

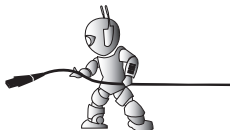
Chiffrement et authentification

Autres applications de la cryptographie.

Tuyêt Trâm DANG NGOC
<dntt@u-cergy.fr>

Université de Cergy-Pontoise

2012–2013



1 Wifi

- Chiffrement par flots
- WEP
- Wi-Fi Protected Access (WPA)

2 Carte à puce

- Exemple : la carte bancaire

3 Marquage d'étiquettes

4 Biométrie

5 Tatouage (watermarking - filigrane)

6 Crédits

1 Wifi

- Chiffrement par flots
- WEP
- Wi-Fi Protected Access (WPA)

2 Carte à puce

3 Marquage d'étiquettes

4 Biométrie

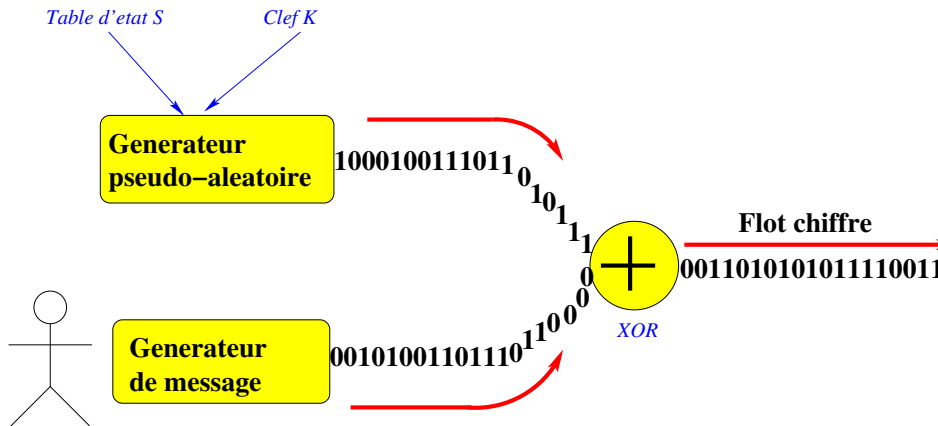
5 Tatouage (watermarking - filigrane)

6 Crédits

Algorithme de chiffrement par flot (*stream cipher*)

Contrairement au chiffrement par bloc (DES, AES, Blowfish, etc.), le chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper.

- **RC4** : le plus répandu, conçu par Ronald Rivest, utilisé notamment par WEP et SSL
- **A5** : utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche,
- **E0** : utilisé par le protocole Bluetooth
- **Py** : un algorithme récent de Eli Biham
- ...

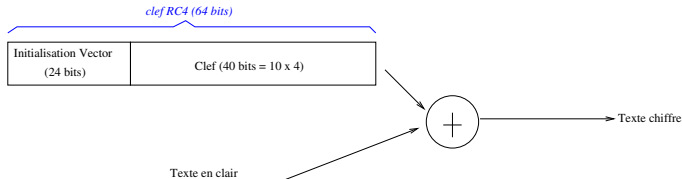


Clef	Message en clair	Message chiffré
"toto"	"Attaque"	B661C9F88FE847
"Clef secrete"	"Attaque"	DB18DA5AD95479
"Clef secrete"	"Attaque demain"	DB18DA5AD95479EE9F7B34CD80DC
"Clef secrete"	"Attaque demain a l'aube"	DB18DA5AD95479EE9F7B34CD80DC33DD56D31C3BB09CE9

Wired Equivalent Privacy (WEP)

Le WEP utilise

- **Confidentialité** : l'algorithme de chiffrement par flot RC4 (clef de 40, 154 ou 232 bits)
- **Intégrité** : la somme de contrôle CRC-32
- **Protocole de gestion des clefs** : aucun



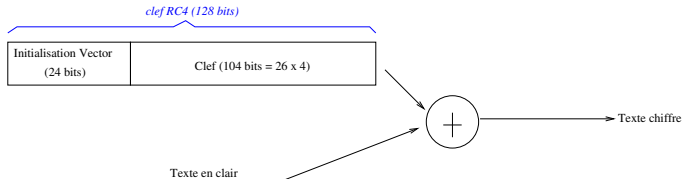
24 bits de la clé servent uniquement pour l'initialisation \Rightarrow seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

(40 bits : attaque par force brute possible)

Wired Equivalent Privacy (WEP)

Le WEP utilise

- **Confidentialité** : l'algorithme de chiffrement par flot RC4 (clef de 40, 154 ou 232 bits)
- **Intégrité** : la somme de contrôle CRC-32
- **Protocole de gestion des clefs** : aucun



