

Protocole DH

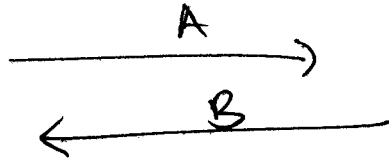
Alice.

Canal.  
#

Bob.

- choisir  $k_{prA} = a \in \{2, 3, \dots, \#C - 1\}$
- Calculer  $k_{pubA} = aP = A = (x_A, y_A)$

- choisir  $k_{prB} = b$
- Calculer  $k_{pubB} = B = bP = (x_B, y_B)$



- Calculer  $aB = T_{AB} = (x_{AB}, y_{AB})$

- Calculer  $bA = (x_{AB}, y_{AB}) = T_{AB}$

$$T_{AB} = aB = a(bP) = (ba) \cdot P.$$

La clé commune  $T_{AB}$  peut être utilisée par chacun  
un chiffreur DES, AES, etc.

§§ 5.4. Sécurité.

Si O. veut attaquer le protocole DH, il a l'information

$(\mathbb{E} \text{ courbe elliptique}), p, P, A, B$  et veut calculer

$T_{AB}$ . Il doit résoudre Probl. LD sur  $CE$  !

$$a = \log_P A \quad \text{ou} \quad b = \log_P B.$$

- les attaques génériques sont plus faibles.
- Note les attaques génériques : shank, Baby-step, ...