Sécurité

- Sûreté de fonctionnement
- Notions de base en cryptographie appliquées à la sécurité des échanges

Sûreté de fonctionnement – Sommaire

Définitions

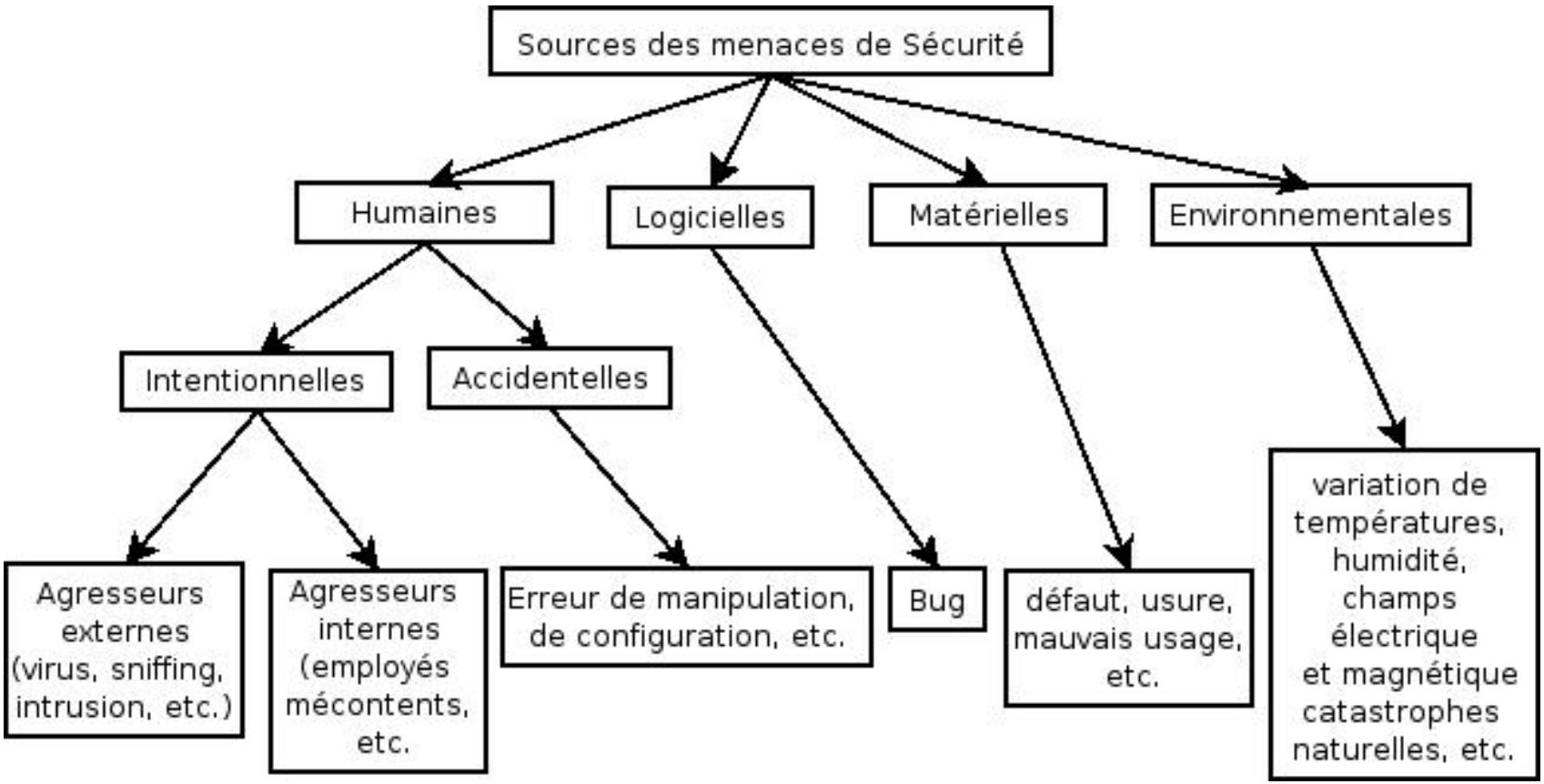
Définition

Sûreté de fonctionnement concerne l'ensemble des mesures prises et des moyens utilisés pour se prémunir contre les dysfonctionnements du système

Définition

Sécurité regroupe tous les moyens et les mesures prises pour mettre le système d'information à l'abri de toute agression

Typologie des sources des menaces



Quelques exemples de menaces de dysfonctinonnement

- défaillance des équipements de traitement (panne)
- dysfonctionnement des mémoires de masse
- défaut des équipements réseau
- défaillance de la fourniture d'énergie involontaire (panne) ou volontaire (grève)
- aggressions physiques comme l'incendie et les inondations

