Sécurité des Systèmes d'Information(suite)

Nadia BENNANI*- Didier DONSEZ**
Université de Valenciennes
**Institut des Sciences et Techniques de Valenciennes
*IUT de Valenciennes
e-mail : {donsez,nbennani}@univ-valenciennes.fr

Sommaire

- La cryptographie
- Sécurité des échanges
- Sécurité du code mobile
- Sécurité de l'identité de l'utilisateur
- Sécurité des BDs
- conclusion

Sommaire

- **La cryptographie**
- Sécurité des échanges
- Sécurité du code mobile
- Sécurité de l'identité de l'utilisateur
- Sécurité des BDs
- conclusion

La cryptographie

Sommaire

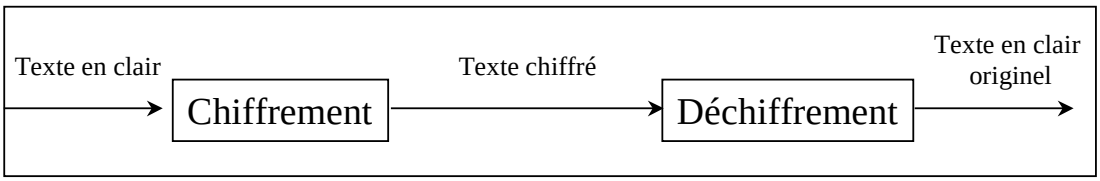
- Terminologie
- Les techniques cryptographiques
- DES: Un algorithme à clé symétrique
- RSA: Un algorithme à clé asymétrique
- Types de chiffrement
- Les protocoles cryptographiques
- Cryptanalyse
- Authentification
- Signature d'un document
- La certification
- La datation
- Intégrité de la conversation : les CAM
- La preuve électronique
- Les aspects législatifs

La cryptographie

Terminologie

La cryprographie:

Science permettant de préserver la confidentialité des messages



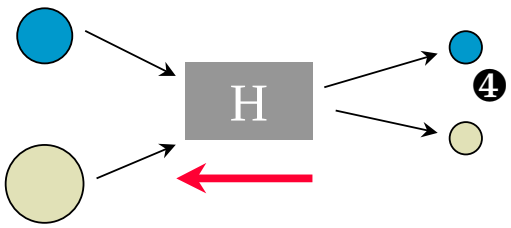
La cryptanalyse

L'art de décrypter des messages chiffrés

La cryptographie

Terminologie(2)

Les fonctions de hachage à sens unique



Proba pour que 2 nombres ait la même empreinte = $1/2^{160}$

La cryptographie

Les techniques cryptographiques

- Le brouillage
- Le chiffrement

Le brouillage

- algorithme privé
  - ex : code de César
    - i'bqnhr pt'b'drs bkzhq *j'crois qu'c'est clair*
    - hal *ibm (cf 2001 l'odyssée de l'espace)*
    - WNT *VMS*
  - ex : 1 bit sur 8 dans une image BMP

    la mafia s échangeait des photos de la « familia »
  - WinZip possède une fonction de brouillage
  - *plus de secret si l 'algorithme est connu*

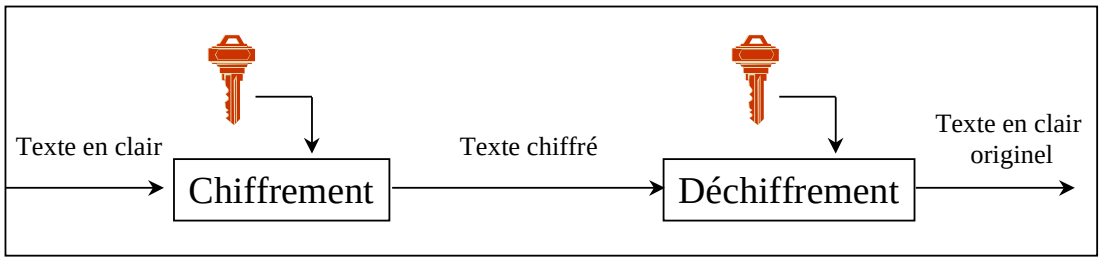
La cryptographie

Les techniques cryptographiques

- Le brouillage

  Algorithme restreint!

- Le chiffrement

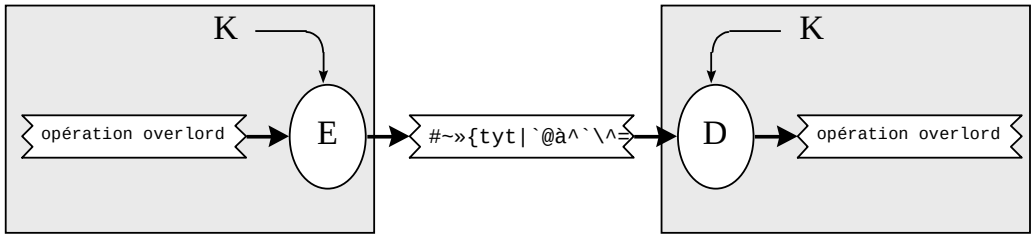


le Chiffrage (Cryptage)

- algorithme public
  - connu de tous
  - le secret est maintenue
    tant que la clé n'est pas connu
  - qui peut être propriétaire : royalties
- chiffrage à clé symétrique
  - (clé secrète)
- chiffrage à clé asymétrique
  - (clé publique / clé privée)

le Chiffrement à clé symétrique (clé secrète)

- 1 seule clé pour chiffrer et déchiffer



- DES (Decryption Encryption Standard - IBM 1977)
- IDEA,Le triple DES, TC2,TC4,...

le Chiffrement à clé symétrique (clé secrète)

Avantages

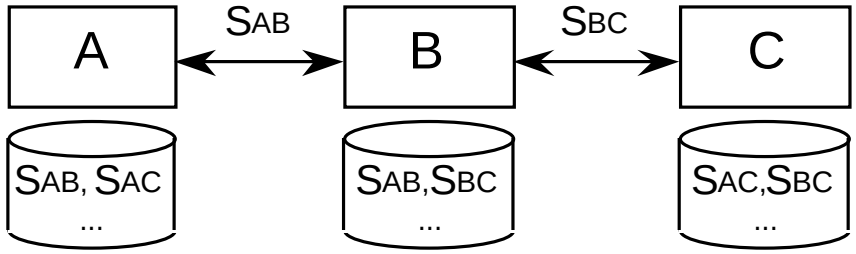
- Rapidité

Inconvénients

- Le problème de la transmission des clés
- Une clé par paire d'interlocuteur!