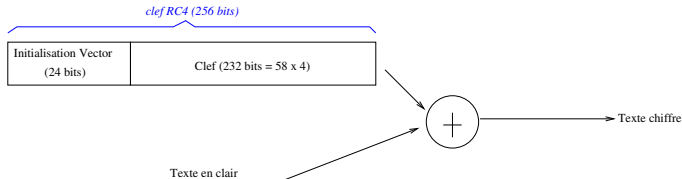
24 bits de la clé servent uniquement pour l'initialisation \Rightarrow seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

(40 bits : attaque par force brute possible)

Wired Equivalent Privacy (WEP)

Le WEP utilise

- **Confidentialité** : l'algorithme de chiffrement par flot RC4 (clef de 40, 154 ou 232 bits)
- **Intégrité** : la somme de contrôle CRC-32
- **Protocole de gestion des clefs** : aucun



24 bits de la clé servent uniquement pour l'initialisation \Rightarrow seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

(40 bits : attaque par force brute possible)

WEP

La clef RC4 est symétrique.

Dans WEP :

- **pas de protocole de gestion des clés** : une unique clé partagée entre tous les utilisateurs.

Authentification

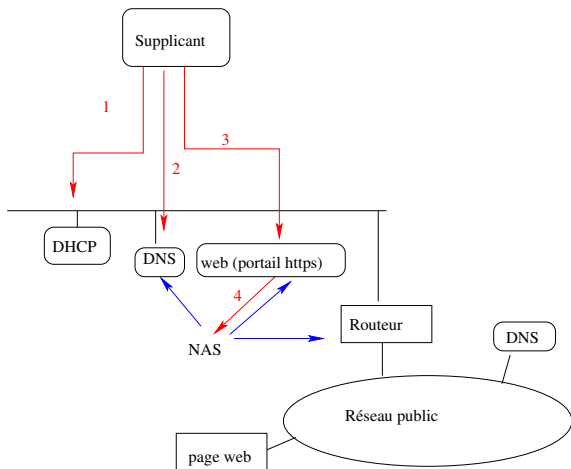
Deux méthodes :

- **Ouvert** : pas de clef demandée. Association faite par le serveur à une requête du client. Les messages peuvent ensuite éventuellement être chiffrés avec la clef WEP.
- **À clef partagé** :
 - 1 le client envoie une requête d'authentification au point d'accès (AP)
 - 2 le point d'accès envoie un texte en clair pour un challenge
 - 3 le client doit chiffrer le texte en clair en utilisant la clef WEP et la renvoyer à l'AP.
 - 4 le point d'accès déchiffre le texte et le compare au texte en clair envoyé et renvoie une réponse positive ou négative
 - 5 Après authentification et association, WEP peut être utilisé pour chiffrer les données.

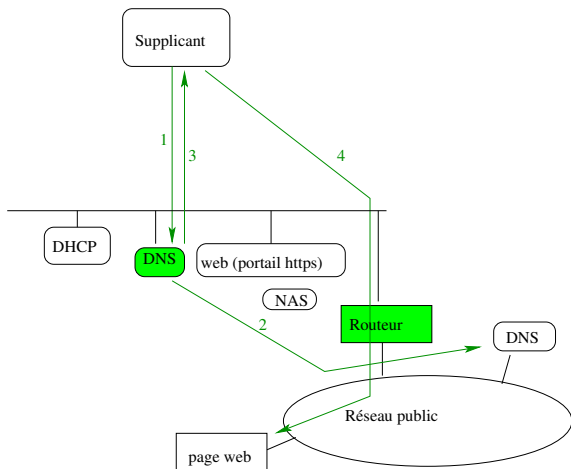
Failles de WEP

- il est possible d'altérer les données et de mettre à jour le CRC du message sans connaître la clé WEP.
- pas de compteur de trame \Rightarrow attaque par rejeu
- **En 2001** : analyse cryptologique [Fluhrer et al.] sur l'algorithme RC4 et l'IV dans WEP montre qu'une attaque passive permet de retrouver la clé RC4 après une écoute clandestine du réseau pendant quelques heures.
- **En 2005** : FBI montre qu'il est possible de pénétrer un réseau protégé par du WEP en 3 minutes en utilisant des outils disponibles publiquement.
- **Depuis juillet 2006** : il est possible de pénétrer les réseaux protégés par WEP en quelques secondes seulement, en tirant parti de la fragmentation des paquets pour accélérer le cassage de la clé.