Les systèmes à tolérance de panne (*fault tolerant*)

Principe

La fiabilité matérielle est obtenue par sélection des composants mais surtout
par la **redondance des éléments principaux**

Techniques de redondance

Définition

Miroitage (*mirroring*) : le système de secours est maintenu en permanence dans le même état que le système actif

Définition

Duplexage (*duplexing*) : équipement disponible qui prend automatiquement le relais du système défaillant

Les mémoires de masse : systèmes RAID

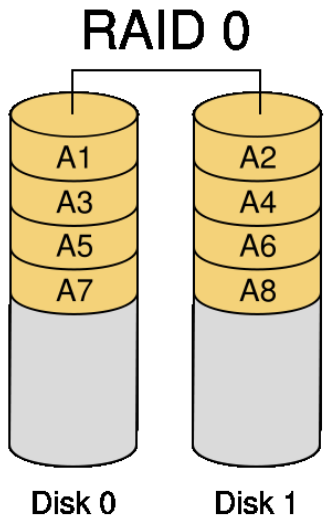
Définition

RAID (*Redundant Array of Independant*[a] *Disk*pr)
Différents stratégies de tolérance de panne apportant différents niveaux de fiabilité et de performance état que le système actif

[a] Hist. *Inexpensive* i.e. bon marché et donc peu fiable

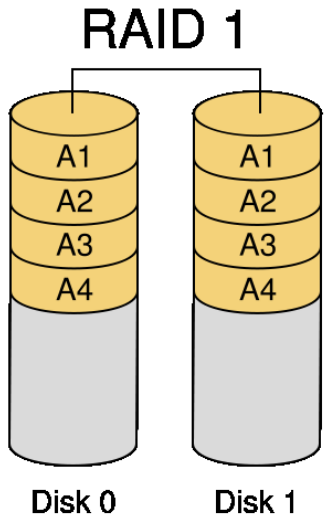
En pratique seuls les niveaux 1 et 5 sont utilisés

RAID 0, appelé "volume agrégé de bandes de données (*striping*)" ou "entrelacement de disques" : **augmente les performances** de la grappe en faisant travailler n disques durs en parallèle.
Chaque disque ne lit et écrit que $1 / n$ des données.

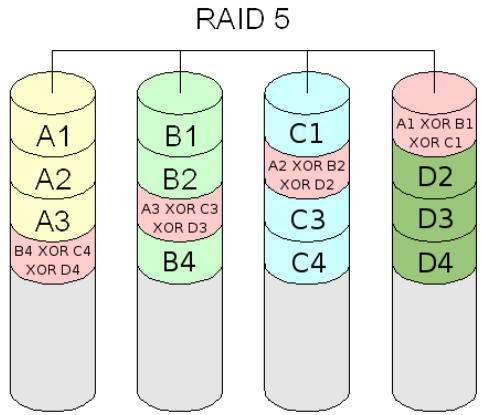


Les mémoires de masse : stratégies RAID

RAID 1, appelé "miroitage de disques" : **augmente la fiabilité** en dupliquant simultanément les données sur chacun des *n* disques de la grappe (accepte une défaillance de *n* - *1* éléments)
Performance en lecture accrue et aucune incidence en écriture.



RAID 5, appelé "volume agrégé de bandes à parité répartie" : **cumule fiabilité** (grâce à codes de contrôle de parité répartis sur chacun des disques –en RAID 4 étaient stockés sur un seul disque)
et **bonne disponibilité** (grâce à la répartition de la parité possibilité de reconstruire un disque défaillant à partir des données et des informations de parités contenues sur les autres disques)



