Protocole DH

Canal.

Alice # 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 $k_{pubB} = B = bP = (x_B, y_B)$

A →

← B

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

- Calculer $bA = (x_B, y_B) = T_{AB}$.

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

La clé commune T_{AB} peut être utilisée par exemple un chiffrement DES, AES, etc.

§§ 3.4. Sécurité.

Si O. veut attaquer le Protocole DH, il a l'information E (courbe elliptique), p, P, A, B. et veut calculer T_{AB}. Il doit résoudre Prob. LD sur CE. :

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

- Les attaques non génériques sont plus faibles.
- Reste les attaques génériques : Shank, Baby-Step, ...