & \{\langle s, n'\rangle\}_k^{z'''} \end{array}\right.$$

$$\left\{\begin{array}{rcl} a, \{\langle n, a\rangle\}_k^r & \overset{?}{\vdash} & \langle y_n, a\rangle \\ a, \{\langle n, a\rangle\}_k^r & \overset{?}{\vdash} & k \\ a, \{\langle n, a\rangle\}_k^r & \overset{?}{\vdash} & z' \\ a, \{\langle n, a\rangle\}_k^r, \langle y_n, n'\rangle & \overset{?}{\vdash} & \langle n, y'\rangle \\ a, \{\langle n, a\rangle\}_k^r, \langle y_n, n'\rangle, \{\langle s, y'\rangle\}_k^{z''} & \overset{?}{\vdash} & \{\langle s, n'\rangle\}_k^{z'''} \end{array}\right.$$

The second system has no solution, because the second constraint reduces to $\perp$.

Consider therefore the first one. There are, a priori, 3 possible rules applications, yielding respectively

$$\mathcal{C}_1 = \left\{\begin{array}{rcl} & y_n = n \wedge z' = r \wedge y' = a & \\ a, \{\langle n, a\rangle\}_k^r, \langle n, n'\rangle & \overset{?}{\vdash} & \langle n, a\rangle \\ a, \{\langle n, a\rangle\}_k^r, \langle n, n'\rangle, \{\langle s, a\rangle\}_k^{z''} & \overset{?}{\vdash} & \{\langle s, n'\rangle\}_k^{z'''} \end{array}\right.$$

$$\mathcal{C}_2 = \begin{cases} y_n = n \wedge z' = r \wedge y' = n' \\ a, \{\langle n,a\rangle\}_k^r, \langle n,n'\rangle \stackrel{?}{\vdash} \langle n,n'\rangle \\ a, \{\langle n,a\rangle\}_k^r, \langle n,n'\rangle, \{\langle s,n'\rangle\}_k^{z''} \stackrel{?}{\vdash} \{\langle s,n'\rangle\}_k^{z'''} \end{cases}$$

$$\mathcal{C}_3 = \begin{cases} y_n = n \wedge z' = r \\ a, \{\langle n,a\rangle\}_k^r, \langle n,n'\rangle \stackrel{?}{\vdash} y' \\ a, \{\langle n,a\rangle\}_k^r, \langle n,n'\rangle, \{\langle s,y'\rangle\}_k^{z''} \stackrel{?}{\vdash} \{\langle s,n'\rangle\}_k^{z'''} \end{cases}$$

We have now to consider the last constraint of the systems:

- for $\mathcal{C}_1$, there is no applicable rule: $\mathcal{C}_1$ has no solution.
- for $\mathcal{C}_2$ we get $z'' = z'''$ and then the system is solved.
- for $\mathcal{C}_3$, all rules force $y' = n'$ and we are back to the previous system.

In summary, there is only one possible solved form: $y_n = n \wedge z' = z'' \wedge z' = r \wedge y' = n'$.

(d) There is no attack on the agreement for this scenario, since $\mathsf{ev}a(n)$ occurs only in a completed trace, in which $\mathsf{ev}b(y_n)$ also occurs. Furthermore, as we have seen, we must have $y_n = n$.

And, for incomplete traces, we have even fewer solutions to the constraint system.

(e) There is an attack on the secrecy of s if there is an execution that yields a frame ϕ, from which we can deduce s. From the question 3c, any complete trace yields the frame $a, \{\langle n,a\rangle\}_k^r, \langle n,n'\rangle, \{\langle s,n'\rangle\}_k^{r'}$. It is not possible to deduce s from this frame.

All other frames that would emerge from incomplete traces are even shorter, therefore we cannot deduce s either from these frames.

(f) Attack in the cas of $P_A(a)\|P_B(a)\|P_B(a)$:

$$\begin{array}{lll} ((a), P) & \to & ((a, \{\langle n, \langle s,a\rangle\rangle\}_k^r), P_1\|P_B\|P_B) \\ & \to^2 & ((a, \{\langle n, \langle s,a\rangle\rangle\}_k^r), \langle n,n'\rangle), P_1\|P_2\|P_B) \\ & \to & ((a, \{\langle n, \langle s,a\rangle\rangle\}_k^r), \langle n,n'\rangle), \mathtt{out}(\{\langle s, \pi_2(\langle n, \langle n',a\rangle\rangle)\rangle\}_k^{r'})\|P_2\|P_B) \\ & \to & ((a, \{\langle n, \langle s,a\rangle\rangle\}_k^r, \langle n,n'\rangle, \{\langle s, \langle n',a\rangle\rangle\}_k^{r'}), P_2\|P_B) \\ & \to & ((a, \{\langle n, \langle s,a\rangle\rangle\}_k^r, \langle n,n'\rangle, \{\langle s, \langle n',a\rangle\rangle\}_k^{r'}, \langle s,n''\rangle), P_2\|P_2) \end{array}$$

where $P_1 = \mathtt{in}(y).\mathsf{if}\ \pi_1(y) = n\ \mathsf{then}\ \mathtt{out}(\{\langle s, \pi_2(y)\rangle\}_k^{r'})$ and $P_2 = \mathtt{in}(z).\ \mathsf{if}\ \pi_1(\mathsf{dec}(z,k)) = \pi_1(\pi_2(\mathsf{dec}(x,k))) \wedge \pi_2(\mathsf{dec}(z,k)) = n'\ \mathsf{then}\ OK$.

In the last configuration, it is possible to deduce s from the frame.

