3ème année

Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo
RSSI - CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - **Cryptographie**
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Terminologie

- Cryptologie = cryptographie + cryptanalyse
  - Cryptographie (κρυπτος = caché) :
    écrire des messages incompréhensibles par des tiers
  - Cryptanalyse : découvrir le(s) secret(s), décrypter

- A ne pas confondre avec stéganographie
  (στεγανος = couvert) → encre sympathique
  filigranes (tatouages)

- Chiffre, chiffrement (pas chiffrage, ni cryptage), déchiffrement, clair, cryptogramme

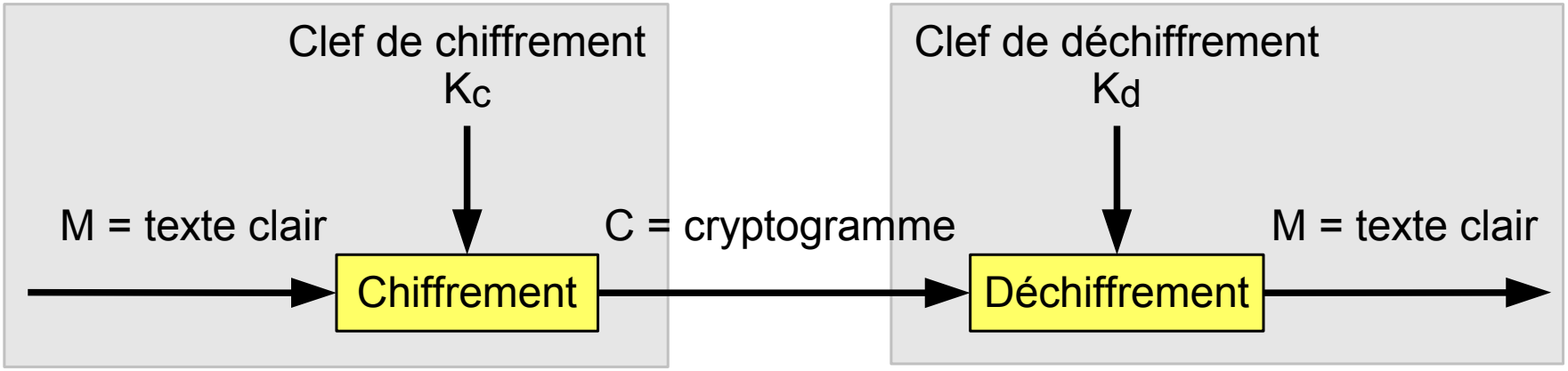
Préambule (1/2)

- C'est un des domaines des mathématiques qui a connu les avancées les plus considérables de la fin du 20ème siècle
  - Il y a rarement des preuves mathématiques générales (de solidité) dans ce domaine
  - Les chiffres se cassent
  - L'implémentation est très délicate, elle casse aussi
  - Il y a peu d'experts et même sans doute de connaisseurs
- C'est difficile et souvent contre-intuitif
  - exemple: chiffrer deux fois peut être dangereux

Préambule (2/2)

- La levée de la main-mise des militaires sur ce domaine est récente et non-vérifiable
- Les difficultés théoriques sont doublées de difficultés réelles d'implémentation
  - exemple: générateurs aléatoires, génération des clefs, protection des clefs, remplissage des blocs vides, etc.
  - notamment au niveau de la mise en oeuvre matérielle

Chiffrement (confidentialité)



- Notation chiffrement $C = \{M\}_{Kc}$
  déchiffrement $M = [C]_{Kd}$
- Confidentialité
  - Sans connaître Kd, il doit être « impossible » de retrouver M
  - Il doit être « impossible » de trouver Kd, même connaissant C et M (attaque par « clair connu »)
  - Il doit être « impossible » de trouver Kd, même connaissant C en choisissant M (attaque par « clair choisi »)

Chiffres symétriques $K_c = K_d (= K)$

- Tous les chiffres connus jusqu'en 1976 !
- Exemples
  - DES (1976)
    - clefs de 56 bits (+8 bits de parité)
    - blocs de 64 bits
  - AES (2000)
    - clefs de 128, 192 et 256 bits
    - blocs de 128 bits

Chiffres à clef publique $K_c \neq K_d$

- Connaissant Kc, il est «impossible» de trouver Kd
  - Kd est privé (seul celui qui connaît Kd peut déchiffrer)
  - Kc est public (tout le monde peut chiffrer): répertoire de clés publiques
- Ex.: RSA (1976)
  - Appuyé (probablement) sur le problème de la factorisation des grands nombres

  $e \cdot d \equiv 1 \bmod((p-1)(q-1))$ $K_c = \{pq, e\}$ $K_d = \{p, q, d\}$
- Ex.: El Gamal (1985)
  - Basé sur la difficulté du calcul du logarithme discret dans un champs fini
  - $y = g^x \bmod p$ $K_c = \{x\}$ $K_d = \{y, g, p\}$

ou-exclusif : un chiffre embarrassant

- $C = M \oplus K$ et $M = C \oplus K$
- Aucune sécurité
  - Calculer $C \oplus C_{\gg k}$ pour k = { 1, 2, ... } et compter les octets identiques. L'indice de coincidence indique la longueur de la clef n (en octets).
  - $C \oplus C_{\gg n} = M \oplus M_{\gg n}$ élimine la clef.
  - On retrouve le message en exploitant les redondances du message d'origine (1,3 bit d'information par octet en anglais ASCII par exemple).
  - Cryptanalyse en quelques minutes.