Echange par clé secrète

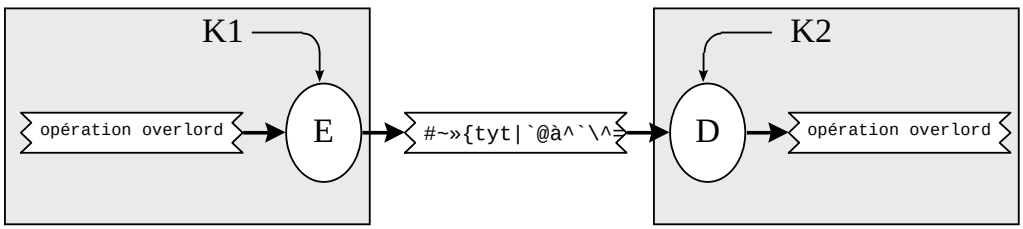
- Gestion exponentielle des Clés
- Echange “sûr” des clés entre les partenaires
- Risque de Trahison : *mais qui est le traître ?*



le Chiffrement à clé asymétrique (clé publique / clé privée)

- 2 clés K1 et K2
  - si chiffrage par K1, déchiffrage par K2
  - si chiffrage par K2, déchiffrage par K1

Remarque : on ne peut pas trouver une clé à partir de l'autre



- RSA *(Rivest Shamir Akermann)*

le Chiffrement à clé asymétrique (clé publique / clé privée)

Avantages

- Confidentialité
- Authentification de l'émetteur
  - Evite la non répudiation

Inconvénients

- Algorithmes très lents!

DES (Decryption Encryption Standard)

- Principe
  - Succession de Rouleaux de Permutation
    - Machine ENIGMA
- DES
  - 56 bits
  - Triple-DES (3*56 bits)
- Limite de DES
  - DES56 « cassable »
    - Juillet 98 : 56 heures par une machine à 250 000 $
      http://www.cdt.org/crypto/
  - Appel d 'offre du NIST pour un remplacant
    - AES (Advanced Encryption Standard)

RSA
(Rivest Shamir Akermann)

Génération des Clés de B

B sélectionne 2 nb. premiers p et q

B calcule γ(N) = ppcm(p-1,q-1)

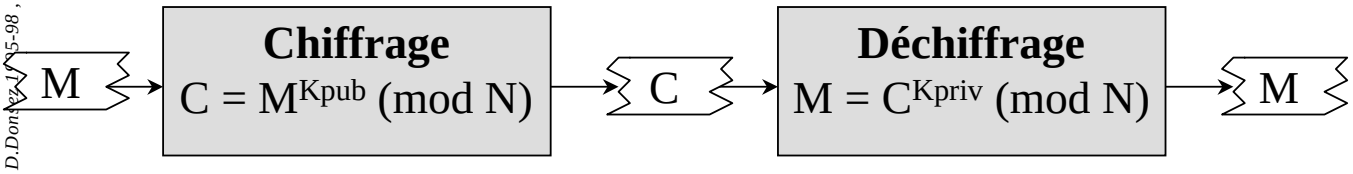
B tire la clé publique Kpub

B calcule la clé privée Kpriv

Kpriv * Kpub = 1 (mod(γ(N))

Privé
- *p, q nombres premiers*
- *Kpriv une clé secrète*

Public
- *N =p*q*
- *Kpub une clé publique*



RSA - Exemple

Génération des Clés de B

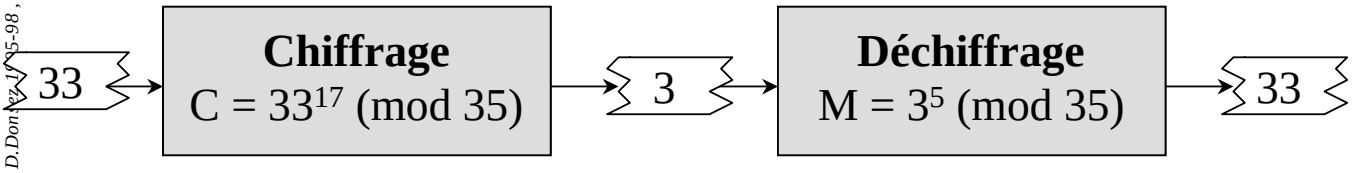
B sélectionne p=5 et q=7

B calcule γ(N=35) = ppcm(4,6)=12

B tire la clé publique Kpub=17

B calcule la clé privée Kpriv

Kpriv * 17 = 1 (mod(12) => Kpriv=5



La cryptographie

Types de chiffrement

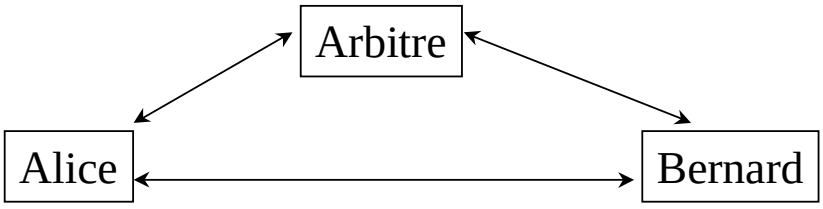
- Chiffrement en mode continu
- Chiffrement par blocs

  Taille des blocs : 64 bits

La cryptographie

Les types de protocoles cryptographiques

- Protocoles avec arbitre



Avantages	Inconvénients
Sûr	Ralentit les transactions
	Coûte cher

La cryptographie

Les types de protocoles cryptographiques(2)

- Protocoles avec juge-arbitre

Deux sous protocoles :
- Sans l'intervention du juge
- Intervention du juge en cas de contestation

➡ Coûte moins cher.

La cryptographie

Les types de protocoles cryptographiques(2)

- Protocoles à discipline intrinsèque

Pas d'intervention de juge

Le moins cher

☞ N'est pas applicable à toutes les situations

Attaques d'un protocole cryptographique

Attaquer :

- Le protocole lui-même
  - Attaque passive
  - Attaque active
- L'algorithme cryptographique utilisé
- Les techniques cryptographiques
  - L'échange de clé
  - Le transfert de clé
  - La phase d 'identification...

La CryptoAnalyse

- Attaque d'un chiffrage
  - l'attaquant cherche à connaître
    - le texte en clair
    - la clé « secrète ou privée » utilisée
  - à partir d'un texte encodé : très difficile
  - à partir du texte clair et du texte encodé : faisable

    Attention aux en-têtes de formulaires !!!!