4. We apply automatically the translation and we get:

$$\begin{array}{rcl} \mathtt{Att}(\{\langle n, \langle s,a\rangle\rangle\}_k^r) & \Leftarrow & \\ \mathtt{Att}(\langle y_n, n'\rangle) & \Leftarrow & \mathtt{Att}(\{\langle y_n, \langle y_s, a\rangle\rangle\}_k^z) \\ \mathtt{Att}(\{\langle s,x\rangle\}_k^z) & \Leftarrow & \mathtt{Att}(\langle n,x\rangle) \end{array}$$

5.

$$\frac{\mathtt{Att}(\{\langle n, \langle s, a\rangle\rangle\}_k^r) \quad \mathtt{Att}(\langle y_n, n'\rangle) \Leftarrow \mathtt{Att}(\{\langle y_n, \langle y_s, a\rangle\rangle\}_k^z)}{\mathtt{Att}(\langle n, n'\rangle)}$$

and

$$\frac{\dfrac{\mathtt{Att}(\langle n, n'\rangle)}{\mathtt{Att}(n)} \qquad \dfrac{\dfrac{\mathtt{Att}(\langle n, n'\rangle)}{\mathtt{Att}(n')} \quad \mathtt{Att}(a)}{\mathtt{Att}(\langle n', a\rangle)}}{\mathtt{Att}(\langle n, \langle n', a\rangle\rangle)}$$

and

$$\dfrac{\dfrac{\dfrac{\mathtt{Att}(\langle n, \langle n', a\rangle\rangle) \quad \mathtt{Att}(\{\langle s, x\rangle\}_k^z) \Leftarrow \mathtt{Att}(\langle n, x\rangle)}{\mathtt{Att}(\{\langle s, \langle n', a\rangle\rangle\}_k^r)} \qquad \mathtt{Att}(\langle y_n, n'\rangle) \Leftarrow \mathtt{Att}(\{\langle y_n, \langle y_s, a\rangle\rangle\}_k^z)}{\mathtt{Att}(\langle s, n'\rangle)}}{\mathtt{Att}(s)}$$

6. Again, we have only to consider the complete traces, and the constraint system that we solved in question 3c. In particular, we must have $y' = n'$. With the same reasoning as in the question 3d, there is no attack on the agreement on n'.

7. There is no attack on the agreement on n (resp. n'), even for multiple copies of the processes

   We only sketch why. An event $\mathsf{ev}a(n_i)$ is triggered when A receives a message $\langle n_i, z_i\rangle$. This is only possible when n_i is deducible from the current frame. Since the key k is never deducible from any frame (it does not appear in clear in any message), n_i can only be deduced from a message where it appears in clear. Hence at a point where B has sent a message $\langle n', z_i'\rangle$.

8. There is an attack if the encryption scheme is malleable.

   We only sketch why. First there are IND-CPA encryption schemes, for which the integrity of the plaintext is not ensured. In particular (as in El-Gamal), we could modify the plaintext, without decrypting it. Using a first session of the protocol, the attacker may get a sample of the encryption with k. Then, in a second session, it could be possible to replace the nonce n with, say, the pair $\langle v, n\rangle$ in the first message sent by a. When b replies, the message $\langle\langle v, n\rangle, n'\rangle$ is replaced with $\langle n, n'\rangle$. Then b has $y_n = \langle v, n\rangle \neq n$, which violates the agreement property.

Exercise 2

They are all false. For the first three ones, we use the completeness of static equivalence: we give in each case a predicate symbol and recipes allowing to distinguish the two sequences.

1. $M(\mathsf{dec}(x_1, x_3))$ holds true on the second sequence of terms and holds false on the first one. And there are IND-CPA encryption schemes that implement the predicate M (decryption succeeds).

2. $EQ(\mathsf{dec}(x_1, x_3), \pi_1(\mathsf{dec}(x_2, \mathsf{dec}(x_1, x_3))))$ holds on the second sequence and not on the first

3. $EK(x_1, x_2)$ holds true on the first sequence and not on the second, and there are IND-CPA encryption schemes that implement EK.

4. First, if u does not contain k_1, k_2 (actually, we only need that it does not contain k_1) as a plaintext, the equivalence is true, using the soundness theorem of the lecture: the two terms are statically equivalent, hence computationally equivalent.

   If $u = k_1$, We can build (as in the exercise from the lecture) an IND-CPA encryption scheme such that, on input x,

   - It returns $0 \cdot \mathcal{E}(x, k, r)$ if $x \neq k$ and $x \neq 1 \cdot k$
   - It returns $1 \cdot \mathcal{E}(k, k, r)$ if $x = k$
   - It returns $1 \cdot \mathcal{E}(1 \cdot k, k, r)$ if $x = 1 \cdot k$

   Then the two distributions can be distinguished: it is sufficient to check the first bit of the ciphertext.

Exercise 3

Consider for instance

$$\begin{array}{rl} A \to B: & \nu n.\nu s, \nu r.\{\langle a, \langle n, s\rangle\rangle\}_k^r \\ B \to A: & \nu n', \nu r'\{\langle n, n'\rangle\}_k^{r'} \\ A \to B: & n' \end{array}$$

And the scenario $\nu k.P_A$ (B does not even play!)

The weak secrecy of s holds in the standard model: the constraint

$$\left\{ \begin{array}{rcl} \{\langle a, \langle n, s\rangle\rangle\}_k^r & \overset{?}{\vdash} & \{\langle n, x\rangle\}_k^{z'} \\ \{\langle a, \langle n, s\rangle\rangle\}_k^r, x & \overset{?}{\vdash} & s \end{array} \right.$$

has no solution, since the first constraint cannot be simplified by any rule.

There is an attack in BC mode: the attacker gets $\{\langle n, s\rangle\}_k^r$, which is sent back to a (i.e., we use the binding $x = s$). He gets s as a reply.

Comment: Some simpler solutions were submitted by students.