NB: C'est un chiffre polyalphabétique de Vigenère (1523-1596)

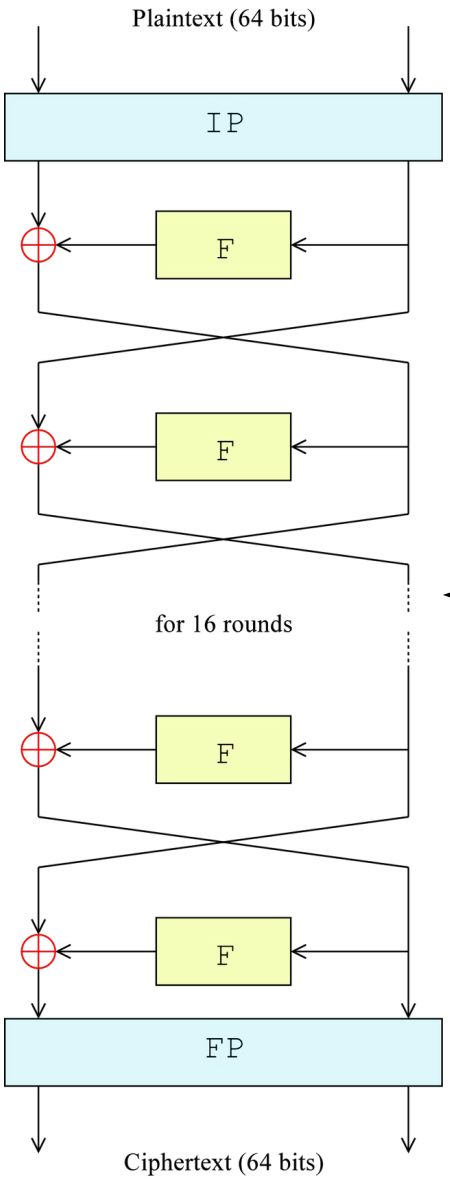
One-time pad : un chiffre parfait

- La clef est une suite de bits aléatoire aussi longue que le message et l'algorithme est le ou-exclusif
  - $C_i = \{M_i\}_{K_i} = M_i \oplus K_i$
  - $M_i = [C_i]_{K_i} = C_i \oplus K_i$
- D'après la théorie de l'information (Shannon), c'est un chiffre incassable (si la clef n'est **jamais** réutilisée)
  - Peu pratique
  - Envisageable

DES : Data Encryption Standard (1975)

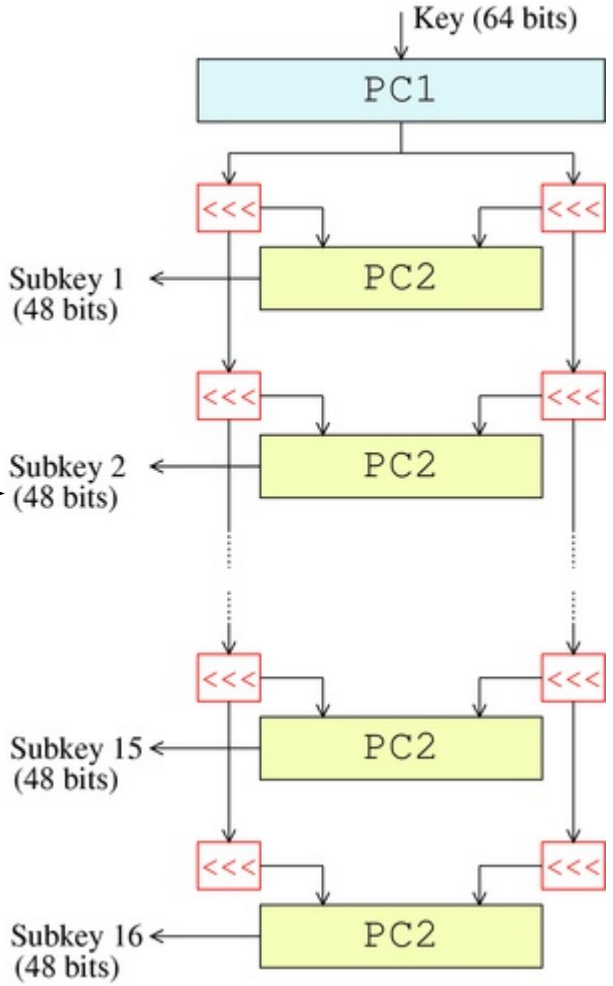
- Historique
  - Une base issue d'IBM. Des améliorations de la NSA.
  - Le premier algorithme controlé par la NSA rendu public... par l'organisme de standardisation.
- Bloc de 64 bits. Clef de 56 bits + 8 bits (ex.: parité)
- Conception orientée vers une mise en œuvre *hardware*
- 3DES : amélioration (générique) répandue
  - clef de 112 bits
- Énormes efforts publics de cryptologie
- Beaucoup de variantes (ex.: *key-dependent S-boxes*)