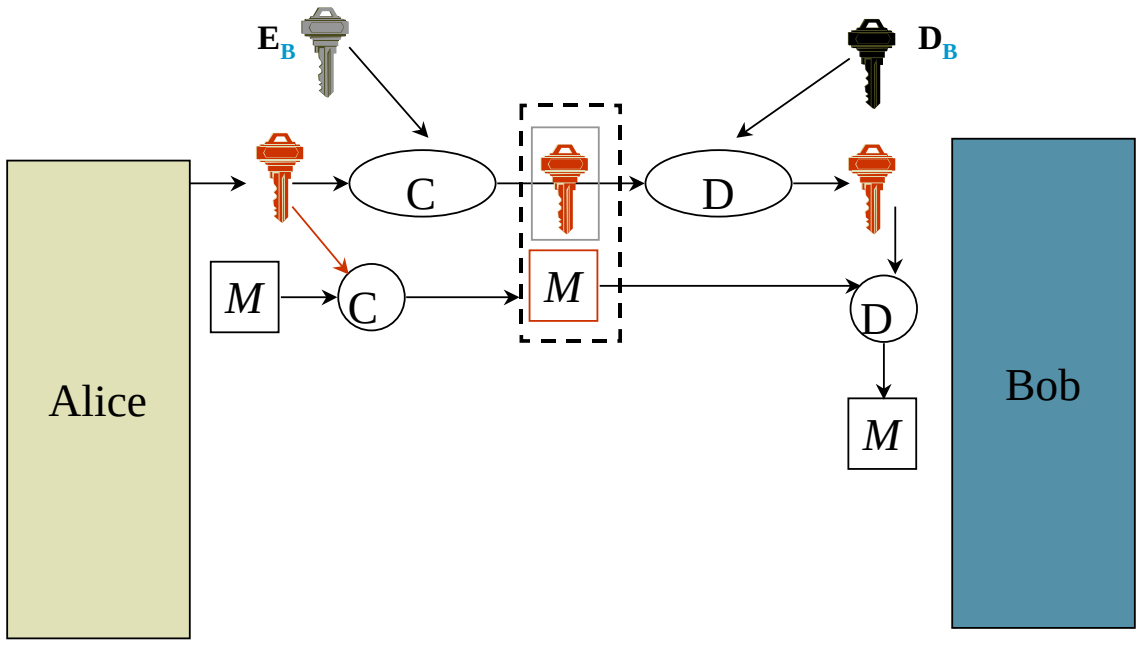
Protocoles cryptographiques

Algorithmes utilisés

- Echange par clé secrète
  - Cryptographie à clé symétrique
- Echange par clé privée / clé publique
  - Cryptographie à clé asymétrique
- Echange hybride
  - Echange d'une clé secrète K
    par Cryptographie à clé asymétrique
  - Echange par clé secrète (K)

Protocoles cryptographiques

Exemple de protocole hybride

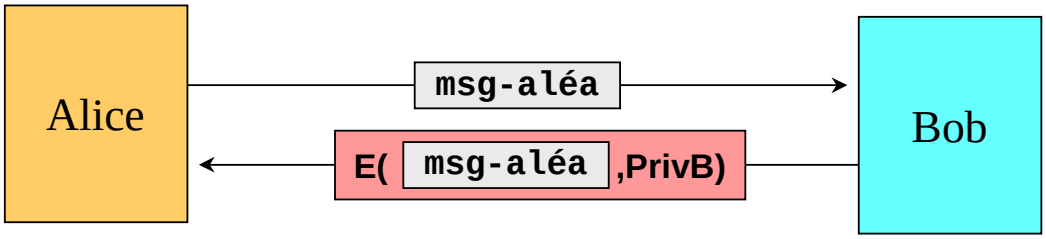


Protocole de sécurisation des données

- Phase 1 : authentification des partenaires
  - certification
- Phase 2 : échange sécurisé d 'une clé secrète pour la session
- Phase 3 : échange sécurisé des messages
  - algorithme à clé secrète
  - intégrité et sans playback

L'authentification

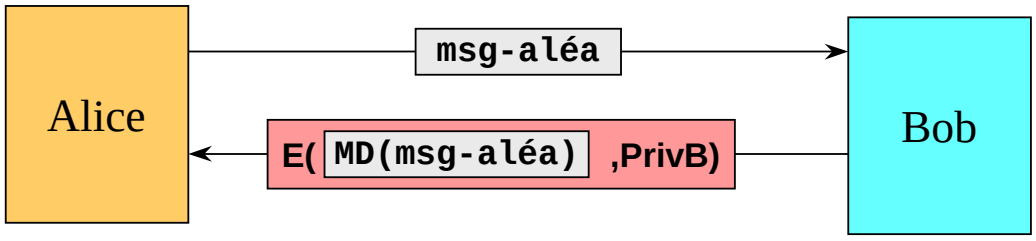
- proposition
  - Protocole



  - Problème
    - attaque de la clé privée de B à partir du message en clair et de son chiffrement.

L'authentification (2)

- Technique:
  - calculé un résumé (digest) difficile à "inverser".
    - fonctions sécurisées de hachage
      MD4, MD2, MD5 (Message Digest)



La cryptographie

Signature numérique

Rôle: permet d'authentifier l'interlocuteur.

Qu'est ce qu'une bonne signature?

- L'authenticité
- Infalsifiable
- Non réutilisable
- Le document signé est inaltérable
- On ne peut la renier

La cryptographie

Signature numérique — Les protocoles

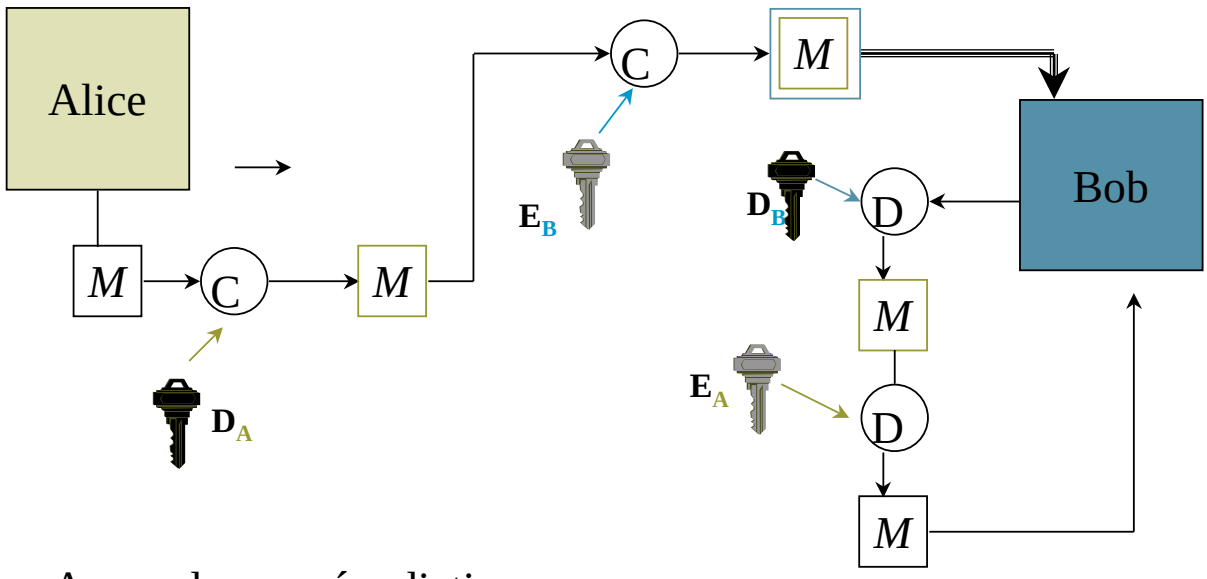
- Utilisation d'un cryptosystème à clé secrète
  - Protocole avec arbitre => Goulot d'étranglement
  - Cher en stockage: archivage des documents signés
- Utilisation d'un cryptosystème à clé asymétrique