Portail captif



Portail captif



Wi-Fi Protected Access (WPA)

WPA-1 (2004 - IEEE 802.11i) utilise

- **Confidentialité** : l'algorithme de chiffrement par flot RC4 avec une clef de 154 bits (128 bits + 48 bits IV)
- **Intégrité** : la somme de contrôle MIC (Message Integrity Code - "Michael" dérivé de MAC) plus sécurisé que CRC32 + compteur de trame pour empêcher les attaques par rejeu.
- **Protocole de gestion des clefs** : protocole Temporal Key Integrity Protocol (TKIP), qui échange de manière dynamique les clés lors de l'utilisation du système.

Wi-Fi Protected Access 2 (WPA2)

- **Confidentialité** : chiffrement basé sur AES plutôt que sur RC4.
- **Protocole de gestion des clefs** : protocole CCMP

802.1X (IEEE 2001)

permet d'authentifier un utilisateur souhaitant accéder à un réseau (filaire ou non) grâce à un serveur d'authentification.

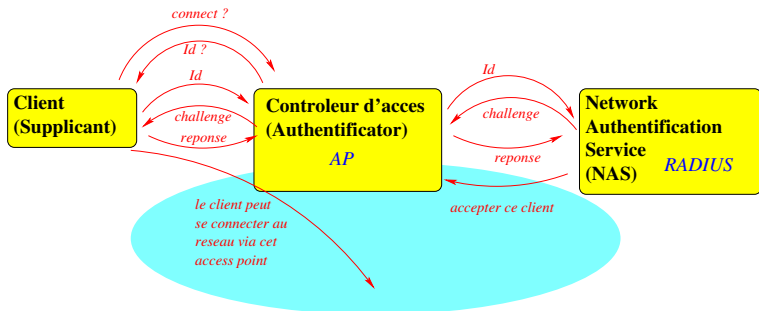
Le 802.1x repose sur le protocole EAP (Extensible Authentication Protocol) dont le rôle est de transporter les informations d'identification des utilisateurs.

Versions de WPA

- **WPA-Enterprise** : : en collaboration avec un serveur d'identification 802.1X chargé de distribuer les différentes clés à chaque utilisateur.
- **WPA-Personal** : : Mode moins sécurisé, appelé Pre-Shared Key (PSK), dans lequel tous les utilisateurs partagent une même phrase secrète.

Extensible Authentication Protocol (EAP)

est un mécanisme d'identification universel, fréquemment utilisé dans les réseaux sans fil et les liaisons Point-A-Point



EAP

- LEAP
- EAP-TLS
- EAP-MD5
- EAP-PSK
- EAP-TTLS
- EAP-IKEv2
- PEAP
 - PEAPv0/EAP-MSCHAPv2
 - PEAPv1/EAP-GTC
- EAP-FAST
- EAP-SIM
- EAP-AKA

Norme à 2 volets La nouvelle norme de sécurité IEEE 802.11i : VOILET 1 :
Solution de transition compatible avec le matériel existant (WPA) :

- WPA Perso
⇒ WPA Pre-Shared Key
 - WPA Entreprise
⇒ 802.1x + EAP
- Rotation de clés - TKIP
(Temporal Key Integrity Protocol) + algorithme de cryptage RC4

VOILET 2 : Solution définitive incompatible avec le matériel existant :

- WPA2 Perso
⇒ WPA Pre-Shared Key
 - WPA2 Entreprise
⇒ 802.1x + EAP
- Nouveau cryptage AES
(Advanced Encryption Standard) en remplacement de RC4

- 1 Wifi
- 2 Carte à puce
 - Exemple : la carte bancaire
- 3 Marquage d'étiquettes
- 4 Biométrie
- 5 Tatouage (watermarking - filigrane)
- 6 Crédits

Cartes à puce

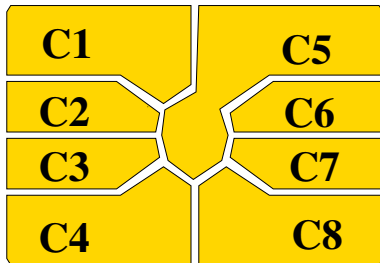
Utilisation intensive de toutes les techniques de sécurités.