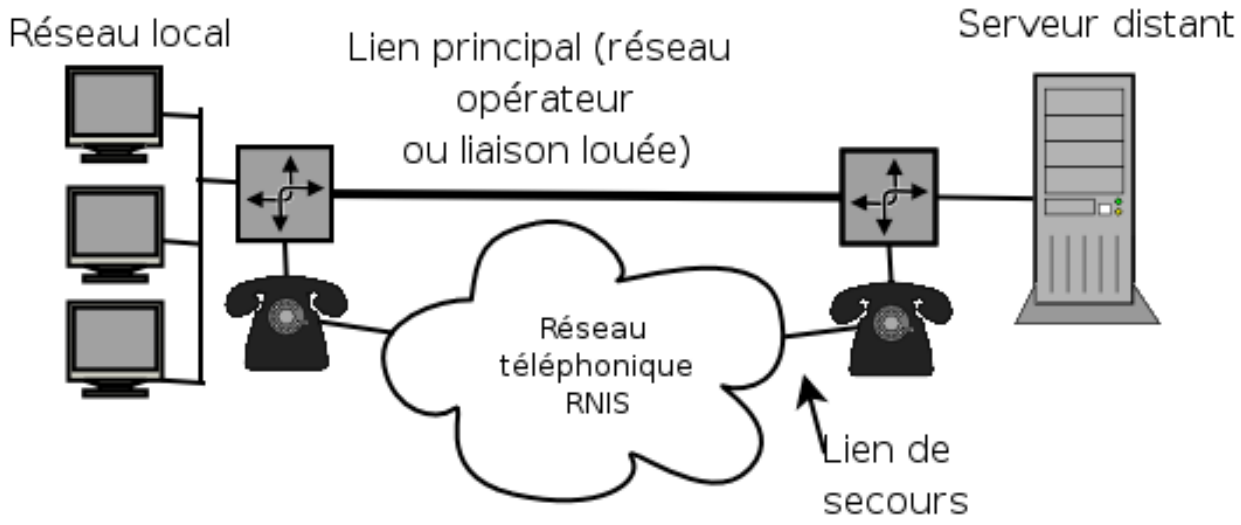
Duplexing de serveurs

le duplexing d'équipement tel que des serveurs constitue le niveau de sûreté le plus élevé :

- gestion des serveurs par un système d'exploitation indépendant
- l'utilisateur est connecté à l'un de serveurs
- toutes les opérations effectuées sur l'un sont recopiées sur l'autre via un canal haut débit
- en cas de défaillance d'un serveur, la connexion de l'utilisateur est basculée sur l'autre
- la panne est totalement transparente

La sûreté des moyens de transport

Réalisée par la redondance des liens obtenue par le **maillage du réseau**ou par le **doublement des raccordements au réseau de l'opérateur**
Dans le second cas, en fonctionnement normal les charges sont équilibrées sur les deux liens
Compte tenu des coûts, les connexions de secours sont établies à la demande en utilisant généralement le réseau téléphonique



L'alimentation électrique

Définition

Onduleur : équipement qui fournit à partir de batteries le courant électrique d'alimentation du système

Deux types :

- **off-line** : relais en cas de défaillance du réseau d'alimentation sur des batteries chargées en continu
- **on-line** : intermédiaire permanent avec le réseau public, qui stabilise le courant en amplitude et en fréquence ; bascule sur le réseau public en cas de panne

L'autonomie de batterie étant généralement fixée à 20 minutes, un **générateur (groupe électrogène)** peut se substituer au réseau d'énergie public

Les contraintes thermiques

- **climatisation** des locaux informatiques entre 20 à 23°C
- **ventilation avec taux de poussière maximale** de $200\mu g/m^3/24$ heures
- **degré hygrométrique (humidité atmosphérique) correct** entre 40% et 85%

Définitions

Définitions

Disponibilité caractéristise le fait de fournir un service continu et non altéré (réseau, données, logiciel...)

Fiabilité probabilité pour que le système fonctionne correctement pendant une durée donnée dans les conditions définies (i.e. proba. de disponibilité)

Maintenabilité probabilité de retour à un bon fonctionnement dans un temps donné

Définitions

MTTR (*Mean Time To Repair*) : temps moyen de toute répération/remise en état du système

MTBF (*Mean Time Between Failure*) : temps moyen de bon fonctionnement (entre deux pannes successives)

Relations entre Disponibilité et MTTR–MTBF

La **D**isponibilité est définie par :

$$D = \frac{MTBF}{MTBF + MTTR}$$

L'**I**ndisponibilité comme son complément :

$$I = 1 - D = \frac{MTTR}{MTBF + MTTR}$$

On a donc :

$$\frac{I}{D} = \frac{MTTR}{MTBF}$$

Pour rendre un système efficace on peut :

- augmenter le MTBF mais les composants réseaux seront plus onéreux
- diminuer le MTTR mais la maintenance sera plus coûteuse

Les structures de fiabilité

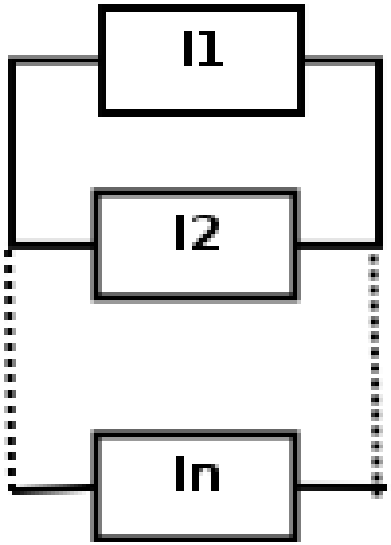
Propriété

La mesure de la disponibilité totale d'un système dépend de sa structure.