L'idée: Alice signe un document

- Alice chiffre un document avec sa clé privée
- Vérifier l'identité d'Alice: Déchiffrer le document avec la clé pulique d'Alice.

La cryptographie

Signature numérique — Echange sécurisé d'un document signé

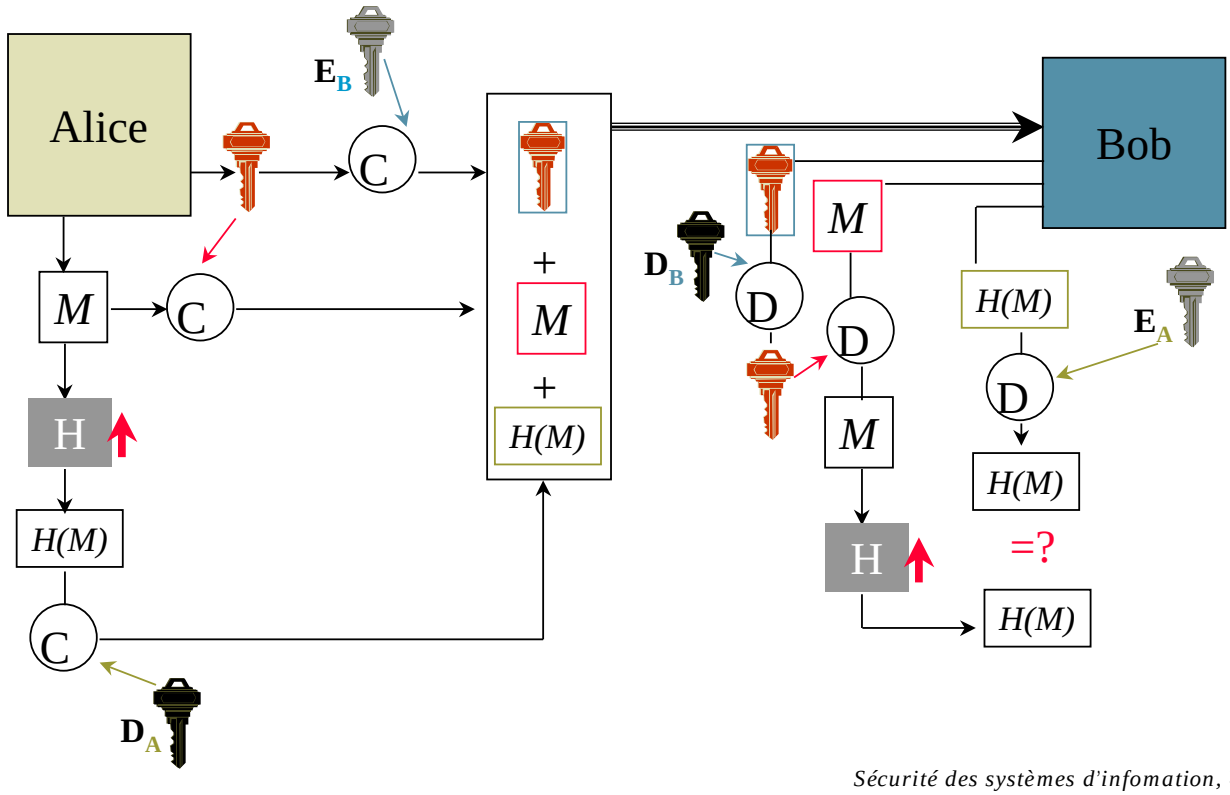


Assure la non répudiation

La signature est lente!

Echange sécurisé d'un document signé

Utilisation d'une empreinte numérique



Echange sécurisé d'un document signé

Utilisation d'une empreinte numérique(2)

Intérêt:

- Signature gardée indépendamment du document
- Moins gourmande en espace
- Chiffrement plus rapide avec un algorithme à clé asymétrique

Gestion des clés

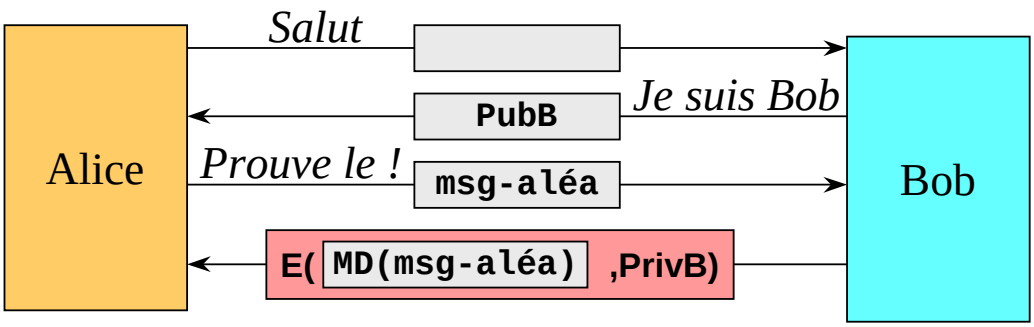
1/Echange des clés de session

- Echange des clés de session
  - ➤ Protocoles à clé symétrique:
    - Avec et sans arbitre
  - ➤ Protocoles à clé asymétrique
  - ➤ Protocoles utilisant la signature numérique

Gestion des clés

2/Echange des clés publiques

- Proposition



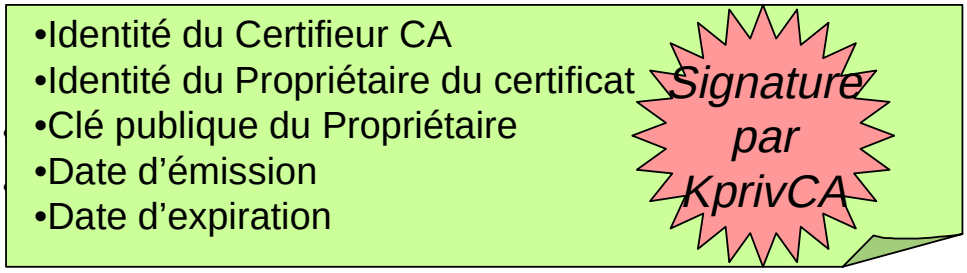
- Problème
  - n'importe qui peut se faire passer pour Bob et communiquer une fausse clé publique.

La Certification

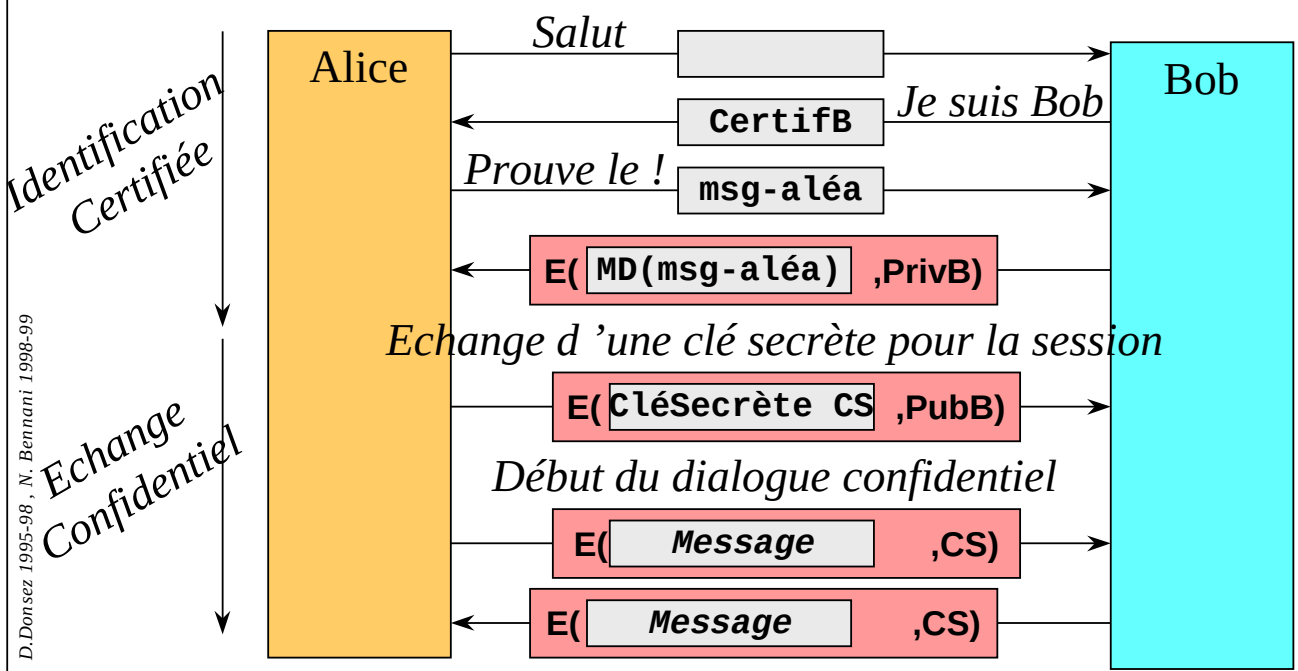
- Technique:

  communiquer son certificat émis et signé
  par une tierce partie CA (Certifying Authority)

  - Le certificat (ISO X509)



L'Identification Certifiée



Certifying Authorities (CA)

«Notaire Electronique»

Service de délivrance de Certificat (X509)

Service de Datation de Documents

- Des Acteurs :

  VeriSign, Canada Postal Service, GTE, CommerceNet ...

- Des Produits :

  Certificate Server de Netscape

  » génération et gestion propre des certificats

- Hierarchie des CA.
- 3 autorités: l 'enregistrement, gestion des certificats, direction des révocation

Service de Certification (i)

- commercialise et émet des certificats à la norme ISO X509

- Procédure de délivrance des certificats

  définit par le CA (pièces notariales, ...)

- CIS (Certificate Issuing System)

  processus sécurisé de fabrication des certificats

  plusieurs opérateur humains indépendants

Service de Certification (ii)

- CRL (Certificate Revocation List)
  - liste des certificats corrompus ou invalidés
  - certificat “cassé”
  - certificat d’un employé licencié
  - Consultation : push, pull
- Problème
  - validité d’un certificat dans les contrats long terme.

Service de Datation

- DTS (Digital Time Stamp)
  - DTS(Document, Date)
    = { Document+ Date } clé_privée_du_CA
  - Processus Confidentiel de Datation:
    - A envoie un **digest** de son document au CA
    - CA retourne une DTS (**digest** , date_garantie_par_le_CA)
  - Problème
    - validité d’une DTS pour un contrat long terme
      => attaque d’un testament ... 15 ans après

Identification

- auprès du réseau
  - coté réseau
    - serveur d'accès

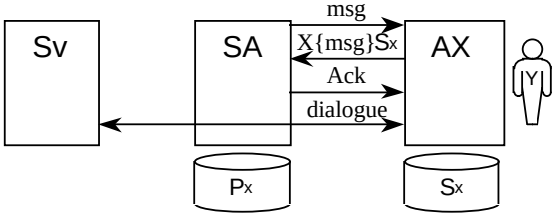
      parfois c'est une fonction du Firewall
  - Coté Terminal
    - Stockage de la clé privée

      Fichier, Carte Magnétique, Carte à Puce, Calculette

Stockage des Clés Privées (i)

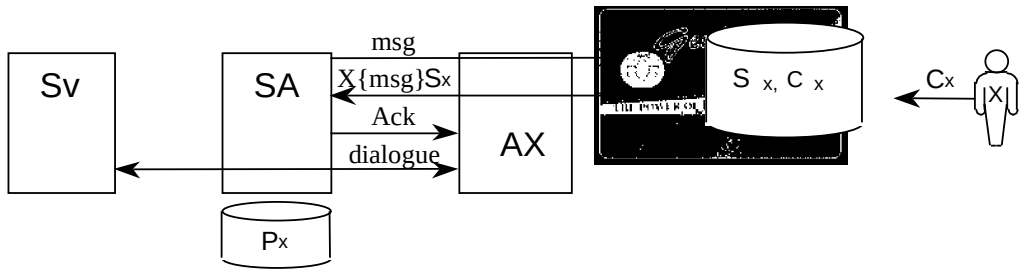
- Fichier ou Carte Magnétique

  - Lecture du fichier contenant la clé privée, Perte/Vol
  - Duplication de la carte magnétique