- Carte sans micro-contrôleur :
- Carte avec micro-contrôleur :
- Carte avec contact : nécessite de mettre la puce dans un terminal
- Carte sans contact : utilisation à distance

Utilisation :

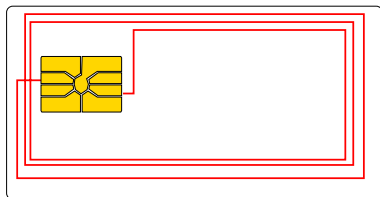
- Carte de paiement : carte bleue
- Porte-monnaie électronique : MONEO
- Pass Navigo
- badge d'identification
- carte de sécurité sociale
- carte SIM des téléphones portable
- identification sur les décodeurs télé
- dans les architectures PKI
- ...

Cartes à puce



Contact	Description
C1	Tension d'alimentation ($V_{cc} +5V$)
C2	Lecture/écriture
C3	Horloge
C4	Reset(0)/Up(1) du pointeur interne
C5	Masse
C6	Tension de programmation ($V_{pp} +21V$)
C7	Entrées/Sortie (données)
C8	Fusible

Carte à puce sans-contact



- pratique (pas besoin de mettre la carte dans le lecteur)
- puce moins exposée (est enchassée dans le corps plastique de la carte)
- Si l'antenne est dans la carte : plus fragile (ne pas plier)
- interception possible des signaux transmis entre la carte et la borne
- dialogue avec la carte à l'insu du porteur... (tous surveillés!)

Sécurité physique

Intrusion invasive (pose de sonde, analyse des circuits, de la ROM, rayon X).

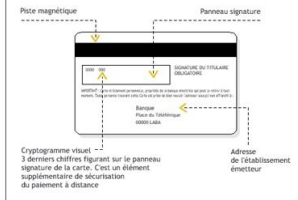
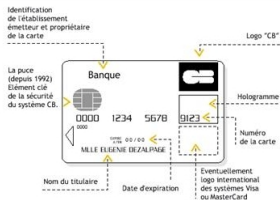
- Mémoire ROM située au plus près du substrat de silicium : il faut en effet retirer finement toutes les couches de métal au dessus, sans pour autant détruire celle de la ROM
- Circuits surmontés d'une couche de métal formant un bouclier qui empêche d'intervenir sur le circuit sans le détruire.
- Mémoires non volatiles chiffrées
- Bus entre le processeur et les mémoires chiffrés et multiplexés
- En dehors des blocs mémoire, toute la conception du circuit est brouillée

Intrusion non invasive (connecteurs, rayonnement électromagnétique) observation et induction de fautes

- perturbation des signaux : horloges désynchronisées, données masquées avec des nombres aléatoires,
- contrôle d'intégrité.

Information contenue dans la carte bancaire

- physique : hologramme, embossage
- au dos : signature du porteur (+ récemment cryptogramme) :
- face : BIN (Bank Identification Number) + Informations sur le porteur (le numéro à 16 chiffres, date d'expiration, nom et prénom du porteur).
- puce : BIN + Informations sur le porteur + valeur de signature
- piste : BIN + Informations sur le porteur + code pays origine + code confidentiel chiffré.



Type d'autorisation

- numéro : correspondance, site en ligne
- numéro embossé + signature : se fait beaucoup à l'étranger
- authentification par code secret : DAB, TPE
- autorisation systématique : DAB, TPE suivant montant

Les 16 chiffres de la CB

16 chiffres sous la forme ABCD EFGH IJKL MNOP

- A : type de carte (Américan Express, Visa (4), MasterCard (5), Discover (6))
- BCD, BCDE, BCDEF : numéro de la banque (BNP, LCL, CA, SG, etc.). La longueur varie selon l'organisme bancaire.
- les numéros qui suivent le numéro de banque jusqu'au O compris, sont les numéros composant le numéro de carte.
- le dernier chiffre (P) correspond à la clef de Luhn qui permet de vérifier la validité du numéro de carte

Clef de Luhn

La clef de Luhn permet de vérifier la validité du numéro de carte.