Deux structures élémentaires :

La structure série

La structure parallèle



Les structures de fiabilité

La structure série : la **D**isponibilité totale est plus petite que celle du composant qui a la plus faible disponibilité

$$D_{totale} = D_1 * D_2 * \ldots * D_n$$

L'**I**ndisponibilité est alors $I_{totale} = 1 - D_{totale}$
Et si $D \approx 1$ (I très petit) alors $I_{totale} = \sum_1^n I_n$

On peut aussi montrer : $MTBF_{serie} = \frac{1}{\sum_{i=1}^{i=n}(\frac{1}{MTBF_i})}$

La structure parallèle : la **I**ndisponibilité totale est plus petite que celle du composant qui a la plus faible indisponibilité

$$I_{totale} = I_1 * I_2 * \ldots * I_n$$

La **D**isponibilité est alors $D_{totale} = 1 - I_{totale}$

De même on peut aussi montrer : $MTTR_{parallele} = \frac{1}{\sum_{i=1}^{i=n}(\frac{1}{MTTR_i})}$

Quizz de synthèse sur la sureté de fonctionnement

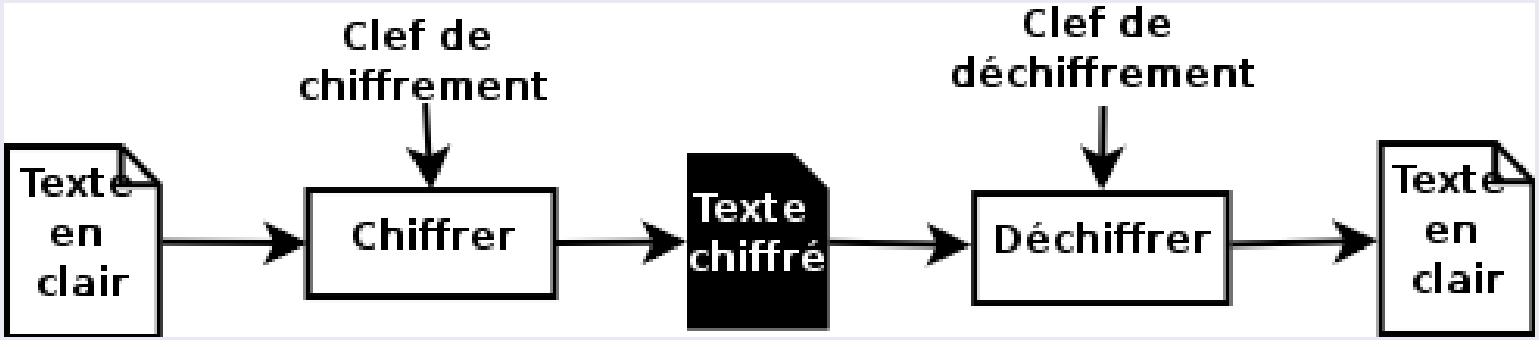
- Quelle est la solution clé aux problèmes de sûreté de fonctionnement (crash disque, serveur surchargée, etc.) ?
- Que signifie les acronymes MTTR et MTBF ? Et comment se définissent-ils l'un par rapport à l'autre ?

Cryptographie et sécurité des échanges– Sommaire

Terminologie

Définitions

Cryptographie : désigne l'ensemble des techniques de chiffrement de l'information



Cryptanalyse : techniques visant à l'obtention du message en clair ou de la clef de chiffrement sans aucune information (*décrypter*[a])

Cryptologie = **Cryptographie** + **Cryptanalyse**

[a] Attention aux anglicismes *crypter* et *cryptage* dérivés de l'anglais *to encrypt* qui signifie *chiffrer*