DES



Chiffre de Feistel

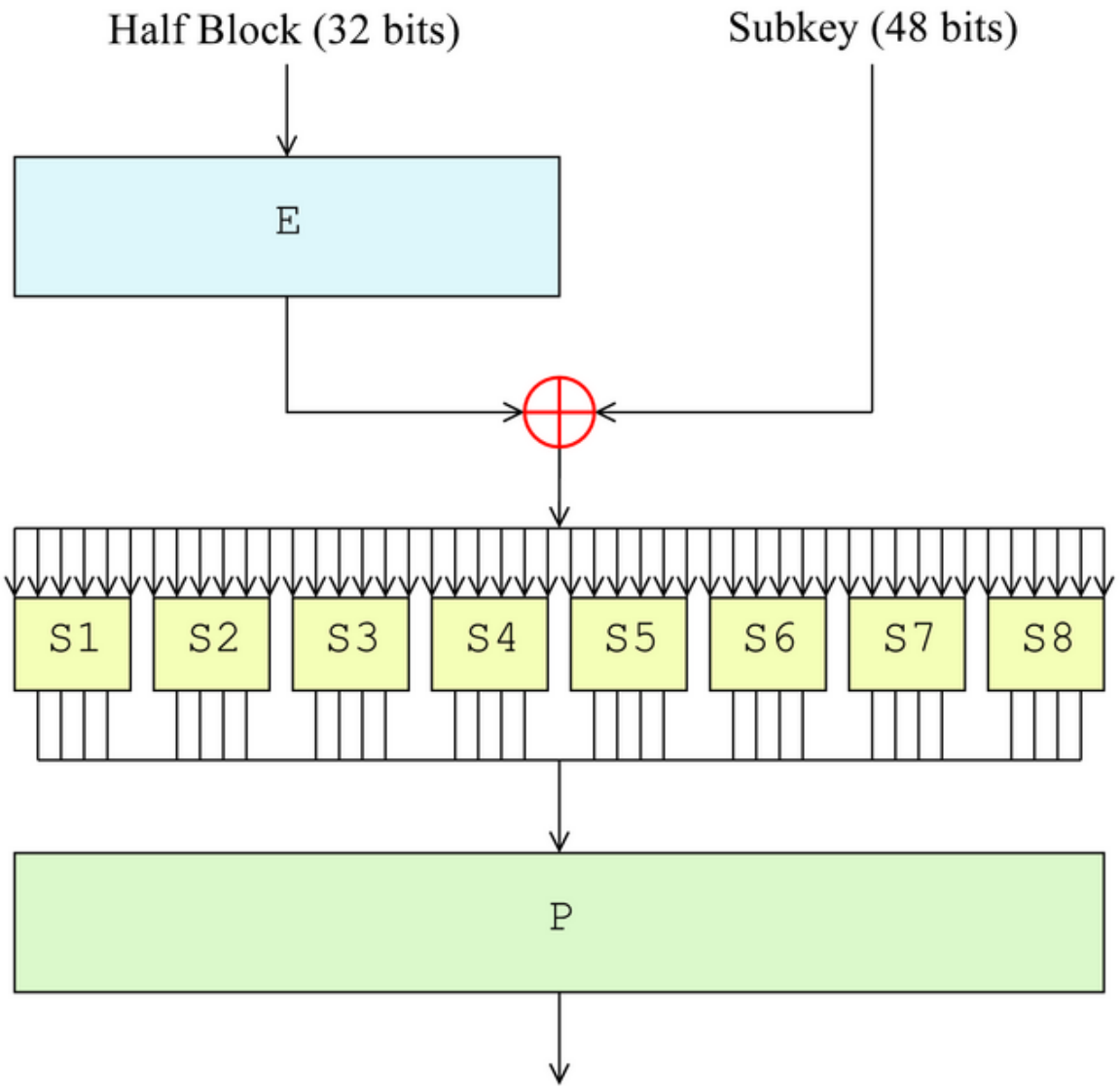
Key schedule



IP: Initial permutation
FP: Final permutation
PC:Permuted choice

http://en.wikipedia.org/wiki/Data_Encryption_Standard

DES

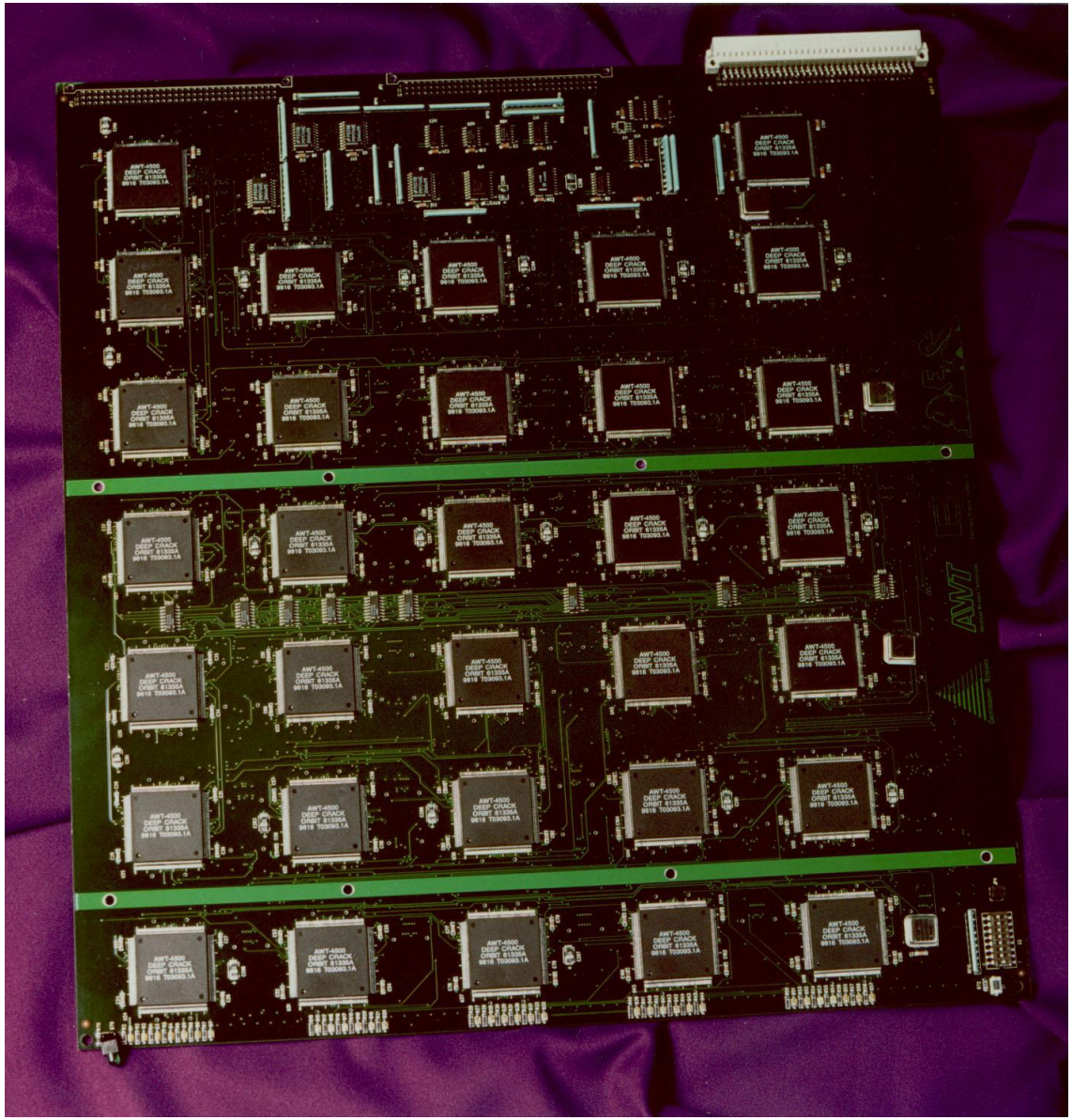


F

E: Expansion
(32 bits → 48 bits)
⊕: *Key mixing*
S1,S8: Substitution *S-boxes*
(6 bits → 4 bits)
P: Permutation *P-box*
(32 bits)

DES

Electronic Frontier
Foundation
DES Cracker
“Deep Crack”
~5 jours



Modes de fonctionnement des chiffres symétriques

$M = M_1 \cdot M_2 \cdot \ldots \cdot M_n$ $C = C_1 \cdot C_2 \cdot \ldots \cdot C_n$

- ECB – *Electronic Codebook*
  - $C_i = \{M_i\}_K$
  - $M_i = [C_i]_K$
- CBC – *Cipher Block Chaining*
  - $C_i = \{M_i \oplus C_{i-1}\}_K$
  - $M_i = C_{i-1} \oplus [C_i]_K$
  - IV sorte de M_0
- Stream ciphers
  - CFB – Cipher Feedback Mode
  - OFB – Output Feedback Mode

Avantages des chiffres symétriques

- Rapides
  - ~1 Gb/s par hard
  - ~100 Mb/s par soft
- Clefs « courtes »
  - typiquement 80 bits pour résister aux attaques brutales (aujourd'hui)
- Pratiques pour chiffrer des fichiers personnels (pas de clef à partager)

Problèmes des chiffres symétriques

- En communication, la clef secrète est partagée
  - l'émetteur et le récepteur doivent se faire confiance, et garder soigneusement la clef secrète