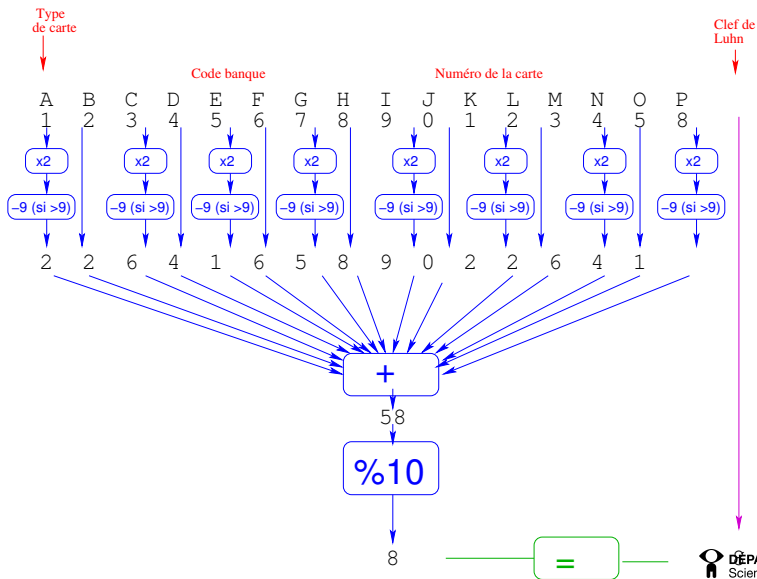
- Pour A, C, E, G, I, K, M, O (un chiffre sur 2), multiplier le chiffre par 2. Si le résultat est plus grand que 9, soustraire 9.
- Soit
$$S = A + B + C + D + E + F + G + H + I + J + K + L + M + N + O$$
et ne garder que le chiffre des unités.
- $P = 10 - S$

Algorithme de vérification trivial.

Le secret par l'obscurantisme n'a duré que (très) peu de temps.

N'importe qui peut générer un chiffre valide.

Clef de Luhn



Problèmes du numéro de CB

Les 16 chiffres de la C.B. suffisent pour commander sur Internet ou par correspondance.

- coup d'oeil indiscret d'un passant, d'un autre client
- employé indélicat qui recopie les factures côté commerçant.
- facturette : avant 2001, les terminaux inscrivaient sur les facturettes les numéros de CB.
- générateur de numéro valide.

- ⇒ Utilisation d'un numéro valide n'appartenant à personne (au détriment du commerçant et/ou de la banque)
- ⇒ Utilisation d'un numéro valide appartenant à quelqu'un (au détriment du porteur réel et/ou de la banque)

Cryptogramme visuel (CCv et CCv2)

Cryptogramme visuel

résultat d'un chiffrement du numéro de carte et d'autres éléments à l'aide d'une clé secrète stockée dans le HSM (Hardware Security Module) de la banque émettrice de la carte.

L'algorithme est secret et aucun site marchand ni aucune autre banque que la banque émettrice n'est en mesure de vérifier le cryptogramme visuel.

Depuis 200X, demande systématique du cryptogramme.

⇒ échec des générateurs de code de CB et de la plupart des espionnages de numéro de code de CB.



e-carte bleue

Elle permet de générer un numéro de carte (+ cryptogramme visuel) qui ne sert que pour une seule transaction (et dont le montant est fixé par l'utilisateur et débité de son compte) plus besoin de laisser ses coordonnées bancaires lors d'un achat sur le web

Plus de problème au niveau de l'écoute de la transaction ou du commerçant indélicat :

- le numéro est unique et ne peut être utilisé qu'une seule fois
- le numéro ne peut être utilisé que pour le montant indiqué par l'utilisateur.

Mais : service payant : les banques facturent au consommateur un risque qu'elles sont normalement censées assumer (la banque est légalement responsable de toutes les fraudes qui peuvent survenir lors d'un paiement qui ne requiert ni code secret ni signature)

Ne résoud pas le problème d'un numéro généré correspondant à votre numéro réel de CB. .

Article L132-4 (inséré par Loi n° 2001-1062 du 15 novembre 2001 art. 36 Journal Officiel du 16 novembre 2001)

La responsabilité du titulaire d'une carte mentionnée à l'article L. 132-1 n'est pas engagée si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de sa carte.

De même, sa responsabilité n'est pas engagée en cas de contrefaçon de sa carte au sens de l'article L. 163-4 et si, au moment de l'opération contestée, il était en possession physique de sa carte.

Dans les cas prévus aux deux alinéas précédents, si le titulaire de la carte conteste par écrit avoir effectué un paiement ou un retrait, les sommes contestées lui sont recreditées sur son compte par l'émetteur de la carte ou restituées, sans frais, au plus tard dans le délai d'un mois à compter de la réception de la contestation."

L'article L. 132-6 fixe le délai de contestation à 70 jours à compter de la date de l'opération.

Le remboursement se fait en général dans les 15 jours qui suivent la réception de la LRAR sans aucune question ou démarche.

Valeur de signature

Le GIE (Groupement des cartes bancaires) utilise RSA. Soient les clefs *Pub* publique et *Priv* secrète du GIE.

