(2.3). Attaques de RSA.

3 types d'attaques exploitant comment RSA est implémenté ou utilisé, au lieu de l'attaque de l'algorithme lui même.

→ • Attaques par protocoles : Exploite la malléabilité de RSA.

Déf. Un cryptosystème est malléable si l'attaquant O. est capable de transformer le chiffré en un autre chiffré qui même a retrouve le clair.

O.
A ⟶ B
y.

•• Par Ex, RSA : soit y le chiffré de RSA où

O remplace y par $s^e \cdot y$ où $s \in \mathbb{N}$.

B déchiffre $s^e \cdot y$ par.

$$(s^e \cdot y)^d \equiv s^{ed} \cdot x^{ed} \equiv s \cdot x \mod n.$$

qui est un clair valide : donc O a détruit le message et B ne le sait pas.

Une telle attaque peut être évitée en utilisant le padding (voir Paul. page 192 – 193.) qui consiste à rajouter une information aléatoire au clair dans le message avant la transmission.