Services rendus par la cryptographie

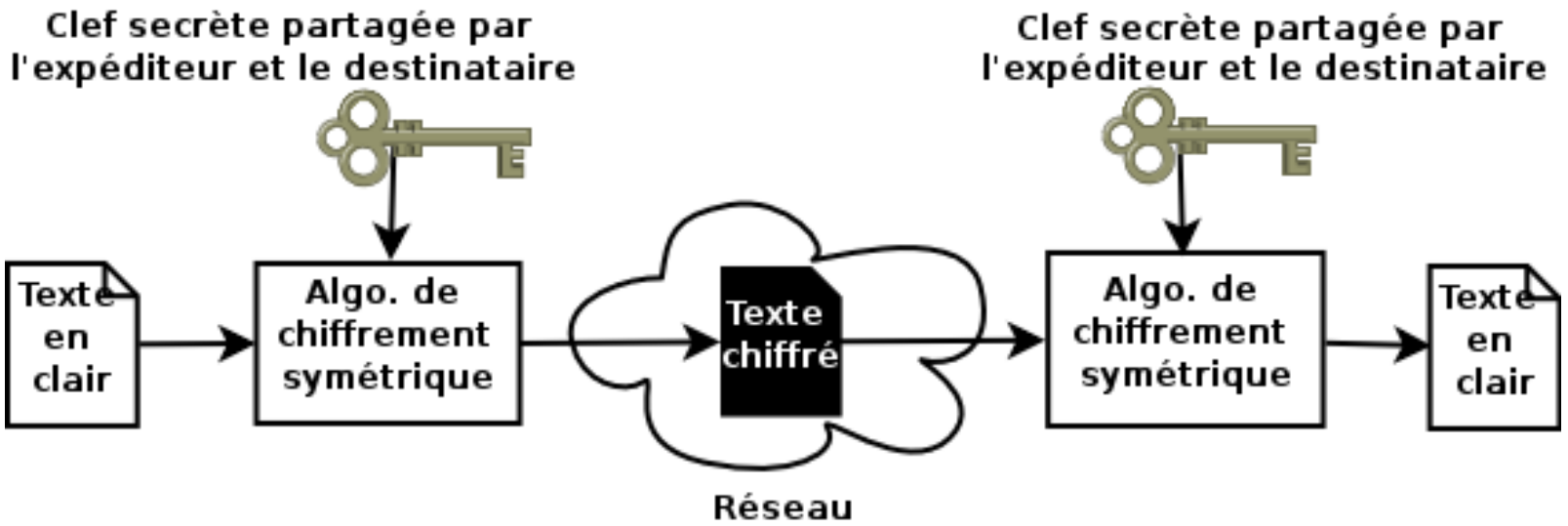
- **Confidentialité** : contenu secret par algorithmes de **chiffrement**
- **Authentification** : validation de l'expéditeur par algorithmes de **signature numérique**
- **Intégrité** : contenu non modifié vérifié par algorithmes de **hachage**
- **Echanges de clefs** de chiffrement pour une session

Algorithmes symétriques

Définition

à clé secrète, ou symétrique : les clefs de chiffrements et déchiffrements sont identiques

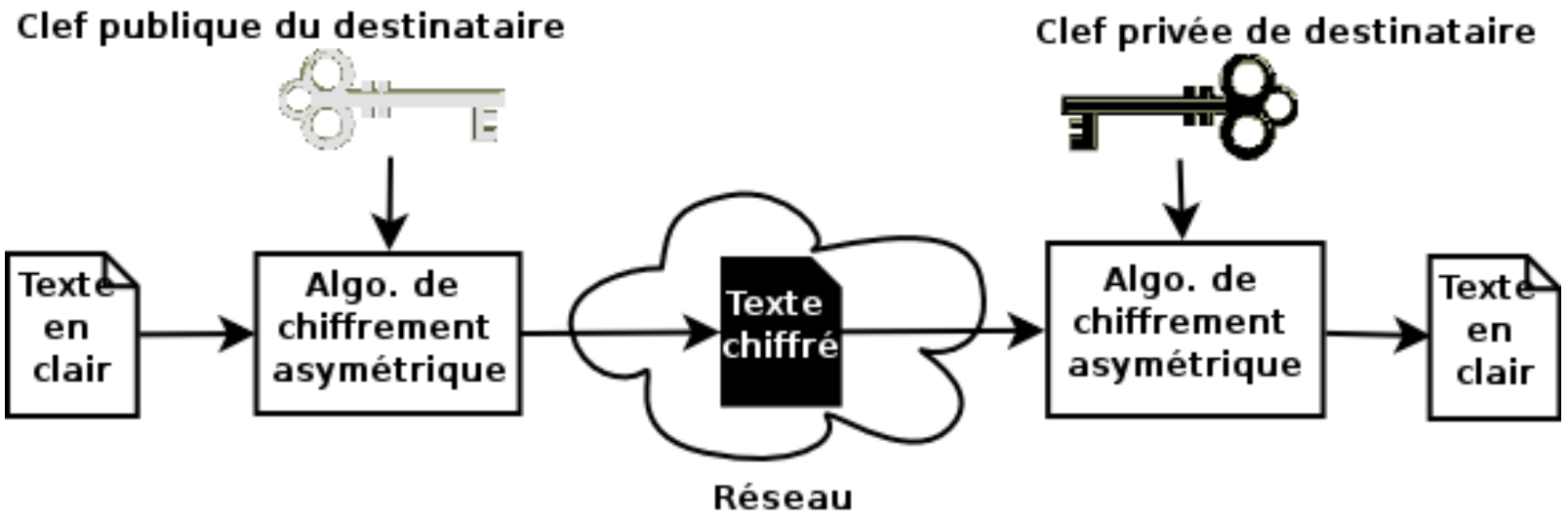
repose sur la non-divulgation des clés et la résistance des algorithmes aux attaques de cryptanalyse