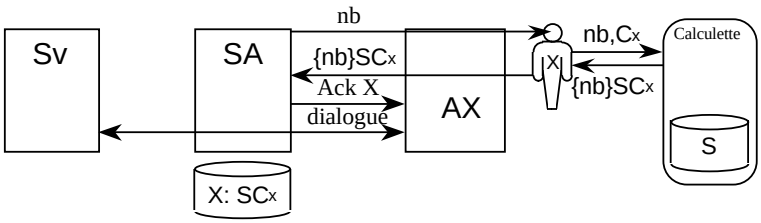
Stockage des Clés Privées (ii)

- Carte à Puce (GemPlus, Schlumberger, JavaCard Forum, ...)
  - Nécessité d'un lecteur ISO par ou sans Contact
  + Lecteur ISO PCMCIA



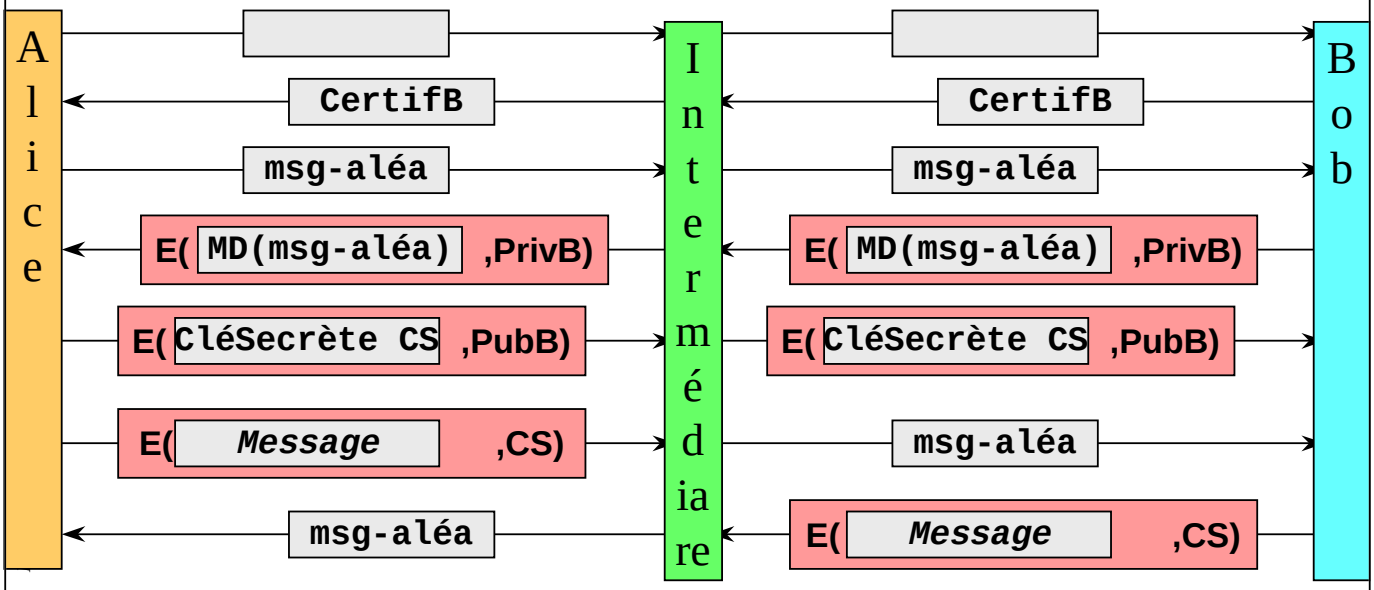
Stockage des Clés Privées (iii)

- Calculette (ActivCard, SecurId, ...)
  - Algorithmes souvent propriétaires
  - Délai d'initialisation : lecture et 2 frappes sans erreur !
  + Accès à des applications par des Serveur Vocaux
    NB: algorithme SecurID dans modems PCMCIA



L'intégrité de la Conversation

- Problème : l'interception des messages



L'intégrité de la Conversation(2)

- Correction
  - MAC : Message Authentification Code
    - ajouter au message échangé une authentification du message
    - MAC : = MD [conversation, clé_secrète]
- Protection contre le playback
  - un numéro de séquence de message ou un numéro aléatoire

La Preuve Electronique

- Dématérialisation du Papier
  le “Zéro Papier”
  - Nécessité d’une preuve électronique
    non répudiable
    - Signature et Datation

La Preuve Electronique aux USA

- en cours de légalisation
  dans les états de Californie, NewYork et Utah.
- Principe d’un contrat papier avec signature manuscrite amenant les deux parties à accepter la signature digitale des futurs documents à échanger.
- le contrat papier spécifie également la méthode de signature et la taille minimum des clés utilisées.

La Preuve Electronique en France

Utilisation Légale des Outils de Chiffrage

- Usage:
  - Certification et Intégrité ("Signature Electronique")
  - Confidentialité
- Dans le Monde
  - Remarque:

    les USA, le Canada interdisent l'exportation de matériel de chiffrage performant (DES < 56 bits est autorisé à l'export depuis le 1/1/97 par le NSA)

  En France

    Pas de règlement pour l'importation

Situation actuelle en France (i)

- 2 organismes
  - SCSSI : Service Central de la Sécurité des Systèmes Informatiques relevant du Premier Ministre
    - contrôle du chiffrage
  - CNIL : Commission Nationale de l'Informatique et des Libertés
    - maintien de la confidentialité dans le secteur médicale
      impose le chiffrage des données personnelles

Commission Nationale de l'Informatique et des Libertés

Situation actuelle en France (ii)

- Intégrité, Authentification, Signature
  Déclaration au SCSSI
- Confidentialité (i.e. chiffrage)
  Demande au SCSSI : réponse lente, très lente.
  Les outils doivent plutôt fonctionner
  suivant le **principe du séquestre des clés**
  - Exemple
    Interdiction de télécharger PGP
    » 6 mois de prison et 200 000 FF d'amende

Echanges Sécurisés avec séquestre des Clés

- 3 partenaires dans l 'échange
  - Alice et Bob
  - Un Tiers de Confiance
- Principe
  - Le tiers de confiance archive la clé de session (DES)
  - Le SCSSI peut inspecter une session passée en récupérant la clé de session auprès du tiers
- Solutions :
  - Agrément SCSSI
  - STOOL de CESIR, MatraNet (www.matranet.com), ...

Situation actuelle en France (iii)

- Tiers de Confiance
  - algorithme permettant le séquestre des clés
    - clé publique / clé privée
    - clés de session !!!
  - TC : "notaire" conservant les clés
  - probablement 1 par secteur d'activité
    - santé, bancaire, assurance ...

Le Futur en France

Loi prévue dans les mois qui viennent...

