Aspects calculatoire et sécurité signature RSA.

- la signature s est de long. $\lceil \log_2 n \rceil \simeq$ 1024. à 3072 bits.
  cette long peut être un pb pour les systèmes consommant peu d'energie tel téléphone cellulaire.
  Le Processus de génération de clés et les calculs ont les mê que pour l'infrastructure cryptage / decryptage.

- Pour Prévenir les attaques, on utilise le concept de Certificat (Authenticité).

- Les attaques pour les mêmes que précédemment vir.
  (chap3. §: 2. RSA) : factoriser n.

- Forger une fausse signature ; Man-in-the middle.
  On peut générer une signature exacte pour un message aléatoire x: