M1 Informatique, november 27, 2017

TD 3: Public keys

1 RSA

Alice and Bob use RSA with a modulus $n = 209$. Alice's public key is 17.

(1) What is Alice's private key?

(2) With plaintexts whose numerical values are less than $n-1$, find the cleartext corresponding to the ciphertext 20.

2 El Gamal

We study El Gamal's behavior in an additive group. For a prime p and $\alpha \in \mathbb{Z}_p$, we compute $\beta \equiv \alpha.a \mod p$. Message M is signed by (γ, δ):

$$\begin{cases} \gamma \equiv k.\alpha \mod p & \text{for } k \text{ random} \\ \delta \equiv (M - a.\gamma).k^{-1} \mod p \end{cases}$$

(1) What are the public and private parameters?

(2) Show that $\gamma.\beta + \gamma.\delta \equiv \alpha.M \mod p$ verifies the signature.

(3) Describe a simple attack against this signature algorithm.

(4) With $p = 37$, $\alpha = 2$, $\beta = 14$ check the validity of $(M, \gamma, \delta) = (8, 10, 32)$ and find the private parameter's value.

3 Key management

Let us consider the following protocol:

(1) $A \to B : K^a \mod p$

(2) $A \leftarrow B : (K^a)^b \mod p$

(3) $A \to B : (K^{ab})^{a^{-1}} \mod p$

- Find the information shared by A and B to use the protocol.
- What information is kept secret and what information is published by both parties?
- Describe and explain this protocol.
- Show that it does not ensure the parties authentication and provide an attack against it. Propose an improvement of the protocol.