Algorithmes asymétriques

Définition

à clé privée et publique distinctes, ou asymétrique : une clef publique pour chiffrer et une clef privée pour déchiffrer
repose sur la difficulté de déduire la clé privée associée à une clé publique (temps non raisonnable)

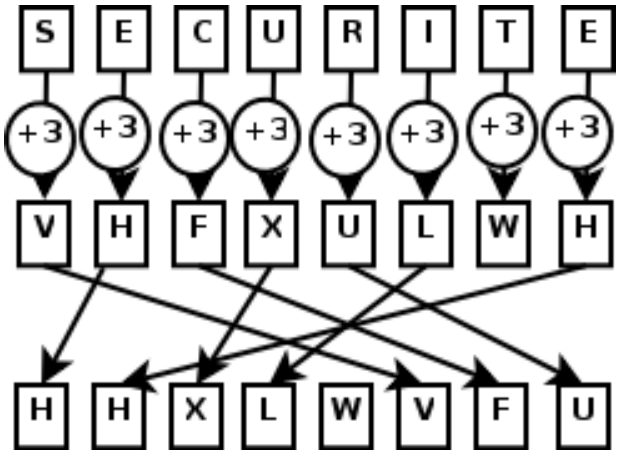


Eléments de comparaison

- **Algorithmes symétriques**
  - autant de clé que d'interlocuteurs
  - problème de diffusion des clés secrètes
  - utilisé pour le chiffrement
- **Algorithmes asymétriques**
  - temps de traitement important d'où non performant pour chiffrer les messages longs
  - utile pour chiffrer mais aussi pour "échanger des clés" et "signer" un message (voir plus loin)
- **Algorithmes asymétriques et symétriques**
  - en général dans le domaine public

Algorithmes symétriques majeurs

DES (*Data Encryption Standard*)
adopté par NIST (*National Institute of Standards and Technology*) en 1977
Données chiffrées (décalage, permuttation, ...) par blocs de 64 bits
avec clé de 56 bits (+8 bits de parité)
Remplacé par : **Triple DES** avec clé de 3*56 bits



Autres algo. :
RC2, RC4, RC5 (*Rivest Code*), diffusé par RSA Sec. Inc. clé jusqu'à 2048 bits
IDEA (*International Data Encryption*) clé de 128 bits sur des blocs de 64 et utilisé par le protocole de messagerie PGP (*Pretty Good Privacy*)
Blowfish développé par Schneier avec clé de longeur variable jusqu'à 448 bits
AES (*Advanced Encryption Standard*) clé de 128, 192 ou 256 sur blocs de 128

Résistance d'un algorithme symétrique et taille de clé

Principe

Plus la clé est longue, plus la proba. de la trouver est faible et donc plus grande est la sécurité

Evaluée par attaque force brute (énumération de toutes les combinaisons de clé)
Si clé a longueur de n bits, alors il existe 2^n possibilités de clé différentes. Soit une moyenne de 2^{n-1} essais pour trouver la bonne clé

Il est devenu relativement simple de "casser" des clés de 40 bits (i.e. environ 10^{12} possibilités),
on préfère chiffrer avec des clés de 128 bits (10^{38} possibilités)
Distributed.net (réseau de machines de par le monde pour du calcul distribué)

- RSA Lab's 56-bit DES-III Encryption Challenge : Terminé le 19 janvier 1999 (après 22,5 heures avec l'aide de EFF's Deep Crack custom DES cracker)
- RSA Lab's 64-bit RC5 Encryption Challenge (RC5-64) : Terminé le 14 juillet 2002 (après 1757 jours et 83% des clés testées)

Algorithmes asymétriques majeurs

Principe

Des paramètres (publiques) d'une fonction mathématique connue permettent de transformer un message clair en chiffré mais ne permettent de déduire les paramètres produisant l'opération inverse