(Discours de Lionel Jospin [19/01/99])

- La législation de 1996 ne serait plus adaptée
- Liberté complète pour l'usage de la cryptographie
- Le tiers de confiance ne serait plus obligatoire

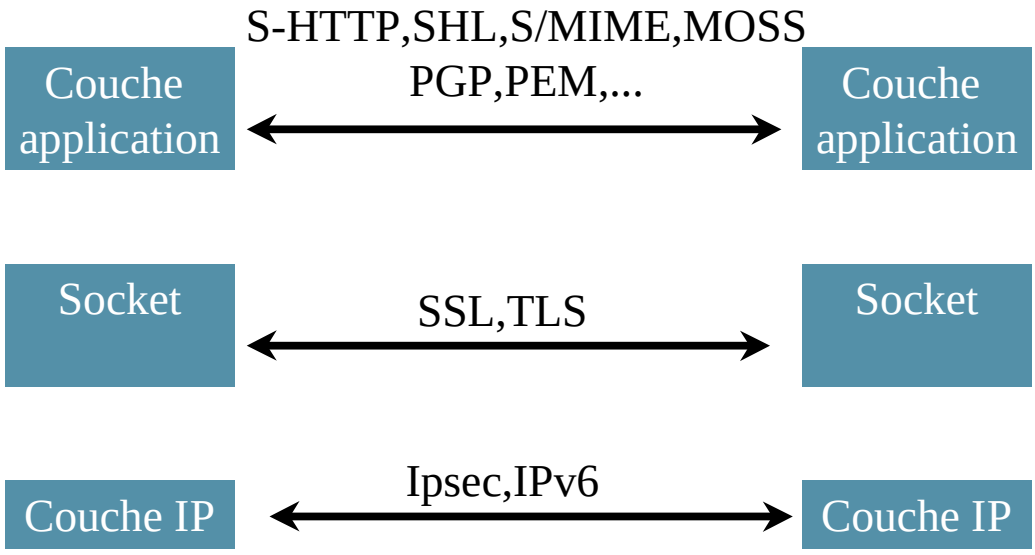
Dans l'attente de la dite loi...

Utilisation libre de cryptosystèmes dont les clés < 128 bits

Sommaire

- La cryptographie
- **Sécurité des échanges**
- Sécurité du code mobile
- Sécurité de l'identité de l'utilisateur
- Sécurité des BDs
- conclusion

Sécurité des échanges



Sécurité des échanges

Couche application

- Applications sans Connexion (ou Datagramme)

  Authentification et Intégrité avec/sans Confidentialité de courriers électroniques

- Applications Conversationnelles (avec Connexion)

  dialogue entre deux applications

  Authentification et Intégrité avec/sans Confidentialité

Échanges Sécurisés

Couche application — en mode datagramme (i)

- PGP (Pretty Good Privacy)
  - Auteur: Phil Zimmermann
  - RSA et IDEA
  - Pas de certificat: climat de confiance
  - Freeware MIT, produits ViaCrypt et RSA Data Security
  - Disponible pour Unix et Mac et Windows en shareware
  - Imcompatible avec MIME

- PEM (Privacy Enhanced Mail) RSA et DES, Certificats X509
  - Type de certificat : hierarchisées
  - Message chiffré puis signé
    - => Forward : Non sûr
  - Commercialisé par RSA(TIPEM),TIS(TISPEM),...
  - assez compliqué à mettre en œuvre

Échanges Sécurisés

Couche application — en mode datagramme (ii)

- PGP/MIME
  - RSA et IDEA, étudié par l'IETF
- S/MIME
  - RC2 et DES, proposé par RSA Data Security
  - étudié par l'IETF
  - Certificat : Pas de hierarchie
  - Intégration du chiffrement et de la signature comme type de contenu
- MOSS (MIME Object Security Services)
  - étudié par l'IETF (RFC 1847-8)
  - les messages sont signés puis cryptés
    - => Destinataires multiples, Un forward sûr

Échanges Sécurisés

Couche application — en mode datagramme (iii)

- MSP (Message Security Protocol)

  environnement X400 puis environnement IP

  étudié du NSA (National Security Agency), norme NIST

  RSA et DES

Échanges Sécurisés

Couche application — en mode datagramme (iv)

- Gestion des Clés (KMP)

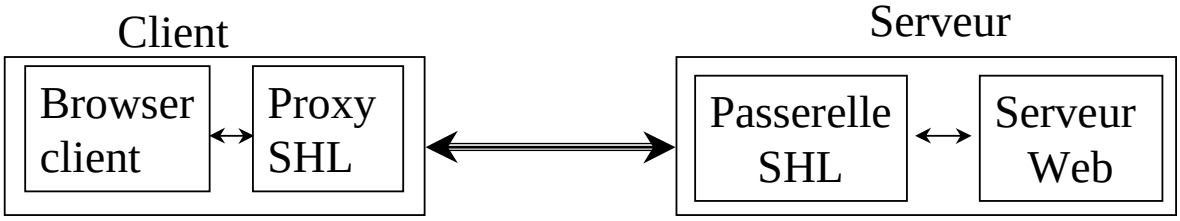
  Key Management Protocol

  - SKIP (Simple Key management for IP)
    - » développé par Sun,
    - » public, soumis à l'IETF et l'ANSI.
  - PSKMP (Photuris Session KMP)
    - » développé par le WG IPSec de l'IETF.
  - ISAKMP (Internet Security Association KMP)
    - » supporté par la NASA.

S-HTTP (Secure HTTP)

- Terisa System fondé par RSA et EIT
  et soutenu par
  America Online, Compuserve,
  Prodigy, IBM, CommerceNet
- Sécurisation du protocole HTTP (niveau 7)
- Accepte différents systèmes de gestion des clés
- Potentiel supérieur à SSL
- Client et serveur peuvent négocier leur politique

SHL (Secure HTTP Layer)



Proposé par MSI (http://www.msi-sa.fr)
Chiffrement, intégrité et authentification (v.2.0)
Triple DES 128 (bientôt 192bits), RSA(1024 bits)
Chiffrement sélectif
Un peu plus lent que SSL

La couche Socket

SSL (Secure Socket Layer)

- Netscape, MasterCard, Bank of America, MCI et SGI
- Se compose de trois protocoles
- chiffrage par clé symétrique (DES, RC4)
- intègre (MAC par MD2, MD5)
- authentification : serveur toujours / client optionel

La couche Socket

SSL (Secure Socket Layer)(2)

Les problèmes

Problème d'aléa

Faiblesse des versions internationales (respect de la loi d'exportation américaine)

Le point fort

Applicable à n'importe quelle application.

