Les techniques de pare-feux (5)

- Les garde-barrières filtrants

éterminer ce qui est autorisé et ce qui

é d'associer des techniques comme la traduction

Sécuriser les échanges de données

ées en confiance :

é

émetteur

é : même sur des supports non sûrs (écoute),
ées ne dôivent pouvoir être lues que par le

égrité : les données ne doivent pas être altérées (ajouts,

épudiation : preuve d'émission,

éception

Rappels sur les techniques (1)

- codage à clé secrète (exemple : DES)

épendant d'un clé prenant en entrée un
é

échiffrement = algorithme symétrique du premier utilisant la
ême clé pour transformer le message codé dans le message

étés

échiffrement rapides

é de reconstituer la clé même en connaissant des
ésultat chiffré

Rappels sur les techniques (2)

- codage à clé publique (exemple : RSA)

és, l'une, privée, pour chiffrer, l'autre, publique,
échiffrer

étés

échiffrement rapides

é de reconstituer la clé privée, même en connaissant la
é publique et des exemples de messages en clair ou codés

é. Message codé avec la clé
être décodé qu'avec la clé privée.

Rappels sur les techniques (3)

- fonction de hashage à sens unique (exemple : MD4,

é et transforme tout
îne de longueur fixe.en sortie un message codé.
ération de déchiffrement

étés

ès importante de la moindre modification du texte

ésentés par 32 chiffres hexadécimaux

L'utilisation de ces techniques (2)

- sécuriser des connexions

à sens unique pour des mots de
e à usage unique (OTP = *One Time Passwords*)

éfi au client
éfi et une clé secrète pour générer une succession desix

és)

é, robustesse ; inconvénients : le défi n'est pas
éatoire (défi n° *n+1* peut se déduire du défi n° *n* => mascarade possible)

L'utilisation de ces techniques (3)

- authentification, intégrité

e à clé publiques ou privées + hashage à

à vis de B, MD5 pour la

é privée

e à B le message et la signature chiffrée

échiffre (RSA) la signature avec la clé publique de A et la compare

égalité : le message provient de A et n'a pas été altéré

L'utilisation de ces techniques (4)

- confidentialité, authentification

e à clé publiques ou privées ou bien à clé

ète

îtiers de chiffrement DES (56 bits) ou triple-DES (= 112 bits, par
é1, décodage avec clé2, codage avec clé1):

L'utilisation de ces techniques (5)

- non répudiation => utilisation d'un tiers (notaire électronique) pour

à A le message chiffré par une clé à usage unique et un id.

à B

çoit la clé

échiffre le message et envoie un accusé de réception au notaire.

ée par la clé privée de l'émetteur