- Comment distribuer ou renouveler la clé ?
  - Chiffrer la nouvelle clé de session avec l'ancienne
  - Chiffrer la clé de session avec une clé spécifique de chaque matériel ⇒ site de confiance (répertoire)
  - Utiliser un système à clé publique (Diffie-Hellmann)
  - Crypto. quantique
  - Pigeon voyageur

RSA

- Clef publique
  - n : produit de deux (grands) nombres premiers p et q (p et q doivent rester secrets)
  - e : premier avec (p-1)(q-1)
- Clef privée
  - d : $e^{-1} \bmod((p-1)(q-1))$
- Chiffrement
  - $c = m^e \bmod n$
- Déchiffrement
  - $m = c^d \bmod n$

El Gamal (signature)

- Clef publique
  - p : premier
  - $g < p$
  - $y = g^x \bmod p$
- Clef privée
  - $x < p$
- Signature
  - k : choisi au hasard, premier avec p-1
  - (a,b) : $a = g^k \bmod p$ et $M = (xa + kb) \bmod (p\text{-}1)$
- Vérification
  - Valide si $y^a a^b \bmod p = g^M \bmod p$

El Gamal (chiffrement)

- Clef publique
  - p : premier
  - $g < p$
  - $y = g^x \bmod p$
- Clef privée
  - $x < p$
- Chiffrement
  - k : choisi au hasard, premier avec p-1
  - C=(a,b) : $a = g^k \bmod p$ et $b = y^k \mathrm{M} \bmod p$
- Déchiffrement
  - $\mathrm{M} = b / a^x \bmod p$

Avantages des chiffres à clef publique

- Pas de confiance mutuelle entre émetteur et récepteur
- Gestion de clé « facile »
  - Répertoire public de clés publiques ou distribution entre pairs
  - La clé privée ne doit « jamais » être transmise
- Permettent des utilisations nouvelles : distribution de clés symétriques, signatures, certificats, …

Échange de clefs symétriques

- Exemple : Alice génère aléatoirement une clé de session K (symétrique) et la chiffre avec la clé publique de Bob
- Exemple : Diffie-Hellmann

  Alice génère aléatoirement :

  n : grand nombre premier tel que (n-1)/2 soit aussi premier
  et choisit g = générateur d'un sous-groupe q de n
  (typiquement, g = 2, q = (n-1)/2)

  x (clé secrète d'Alice) est tel que $\log_g n < x < q$

  1. Alice calcule $K_a = g^x \bmod n$ et transmet (n, g, K_a) à Bob.
  2. Bob génère aléatoirement y (clé secrète de Bob),
     calcule $K_b = g^y \bmod n$, et transmet K_b à Alice.
  3. Alice et Bob peuvent alors calculer séparément une clé de session
     $K = K_b{}^x \bmod n = K_a{}^y \bmod n = g^{xy} \bmod n$

Inconvénients des chiffres à clef publique

- Calculs complexes
  - lents (~1 Mb/s)
  - clef longue (1024 ou 2048 bits), sauf avec des courbes elliptiques (~160 bits)

- Problèmes spécifiques
  - Intégrité des répertoires de clés publiques
  - Durée de vie des clés
  - Révocation
  - Nécessité de partager des clés privées ?
  - Limitation des algorithmes : ex. chiffrer un petit M par RSA

Fonctions de hachage → empreinte

- « One-way hash function » H
  - L'empreinte H(M) est de taille fixe n (ex: 128 bits) quelle que soit la longueur de M
  - La probabilité que 2 messages différents M et M' aient la même empreinte H(M)=H(M') est $\sim 1/2^n$
  - Connaissant M, il est facile de calculer H(M)
  - Connaissant M, il est impossible de trouver $M' \neq M$ tel que H(M') = H(M)
- Exemples: MD5, SHA-1, SHA-256, DES en mode CBC
- Typiquement, on découpe M en blocs m_1, m_2, ..., m_k
  $h_1=F(cte,m_1)$, $h_2 = F(h_1,m_2)$, ..., $h_k = F(h_{k-1},m_k) = H(M)$

Application : intégrité

- Communications : contre interception et modification transmettre le message et l'empreinte par des canaux indépendants
- Fichiers : détection de modifications
  - Exemples : Tripwire, Samhain
  - Sur une machine de confiance, calculer les empreintes des fichiers stables (OS, programmes, configuration, ...) et les stocker de manière protégée
  - Périodiquement ou en cas de doute, recalculer les empreintes et les comparer (sur une machine de confiance)

Signature (intégrité)

- Ks = clef de signature ; Kv = clef de vérification
- Signatures symétriques Ks = Kv
  - Exemple: dernier bloc DES-CBC
  - Signataire et vérificateur doivent se faire confiance
  - La signature n'est pas valable devant un juge
- Signatures asymétriques Ks ≠ Kv
  - Hachage puis chiffrement empreinte: Ks=Kc, Kv=Kd
  - Vérifiable par des tiers

