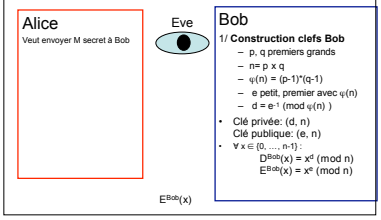
RSA

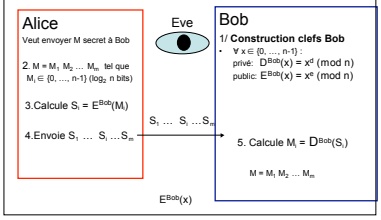
Rivest / Shamir / Adleman (1977)

1. Chiffrement RSA : E et D
2. Validité de RSA
   1. E (D (x)) = D(E(x)) = x
   2. E est facile à calculer
   3. E est difficile à inverser sans connaître D
3. Signature RSA
   1. Directe
   2. Avec résumé du message

Chiffrement RSA



Chiffrement RSA



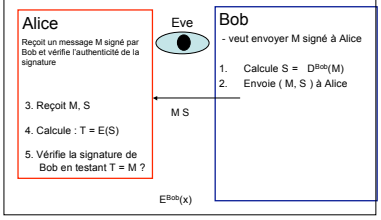
Validité de RSA

- D^{Bob} est la réciproque de E^{Bob} :
  - $\forall x \in \{0, \ldots, n-1\}$: $D^{Bob}(E^{Bob}(x)) = E^{Bob}(D^{Bob}(x)) = x$
- E^{Bob} est une fonction à sens unique *chausse-trappe*:
  - $E^{Bob}(x)$ est peu coûteuse à calculer
  - $D^{Bob}(x)$ est peu coûteuse à calculer
  - Calculer *d* à partir de (*n* et *e*) est calculatoirement aussi difficile que factoriser *n*
- Générer une clef RSA [(n,d), (n,e)] est peu coûteux

Applications
Chiffrement à clef publique / RSA

- Authentification
- Signature

Signature RSA



Signature RSA du résumé