- **RSA** (*Rivest, Shamir et Adleman*) clé de longeur variable ; facile de calculer le produit de 2 grands nombres premiers ; difficile de trouver les facteurs premiers de celui-ci (problème de la décomposition en produit de facteurs premiers)
- **Diffie-Hellman** repose sur difficulté de calculer un logarithme discret ; Utilisée dans IPSec
- **Cryptosystèmes à courbes elliptiques** 1985–2005. Algo. propriétaire ; repose sur difficulté de calculer un logarithme discret

RSA

Une fonction de chiffrement :

$$\text{Chiffré} = \text{Clair}^{public} \text{ modulo } n$$

avec *Clair*, message en clair et *Chiffré*, message chiffré
n, produit de nombres premiers (non divisible excepté par 1 et eux-même)
et *public* et *privé*, deux clés
Et une fonction de déchiffrement identique :

$$\text{Clair} = \text{Chiffré}^{prive} \text{ modulo } n$$

Signature par clé privé

Comment Bob puisse-t-il être sûr que c'est bien Alice qui lui adresse un message ?

Principe

L'émetteur **chiffre avec sa clé privée** *son message*

- *Alice_priv(Message_clair) = Message_chiffrée*

et le récepteur le **déchiffre avec la clé publique** *de l'émetteur*

- *Alice_pub(Alice_priv(Message_clair)) = Message_clair*

Algorithmes de signatures :
RSA, **DSA** (*Digital Signature Algo.*) développé et utilisé par le gouvernement des Etats-Unis, **GOST** (*Gosudarstvennyi Standard of Russian Federation*), ...

Calcul d'une empreinte pour vérifier l'intégrité

Comment Bob puisse-t-il être sûr que personne n'a modifié le message qu'Alice lui a adressé ?

Principe

1. *L'émetteur utilise une* **fonction de hachage** *pour calculer* **empreinte (digest)** *du message qu'il joint à son envoi*
2. *Le récepteur recalcule l'empreinte avec la même fonction de calcul qu'il applique au message reçu*
3. *S'il constate une différence alors le message a été altéré*

- Empreinte courte, irréversible et proba. faible que 2 messages aient empreinte identique
- Principales fonctions : **MD5** (*Message Disgest #*) de 1992 défini dans RFC 1321 et conçu par Rivest fournit empreintes de 128 bits, **SHA-1** (*Secure Hash Algorithm*) de 1993 fournit empreintes de 160 bits

Echange de clé secrète : l'enveloppe digitale

Problème

- *Lenteur des algo. asymétiques pour les longs messages*
- *Difficulté d'échanger clés secrètes pour algo. symétrique*

Solution

L'enveloppe digitale qui combine les deux types d'algo.
Utilisation d'un algorithme de chiffrement asymétrique pour échanger une clé de chiffrement symétrique dite **clé de session**

En pratique,

1. l'un des correspondant génère une clé secrète,
2. chiffre le message avec cette clé
3. qu'il communique avec le message chiffré à l'aide de la clé publique du destinataire

Comment vérifier la clé publique du destinataire ?

Echange de clé secrète : protocole de Diffie-Hellmann

Permet de construire clé secrète sans qu'elle circule sur le réseau
Repose sur le fait que

$$(g^a mod(p))^b mod(p) = (g^b mod(p))^a mod(p)$$

Alice et Bob vont donc

- s'échanger deux nombres g et p
  avec p premier et g inférieur à p et primitif[1] par rapport à p
- choisir chacun un nombre secret. Resp. a et b
- calculer la valeur $(g^a mod(p))$ pour Alice et $(g^b mod(p))$ pour Bob et se les envoyer
- calculer la clé secrète à partir de la clé reçue. Resp. $(g^b mod(p))^a mod(p)$ pour Alice et $(g^a mod(p))^b mod(p)$ pour Bob

[1] est primitif si il existe un v tel que $g^v = u \ mod p$ pour tout u allant de 1 à $p-1$

Infrastructure de Gestion de Clés Publiques (IGC)

Plus connu sous le nom anglais **PKI** (*Public Key Infrastructure*)

Problème

- *Risque de substitution d'identité (Man-in-the-middle)*
  Alice demande à Bob sa clé publique mais Charlie répond à sa place en fournissant la sienne
- *Impossibilité de mémoriser l'ensemble des clés publiques de tous les correspondants*

Besoin d'un tiers de confiance qui ait les fonctions suivantes :

- génération de clé privé et publique et attribution à une entité
- gestion de certificats
- diffusion de clés publiques