    Il faut être sûr de ce que l'on signe !
  - Peuvent servir à sécuriser les répertoires de clefs publiques
    - Chaque entrée du répertoire est signée par une autorité (de certification).
    - Les clés des AC sont structurées dans un répertoire en arbre

L'époque contemporaine

- 2004
  - Il y a de sérieux doutes théoriques sur MD5 (classes de collisions)
  - Il y a des possibilités d'extrapolation sur SHA-1
- 2005
  - MD5 n'est plus considérée de confiance
  - Il y a des doutes théoriques sur SHA-1 (collisions en nombre)
- 2006
  - Des rumeurs entourent SHA-1 (« les calculs sont en cours »)
- 2007-11-02 NIST *hash function competition* (SHA-3)
- 2010-12-10 : 5 finalistes

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

Julius Caesar

http://www.cits.rub.de/**MD5Collisions**/

```
ortalo@hurricane:~/$ md5sum letter_of_rec.ps order.ps
a25f7f0b29ee0b3968c860738533a4b9  letter_of_rec.ps
a25f7f0b29ee0b3968c860738533a4b9  order.ps
ortalo@hurricane:~/$
```

Schémas à seuil

- Stocker K sous la forme d'un ensemble de valeurs Ki (images) telles que
  - S images permettent de reconstruire le secret (S est le seuil)
  - S-1 images n'apportent aucune information
- Si on sait générer N images (avec N>S), alors on tolère de perdre jusqu'à N-S images
- Exemple d'idée
  - Si l'on connait S=n+1 point d'un polynôme P de degré n, on sait recalculer les coefficients a_n du polynôme
    (n+1 équations à n+1 inconnues)
  - Passer dans un corps de Galois (modulo q avec q premier)

Autres sujets (non-abordés)

- Stéganographie
- *Watermarking* (tatouage)
- Générateurs aléatoires
- Génération de nombres premiers
- Écrous (key escrow)
- Vote
- Horodatage
- Destruction
- Protocoles

- Cryptanalyse
  - Premiers cours...

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - **Politiques de sécurité formelles**
  - Critères d'évaluation normalisés

Politiques et modèles de sécurité

- La politique de sécurité
  - « *est l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensibles et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique*. » [ITSEC, 1991]
  - physique, administrative, logique
- Modèle de sécurité
  - Formalisme ou représentation mathématique
- Partition entre entités
  - actives: sujets *s*
  - passives: objets *o*

Politiques discrétionnaires et obligatoires

- Politique discrétionnaire
  - chaque objet *o* est associé à un sujet *s* précis, son propriétaire qui manipule les droits d'accès à sa discrétion
  - le propriétaire peut librement définir et transmettre ces droits à lui-même ou un autre utilisateur
- Politique obligatoire
  - règles discrétionnaires (droit d'accès)
  - *plus* : règles incontournables (habilitation)

Matrice de contrôle d'accès

[Lampson 1971]

- Machine à états : état = (S,O,M)
  - O ensemble d'objets
  - S ensemble de sujets ($S \subseteq O$)
  - $M(s,o)$ est l'ensemble des droits que le sujet s possède sur l'objet o
  - les droits sont pris dans un ensemble fini A

Modèle HRU (1976)

- Commandes de modification

  command $\alpha(x_1, x_2, ...x_k)$

  if $a' \in M(s',o')$ and $a'' \in M(s'',o'')$ and ... and $a^{(m)} \in M(s^{(m)},o^{(m)})$

  then op_1; op_2; ...; op_n

  end

  $a^{(i)} \in A$

  op_i: *create a into M(s,o)* *delete a from M(s,o)*

  create subject s *destroy subject s*

  create object o *destroy object o*

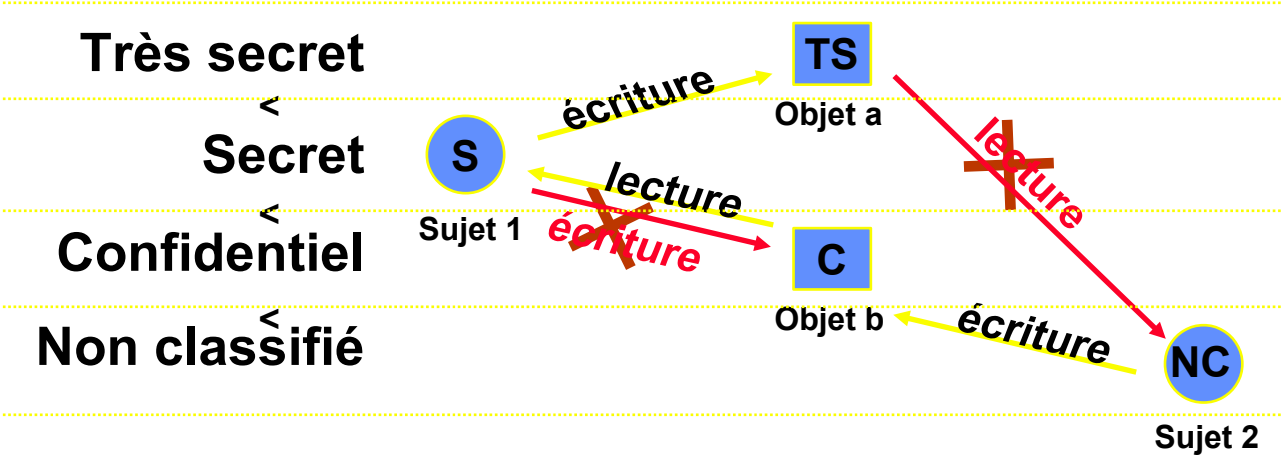
- Problème de protection (Q_0 sûr pour *a*)
  - *indécidable* dans le cas général
  - *décidable* pour les systèmes à mono-opération (n=1)