- Infos = Information sur le porteur : nom, numéro de carte, date de validité, etc.
- Fonction de hachage f compulsant les informations : $Y = f(\text{infos})$
- Y est chiffré avec la clé secrète *Priv* du groupement des cartes bancaires.
- La valeur *VS* (Valeur de Signature) résultante est stockée une fois pour toute lors de la fabrication de la CB. $VS = \text{Priv}(Y)$

Authentification de la carte (hors-ligne)

La carte est introduite dans le terminal. Validité de la carte

- Le terminal connaît la clef publique Pub du GIE.
- Le terminal lit les informations portées par la carte
- Le terminal calcule $Y1 = f(info)$
- Le terminal lit la valeur de signature VS portée par la carte
- Le terminal calcule $Y2 = Pub(VS) = Pub(Priv(Y))$
- Le terminal compare $Y1$ et $Y2$: Si $Y1 = Y2$ alors la carte est valide.

$Priv$ doit rester secret (fabrication et l'écriture des VS sur la puce se fait dans des locaux très sécurisés)

L'affaire Humpich (1998)

Depuis 1990 et jusqu'en 1998, le GIE utilise RSA avec $n = p \times q$ de taille 320 bits.

En 1998, Serge Humpich arrive à factoriser n (et donc à trouver p et q et donc $Priv = Pub^{-1} \text{mod}((p-1)(q-1))$).

La carte est donc considérée comme valide.

Depuis : n est sur 768 bits (pour l'instant incassable).

Identification de l'utilisateur par code confidentiel

Le code confidentiel (code PIN) est stocké (sous forme chiffrée) à la fois dans la puce et sur la piste magnétique de la carte.

- le terminal demande le code confidentiel à l'utilisateur
- l'utilisateur tape son code
- le terminal transmet le code à la carte
- si le code est valide, la carte le signale au terminal.

Attaque par Yes-Card

- le pirate introduit une Yes-Card dans le terminal
- après validation (voir Humpich)
- le terminal demande le code confidentiel à l'utilisateur
- le pirate tape un code quelconque
- le terminal transmet le code à la carte
- sans en tenir compte, la carte signale au terminal que le code est correct (Yes!)

Leçon à en tirer

Il est nécessaire d'utiliser un algorithme incassable, mais cela ne suffit pas, il faut que le protocole et le contexte soit également bien pensé.

- validation de la carte (incassable maintenant)
- demande de code (utilisation de la YES-card), mais si carte pas validée cette étape n'a pas lieu d'être.

Or ici, deux phases indépendantes. Donc :

- le pirate met une vraie carte bancaire valide dans le lecteur (validation OK)
- le pirate retire la carte et insère la YES-card (habilement car il ne faut pas que le contact se perde).

Phase de vérification distante

Demande d'autorisation (systématique, suivant le montant de l'achat, ou aléatoirement).

Authentification en ligne (DES et T-DES depuis 1999) :

- Le terminal interroge un centre de contrôle à distance (CCD)
- le CCD envoie à la carte une valeur aléatoire x
- La carte calcule $y = f(x, K)$, où K est une clé secrète, inscrite dans la partie illisible de la carte, et f est la fonction de chiffrement du T-DES.
- La carte transmet y au CCD, qui lui-même calcule $y_2 = f(x, K)$
- Si $y_2 = y_1$, le CCD donne l'autorisation.

Remarquons que ceci nécessite que le centre connaisse la clé secrète de toutes les cartes.

- 1 Wifi
- 2 Carte à puce
- 3 Marquage d'étiquettes**
- 4 Biométrie
- 5 Tatouage (watermarking - filigrane)
- 6 Crédits

Etiquetage

- Code à une dimension
 - Code Poste
 - Code-barre
- Code à deux dimensions
 - QRCode
 - Maxicode
- Code RFID



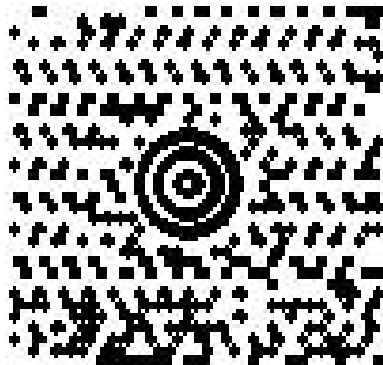
Etiquetage

- Code à une dimension
 - Code Poste
 - Code-barre
- Code à deux dimensions
 - QRCode
 - Maxicode
- Code RFID



Etiquetage

- Code à une dimension
 - Code Poste
 - Code-barre
- Code à deux dimensions
 - QRCode
 - Maxicode
- Code RFID