Certificat numérique

Définition

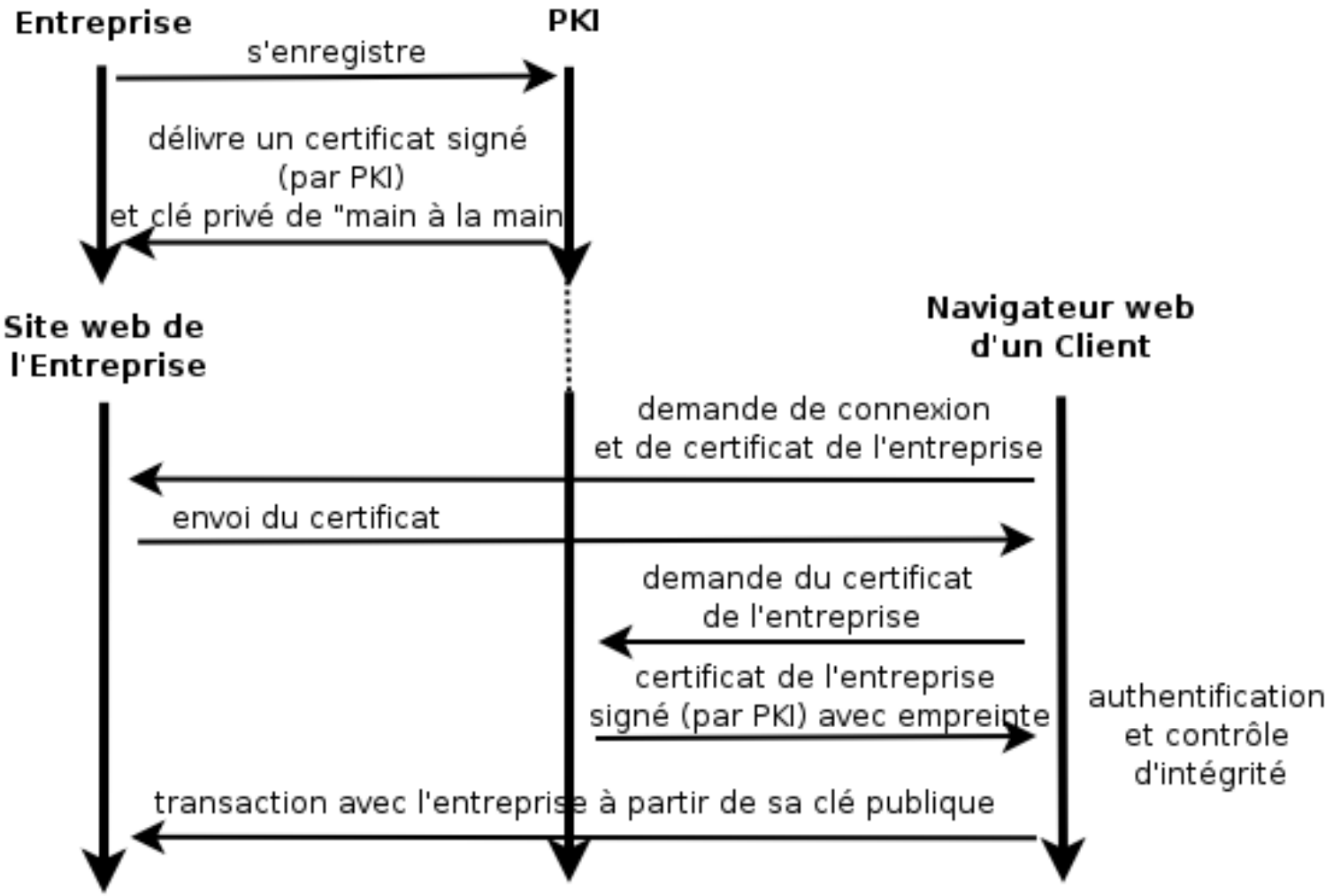
Certificat : carte d'identité numérique (clé publique) d'une entité signée et avec empreinte par un tiers de confiance

Contient

- Numéro de série
- Id. de son propriétaire
- Id de l'organisme délivreur
- Clé publique délivrée
- Période de validité
- Signature du certificat
- ...

Le format le plus courant provient du standard X.509 (voir le menu préférence de son navigateur)

Exemple de délivrance de certificats numériques



Quizz de synthèse sur la cryptographie appliquée à la sécurité des échanges

- Quels algorithmes me permettent d'assurer la confidentialité ? L'authentification ? L'intégrité ?
- Comment puis-je signer une message à l'aide d'un algorithme asymétrique ? à l'aide d'un algorithme symétrique ?