Sécurité des Systèmes D'Information Non-Mandatory Exercice Sheet 6 : Digital Signature and Authentication

4 Décembre 2019

You can submit on Moodle, before **December 9th, 2019 at 5pm**.

Your answers should be justified.

Exercice 1 : A quite fragile RSA based signature scheme.

We have A's public and private RSA keys, respectively (e,n) and (d,n). To sign a message m, A computes $y = m^d \mod n$, and sends (m, y) to B. To verify the signature, B computes $x = y^e \mod n$ and accepts the signature iff $x = m$.

- Find a message (other than 0 and 1) easy to falsify even if we possess only the public key.
- B chooses a number a, computes $a^{-1} \mod n$, and then asks A to sign the message $m = a^e k \mod n$. What is B trying to do ? If A signs m, what will B be able to do ?
- Now, you want to falsify a given message m. You're allowed to have two chosen messages (which means, choose two messages m_1 and m_2 for which you will obtain the corresponding signatures). Choose m_1 and m_2 wisely to allow the falsification of m.

Exercice 2 : A very simple authentication scheme

We have A and B, each with their respective private keys K^a_{priv} and K^b_{priv}, and respective public keys K^a_{pub} et K^b_{pub} :

- B sends a random challenge r_1 to A.

- A chooses a random challenge r_2, then sends $(r_2, K^a_{priv}(r_1))$ to B.
- B checks $K^a_{priv}(r_1)$ with A's public key. If B finds r_1, then he accepts A's identity, and sends back to A $K^b_{priv}(r_2)$.
- Similarly, A uses B's public key to check $K^b_{priv}(r_2)$, and if A finds r_2, A accepts B's identity.

We consider on secure channel where messages are not intercepted. Show this protocol is not secure, as an entity C can authenticate to B as A.

Exercice 3 : An improved (?) authentication scheme.

With the same A,B, and same keys as before, we're now trying this scheme :

- B sends a random challenge r_1 to A.
- A chooses a random challenge r_2, and sends $(r_2, K^a_{priv}(r_1 \parallel r_2))$ to B (this time, A encrypts the concatenation of r_1 and r_2).
- B checks $K^a_{priv}(r_1 \parallel r_2)$ with A's public key. Once again, he accepts A's identity iff he finds $r_1 \parallel r_2$. Then, he sends $K^b_{priv}(r_1 \parallel r_2)$ to A.
- A checks $K^b_{priv}(r_1 \parallel r_2)$ with B's public key, and accepts B's identity iff he finds $r_1 \parallel r_2$.

Once again, we consider on secure channel where messages are not intercepted. Show that this protocol is still not secure, as if A tries to authenticate to C, C can use it to authenticate to B as A.
How would you improve this scheme ?