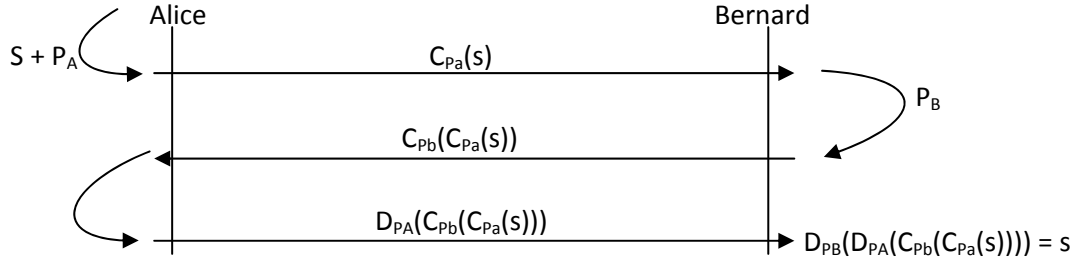
Bases de cryptographie

Pourquoi la cryptographie ?

- Confidentialité
- Identification
- Intégrité

1. *Echange de clefs.*

a.



b. Ca vaut « m ».

c. Voir schéma.

d. Eve ne connait ni P_A, ni P_B.

e. La condition sur les fonctions est **la commutativité**.

f. Pour Bernard : $a^B=(Y^A)^B=Y^{AB}$
Pour Alice : $b^A=(Y^B)^A=Y^{AB}$

g. La clé commune est Y^{AB}.

h. Eve connait uniquement Y^A et Y^B.

i. $f(x)=y^x \bmod(P)$
Exemple : P=17 Y=4 A=3 B=6
$a=4^3 \bmod(17) = 64 \bmod(17) = 13$ > $a^B \bmod(P)= 13^6 \bmod(17)=\mathbf{16}$
$b=4^6 \bmod(17) = 4096 \bmod(17) = 16$ > $b^A \bmod(P)= 16^3 \bmod(17)=\mathbf{16}$

j. Alice et Bernard possèdent la clé secrète sans l'avoir échangée : ils ont le même résultat.

k. Eve ne dispose que de $Y^A \bmod(P)$ et $Y^B \bmod(P)$. La fonction modulo étant sans retour, elle ne peut pas retrouver la clé secrète.

l. Le seul inconvénient, il faut que les 2 personnes soient « en ligne ».

2. *Cryptographie asymétrique, exemple RSA*

a. La clé privée est utilisée pour décrypter, la clé publique pour crypter (ou inversement).

b. La relation fondamentale, est encore une fois la commutativité.

c. On ne peut pas trouver la clé privée à partir de la clé publique.

d. Schema (voir cours).

e. Eve ne dispose que des clés publiques. Ainsi, elle ne peut pas décrypter.

f. Il n'y a pas besoin d'un échange dynamique, il suffit que la clé publique soit disponible quelque part (internet, …).

g. L'inconvénient est le temps de calcul.