Autres modèles dérivés

- Take-Grant (1976)
  - algorithme de décision de complexité linéaire
- SPM et TAM (1988, 1992)
- rôles
  - RBAC (1996)

Politique multiniveau de Bell-LaPadula (1975)

- niveau (d'habilitation) des sujets *h(s)*
- niveau (de classification) des objets *c(o)*
- interdire les fuites d'information d'un objet vers un objet de niveau inférieur
- interdire à tout sujet d'obtenir des information d'un objet de niveau supérieur à son habilitation



Modèle de Bell-LaPadula

- classification *cl* : ensemble totalement ordonné
- compartiment *C* : ensemble de catégories
- $n=(cl,C)$, $n'=(cl',C')$: $n \preccurlyeq n' \Leftrightarrow cl \leq cl'$ et $C \subseteq C'$ (treillis)
- propriété simple

  $$\forall s \in S,\ \forall o \in O,\ \text{read} \in M(s,o) \Rightarrow c(o) \preccurlyeq h(s)$$
- propriété $\star$

  $$\forall s \in S,\ \forall (o,o') \in O^2,\ \text{read} \in M(s,o) \wedge \text{write} \in M(s,o') \Rightarrow c(o) \preccurlyeq c(o')$$

Inconvénients de BLP et Politique de Biba

- Inconvénients
  - L'information se dégrade constamment par surclassification (ou on introduit des procédures de déclassification hors modèle)
  - Le modèle ne représente pas tous les flux d'information et ne prend pas en compte les canaux cachés
- Politique de Biba
  - duale de BLP pour assurer l'intégrité
  - droits = { modifier, observer, invoquer }
  - inconvénient similaire : le niveau d'intégrité de l'information se dégrade constamment

Politiques de contrôle d'interface – Modèle

- ensemble S de sujets, ensemble Γ de commandes ou opérations, ensemble d'états Σ du système, σ_0 état initial
- un ensemble Out dont les éléments sont les sorties visibles par un utilisateur
- out : $\Sigma \times S \rightarrow \text{Out}$ do : $\Sigma \times S \times \Gamma \rightarrow \Sigma$
- **trace**, suite ordonnée de commandes
  $w \in traces = (S \times \Gamma)^*$
- $[w] \in \Sigma$ état atteint en partant de σ_0
- $\langle\ \rangle$, $\nu \cdot \gamma_1(u_1) \cdot \gamma_2(u_2) \cdot \ldots \cdot \gamma_n(u_n)$, $(\gamma_i)_{1 \le i \le n}$, $(u_i)_{1 \le i \le n}(u_i)$
- Γ_{out}, read(u), highin(u), lowout(u), lowin(u)

Non-interférence

[Goguen&Meseguer 1982]

- purge : S × traces → S

$$purge(u, \langle\rangle) = \langle\rangle$$

$$purge(u, hist \cdot command(u')) = \begin{cases} purge(u, hist) \cdot command(u') & si\ h(u) \geqslant h(u') \\ purge(u, hist) & si\ h(u) < h(u') \end{cases}$$

- propriété

$$\forall u \in S, \forall w \in traces, \forall c \in \Gamma_{out}$$

$$out(u, w \cdot c(u)) = out(u, purge(u, w) \cdot c(u))$$

- assez proche de l'intuition mais aussi très forte

Non-interférence & co.

- Proche de l'intuition (vs. BLP)
  - interdit les canaux cachés
  - autorise des opérations (sans interférence)
- Limitations
  - interdit l'utilisation de canaux cryptographiques (même parfaits)
  - applicable seulement aux systèmes déterministes
- ***Non-déductibilité*** [Sutherland 1986] puis ***Non-interférence généralisée*** [McCullough 1987] visent les systèmes non-déterministes
- La ***restriction*** [McCullough 1990] vise à préserver la propriété en cas de composition de deux systèmes

Politiques de contrôle de flux

[Bieber&Cuppens 1992, d'Ausbourg 1994]