SecureNet

- Terisa System et Netscape
- But:
  - supporter à la fois
    SSL et S-HTTP

Échanges Sécurisés

Avantages & Inconvénients

- Couche application
  - Non-Répudiation
  - Certification
  - Adaptée aux besoins de l'application
- Couche Socket
  - Indépendance / plateforme
  - Applicable quelque soit l'application
  - Ne traite pas la non répudiation

Échanges Sécurisés

Avantages & Inconvénients(2)

- La couche IP
  - Transparence / utilisateur et l'application
  - Endigue les attaques: trucage IP, écoute
  - UDP (User Datagram Protocol)
  - Changement de la structure IP : complexe
  - Ralentit le débit du réseau

Sommaire

- La cryptographie
- Sécurité des échanges
- **Sécurité du code mobile**
- Sécurité de l'identité de l'utilisateur
- Sécurité des BDs
- conclusion

La sécurité des codes mobiles (i)

Qu'est ce qu'un code mobile ?

- un code disponible sur un serveur de fichiers (httpd)
- le chargement de ce code sur votre client
  - pour installation ou mise à jour
    HTTP
    ou « push »
- l 'exécution de ce code sur votre client
  - en général, encaspuslé dans un page HTML
    joué par un butineur Web (browser)
- Risque
  - Virus, Usurpation d 'identité derrière un Firewall, ...

La sécurité des codes mobiles (ii)

- Java, CAML, TeleScript, JavaScript ...
  - bytecode interprété
    - contrôle de code au chargement
    - applications
      applets (appliquettes en vf), servlets, « aglets » (agents mobiles), le « push »

- Sécuriser l'usage des codes mobiles
  - bytecodes non signés
    - Bac à sable (Sandbox)
      pas d 'accès aux ressources du poste
      connexion réseau seulement vers le serveur d 'origine
  - bytecodes signés
  - Le «firewalling»
  - Proof carrying Code

Sommaire

- La cryptographie
- Sécurité des échanges
- Sécurité du code mobile
- **Sécurité de l'identité de l'utilisateur**
- Sécurité des BDs
- conclusion

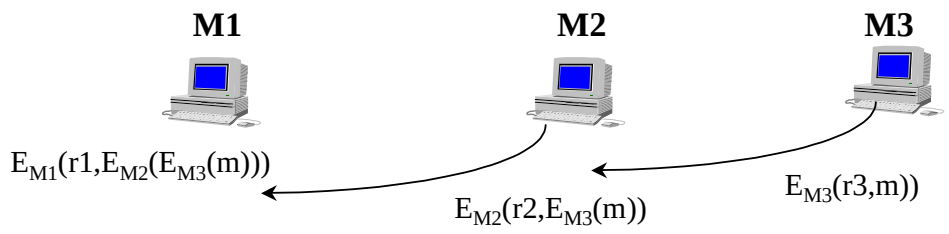
Sécurité de l'identité de l'utilisateur

Le problème:

Comment préserver l'anonymat des utilisateurs d'Internet?

Solutions:

- Les «mixs»



Sécurité de l'identité de l'utilisateur (2)

- Les «proxys»
- Les «crowds»

  UNIX, Windows

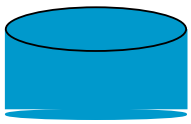
Sommaire

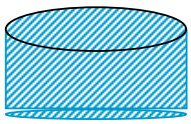
- La cryptographie
- Sécurité des échanges
- Sécurité du code mobile
- Sécurité de l'identité de l'utilisateur
- **Sécurité des BDs**
- conclusion

Sécurité des Bases de Données

Enreg

Index | E(Enreg)





BD

Méta-BD

Index = f(nom)

Sommaire

- La cryptographie
- Sécurité des échanges
- Sécurité du code mobile
- Sécurité de l'identité de l'utilisateur
- Sécurité des BDs
- **conclusion**

Validité d'un Chiffrage

- dépendant de la nature de la donnée à protéger
  - transaction bancaire
    - » quelques minutes
  - secret d'état, signature de contrat à long terme
    - » 50 ans
- dimension de la clé
  - plus la clé est grande, elle est difficile à casser
- Evolution de la technologie
  - Augmentation constante de la puissance de calcul
  - Le coût diminue (/10) tous les 5ans

La sécurité n'est pas statique !

- Liste de diffusion
  - CERT (Computer Emergency Response Team)
  - IETF (Internet Engeneering Task Force)
    - Alerte à Malibu !
- Audit Sécurité
  - 20% du budget "Sécurité" par an

Bibliographie (i)

- Cryptographie

  Applied Cryptography, by Bruce Schneier (Wiley), ISBN 0-471-59756-2 (ISBN 2-84180-036-9 en VF)

- Législation

  www.cnil.fr

  Echange de Données Informatisé : Contrôle et audit d'un système EDI, AFNOR & EDIFRANCE 1994, ISBN 2-12-481312-9.

  G. Beaure d'Augère, P. Bresse, S. Thuillier, «Paiement numérique sur Internet», Ed ITP France, 1997, ISBN 2-84180-160-8

Bibliographie (ii)

- Sécurité des Systèmes UNIX

  Unix System Security: A Guide for Users and System Administrators by David Curry, O'Reilly

  Practical Unix Security, by Simson Garfinkel and Gene Spafford,O'Reilly,ISBN 0-937175-72-2

- Internet Security Alerts
  - RISKS

    Forum on Risks to the Public in Computers and Related Systems, http://catless.ncl.ac.uk/Risks
  - CERT

    ftp://ftp.cert.org/pub/cert_advisories/

Bibliographie (iii)

- Sécurité des Serveurs Web

  How to Set Up and Maintain a World Wide Web Site: The Guide for Information Providers, by Lincoln D. Stein (Addison-Wesley), ISBN 0-201-63389-2

  Managing Internet Information Systems, by Cricket Liu, Jerry Peek, Russ Jones, Bryan Buus, and Adrian Nye (O'Reilly), ISBN 1-56592-051-1

- Firewalls

  Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steven M. Bellovin,Addison-Wesley, ISBN 0-201-63357-4

  Building Internet Firewalls, by D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly, 1st Edition September 1995, ISBN 1-56592-124-0

Bibliographie (iv)

- CORBA

  CORBA 2.1, «Security Service Specifications», OMG 1997

Vos suggestions et vos remarques

- Merci de me les retourner à
  - Didier DONSEZ, donsez@univ-valenciennes.fr, Fax 03 27 14 11 83
- Avez vous trouvé ce cours instructif ?
  - Est il complet ?
  - Qu 'est qu 'il manque ?
  - Qu 'est que vous auriez aimé voir plus développé ?
  - Est il bien organisé ?
  - ...
- Quels sont votre fonction et votre domaine d 'activité ?