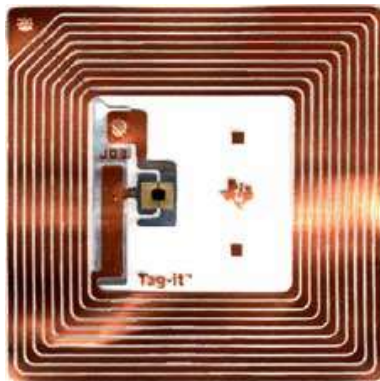
Etiquetage

- Code à une dimension
 - Code Poste
 - Code-barre
- Code à deux dimensions
 - QRCode
 - Maxicode
- Code RFID



Etiquetage

- Code à une dimension
 - Code Poste
 - Code-barre
- Code à deux dimensions
 - QRCode
 - Maxicode
- Code RFID



Principe RFID (Radio Frequency ID)

- Un tag (ou marqueur ou radio-étiquette ou transpondeur) est constitué d'une puce et d'une antenne (et parfois d'une batterie).
- Les dispositifs actifs émettent des radiofréquences qui vont activer les marqueurs qui passent devant eux en leur fournissant à courte distance l'énergie dont ceux-ci ont besoin.
- Suivant la fréquence :
 - fréquence basse : meilleure pénétration dans la matière (eau, corps humain), distance de quelques mètres
 - fréquence haute : meilleur débit, distance jusqu'à 200m



Classes 1-2

Classe 1 (passif)

- mémoire accessible en lecture seulement
- identifiant unique (de 128 bits)
- protocole simple : lorsqu'interrogé, renvoie son identifiant

⇒ pas cher (5ct), bonne durée de vie, non sécurisée. Utilisé pour la traçabilité.

Classe 2 (passif)

- algorithme cryptographique symétrique
- quelques centaines de bits réinscriptibles

⇒ pas trop cher(50ct), bonne durée de vie, peu sécurisée, clef symétrique (et donc partagée).

Classes 3-4

Classe 3 (semi-passif)

- source d'énergie pour les calculs, communication avec énergie du lecteur
- traçabilité par le produit (enregistrement des données à intervalles réguliers)
- chiffrement clef publique/clef privée

⇒ un peu plus cher (1EUR), sécurisée

Classe 4 (actif)

- batterie pour les calculs et la communication
- grande distance, initiation de la communication
- tags communiquent entre eux

⇒ cher (quelques euros), pile de 3 à 10 ans.

Contrôle d'accès par identification

- Le lecteur demande l'ID du RFID.
- L'ID est envoyé, le lecteur consulte sa base pour vérifier que cet ID a le droit

Contrôle d'accès par question/réponse (challenge)

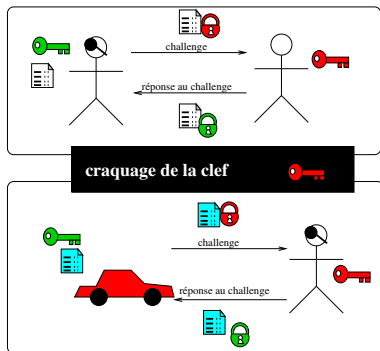
- Le lecteur envoie une valeur aléatoire C au tag
- le tag chiffre cette valeur C avec une clef secrète connu par le lecteur et le tag

Cas d'attaque (1) par cassage de clef

Le contrôle du démarrage de certaines voitures utilisent un challenge RFID (inséré dans la clef de la voiture).

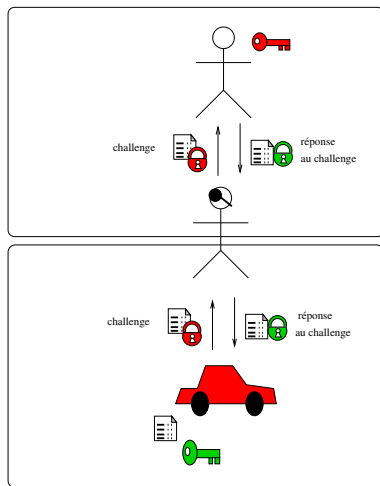
Clef symétrique secrète de 40 bits (seulement !).


- le pirate s'assoit à côté de sa victime
- le pirate interroge le tag de la victime avec un challenge de son choix
- il reçoit le challenge chiffré avec la clef secrète.
- le pirate essaye toutes les combinaisons pour la clef (2^{40}) : pour chacune de ces clefs essayé, il essaye de retrouver le même résultat au challenge.
- une fois la clef secrète trouvée, il n'a plus qu'à forcer (mécaniquement) la serrure...



Cas d'attaque (2) par relai (Technique de l'homme du milieu)

- le pirate se met entre le lecteur et la victime
- le lecteur envoie un challenge au pirate
- le pirate transmet le challenge à la victime
- le tag de la victime répond au challenge
- le pirate transmet cette réponse au lecteur.

