

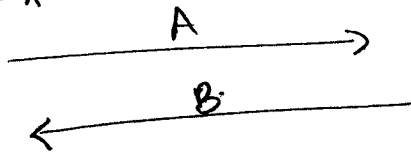
§ 5.3. Établissement de clés par cryptographie Asymétrique / 5.5

Rappelons :

protocole DH. d'échange de clés

A.

- choisir aléato. $a = k_{prA}$
- Calculer $A = \alpha^a \text{ mod } p$
 $= k_{pubA}$



- $k_{AB} = B^a \text{ mod } p$

B

- choisir aléat. $b = k_{prB}$
- Calculer $k_{pubB} = \alpha^b$

- $k_{AB} = A^b \text{ mod } p$

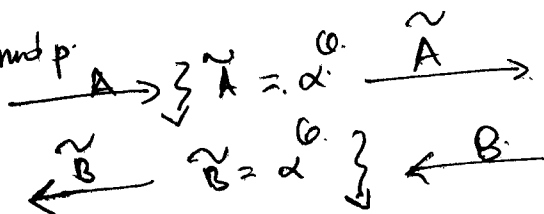
(et l'attaque suivante (valable pour tout syst. asymétrique)

Attaque MITM. (Man-in-the-middle).

A

- $a = k_{prA}$
- $A = k_{pubA} = \alpha^a \text{ mod } p$

B. Oscar



- $k_{AO} = (\tilde{B})^a \text{ mod } p$

- $k_{AO} = A^0 \text{ mod } p$

- $k_{BO} = \tilde{B} \text{ mod } p$

B.

- $b = k_{prB}$
- $B = \alpha^b \text{ mod } p$
 $= k_{pubB}$

- $k_{BO} = (\tilde{A})^b \text{ mod } p$

⇒ Oscar peut intercepter et lire les messages entre A et B à leur insu.

La notion de certificat permet de parer à cette attaque MITM.