## § 5.3. Etablissement de clés par cryptographie Asymétrique

Rappelons :

**protocole DH. d'échange de clés**

| A | B |
|---|---|
| • choisir aléato. $a = k_{prA}$ | • choisir aléat. $b = k_{prB}$ |
| • calculer $A = \alpha^a \bmod p$. $= k_{pubA}$ | • calculer $k_{pubB} = \alpha^b \bmod p$. |
| $\xrightarrow{A}$ | |
| | $\xleftarrow{B}$ |
| • $k_{AB} = B^a \bmod p$. | • $k_{AB} = A^b \bmod p$. |

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

**Attaque MIM. (man-in-the-middle).**

O : Oscar

| A | B. |
|---|---|
| • $a = k_{prA}$ | • $b = k_{prB}$. |
| • $A = k_{pubA} = \alpha^a \bmod p$. | • $B = \alpha^b \bmod p$. $= k_{pubB}$. |
| $\xrightarrow{A}$ O intercepte $\tilde{A} = \alpha^o$. | $\xrightarrow{\tilde{A}}$ |
| $\xleftarrow{\tilde{B}}$ O intercepte $\tilde{B} = \alpha^o$. | $\xleftarrow{B}$ |
| • $k_{AO} = (\tilde{B})^a \bmod p$. | • $k_{BO} = (\tilde{A})^b \bmod p$. |

• $k_{AO} = \tilde{A}^o \bmod p$

• $k_{BO} = \tilde{B}^o \bmod p$.

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

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