- *(o,t)* : entrées, sorties ou points internes (et temps)
- dépendance causale : *(o',t')* $\rightarrow$ *(o,t)* avec *t'* < *t*
- cône de causalité: *cone(o,t)* = { *(o',t') / (o',t')* $\rightarrow^*$ *(o,t)* }
- cône de dépendance: *dep(o,t)* = { *(o',t') / (o,t)* $\rightarrow^*$ *(o',t')* }
  - si *s* connait une sortie x_o il peut inférer *cone*(x_o)
  - si *s* connait une entrée x_i il peut inférer *dep*(x_i)
- confidentialité
- intégrité

$$\bigcup_{x_o \in O_s} cone(x_o) = Obs_s \subseteq R_s$$

$$\bigcup_{x_i \in A_s} cone(x_i) = Alt_s \subseteq W_s$$

Politiques spécifiques

- Politique d'intégrité de Clark et Wilson
  - données contraintes (CDI) et non-contraintes (UDI)
  - validation des procédures de traitement (TP) + procédure(s) de vérification d'intégrité (IVP)
  - gestion des relation entre données et procédures
- Muraille de Chine (ou Brewer-Nash)
  - étude de classes de conflits d'intérêts
  - dans un contexte dynamiques
- ...
  - données médicales
  - recommandations
  - **rôles**

Politique de sécurité

- Objectifs de sécurité : exemples
  - confidentialité : le dossier médical ne peut être consulté que par le patient ou son médecin traitant
  - intégrité : un chèque de plus de 1000 doit être validé par un ordonnateur et un comptable
  - disponibilité : si la carte et le PIN sont valides, le distributeur de billet doit fournir l'argent dans les 30 secondes
- Règles de sécurité : exemples
  - un fichier ne peut être lu que par les utilisateurs autorisés par le propriétaire du fichier
  - un message de type « chèque de + de 1000€ » n'est valide que s'il est signé par P1 et T2 et que les signatures sont valides
  - l'insertion d'une carte lance automatiquement l'action

Cohérence d'une politique

- La politique est cohérente si, partant d'un état quelconque où les objectifs sont satisfaits, il n'est pas possible d'atteindre, en respectant les règles, un état où ils ne sont plus satisfaits
- Intérêts d'un modèle formel
  - Décrire de manière précise les objectifs et les règles
  - Prouver des propriétés sur la politique (cohérence, complétude, ...) et sur son implémentation par le système informatique

Logique déontique
(une logique modale)
P, **O**, **F**
($\Box$, $\Diamond$)

Politique, protection et contrôle d'accès

- Les règles doivent être mises en oeuvre par des mécanismes (matériels, logiciels)
- Facile à imaginer pour les règles du type « il est permis de... » ou « il est interdit de... » – mécanismes de protection – instructions privilégiées, contrôle d'accès à la mémoire, contrôle à l'ouverture des fichiers, etc.
  ➞ autorisation
- Difficile pour les règles du type « il est obligatoire de... » ou « il est recommandé de... »
  ➞ actions automatiques, gestion de ressources

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - **Critères d'évaluation normalisés**

Les « Critères »

- Historique
  - TCSEC – Trusted Computer System Evaluation Criteria – DoD 1985 (Livre orange) et TNI – Trusted Network Interpretation of the TCSEC (Livre rouge)
  - ITSEC – Information Technology Security Evaluation Criteria (EEC 1991)
  - JCSEC, CTCPEC
  - CC – Common Criteria (norme ISO depuis ~2000)

Le livre orange : niveaux

D	Protection minimale	
C1	Protection discrétionnai	sécurité discrétionnair
C2		audit
B1	Protection obligatoire	labels
B2		protection structurée
B3		domaines de sécurité
A	Protection vérifiée	vérification

Le livre orange : critères (1/2)

- Doctrine de sécurité
  - Contrôle d'accès discrétionnaire
  - Réutilisation d'objet
  - Labels
  - Contrôle d'accès obligatoire
- Responsabilité
  - Identification et authentification
  - Cheminement sûr
  - Audit
- Assurance opérationnelle
  - Architecture du système
  - Intégrité du système
  - Analyse des canaux cachés
  - Gestion d'une installation
  - Reprise sûre

Le livre orange : critères (2/2)

- Assurance du cycle de vie
  - Essai de la sécurité
  - Spécification et vérification
  - Gestion de la configuration
  - Distribution sûre
- Documentation
  - Guide l'utilisateur
  - Manuel d'installation sûre
  - Documentation des essais
  - Documentation sur le concept de sécurité

ITSEC - Critères

- Classe de fonctionnalité
- Assurance de conformité : E1 à E6
- Assurance d'efficacité
  - Construction
    - Pertinence de la fonctionnalité
    - Cohésion de la fonctionnalité
    - Résistance des mécanismes
    - Estimation de la vulnérabilité de construction
  - Exploitation
    - Facilité d'emploi
    - Estimation de la vulnérabilité en exploitation

Nice quote on criteria

- CC – ISO 15408
  - Common Criteria

« For the most part, the protection profiles define away nearly all of the interesting threats that most systems face today. » *in* Fedora and CAPP, lwn.net, 10 dec. 2008.