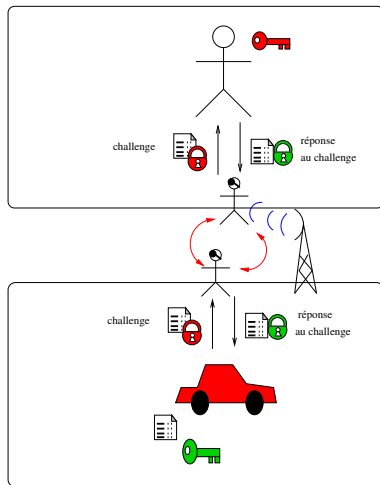


Pb de distance résolue à l'aide d'un complice par téléphone. ⇒  DÉPARTEMENT
Sciences Informatiques

difficile par mesure du temps de réponse.

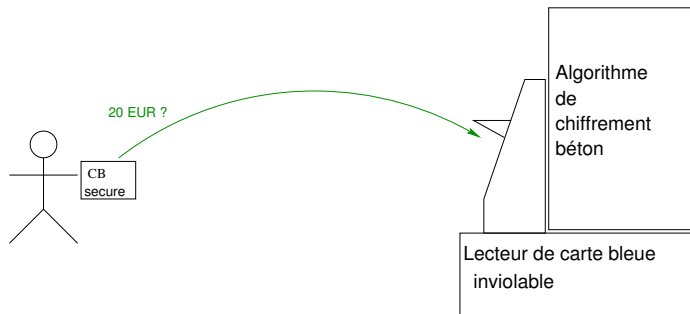
Cas d'attaque (2) par relai (Technique de l'homme du milieu)

- le pirate se met entre le lecteur et la victime
- le lecteur envoie un challenge au pirate
- le pirate transmet le challenge à la victime
- le tag de la victime répond au challenge
- le pirate transmet cette réponse au lecteur.

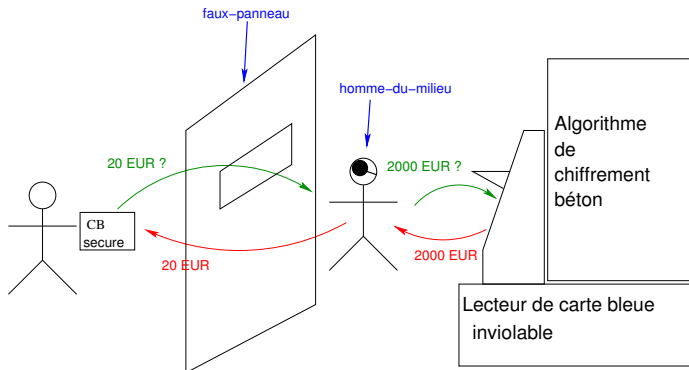


Pb de distance résolue à l'aide d'un complice par téléphone. ⇒ **Parade** DÉPARTEMENT Sciences Informatiques

Un algorithme incassable ne suffit pas, la sécurité doit être pensée dans son ensemble.



Un algorithme incassable ne suffit pas, la sécurité doit être pensée dans son ensemble.



- 1 Wifi
- 2 Carte à puce
- 3 Marquage d'étiquettes
- 4 Biométrie**
- 5 Tatouage (watermarking - filigrane)
- 6 Crédits

Méthode d'authentification

Améliorer le confort de l'utilisateur sans compromettre la sécurité (souvent contraignante (mot de passe, login)).

Authentifier une personne physique :

- quelque chose qu'on connaît : mot de passe, code PIN
- quelque chose qu'on possède : carte à puce, clef physique
- quelque chose que l'on est : empreinte digitale, iris, carte de vaisseau sanguin, ADN, visage, voix

On parle d'authentification forte lorsqu'on utilise au moins deux méthodes d'identification.

Exemple :

- carte à puce + PIN.
- mot de passe + reconnaissance vocale
- clef physique + reconnaissance du visage

⇒ choix compromis entre niveau de sécurité, prix et facilité d'utilisation

Quelque chose que l'on est : la biométrie

- voix
- lecture de l'iris
- reconnaissance faciale
- empreinte digitale
- reconnaissance de la configuration des vaisseaux sanguins (d'une partie de la main ou du doigt)
- ADN

⇒ mis en péril la confidentialité des données personnelles

⇒ si contrefait (faux-doigt, photo de visage, enregistrement sonore, etc.)

difficulté voire impossibilité de changer...

Chiffrement biométrique (biocryptographie)

transforme tout trait biométrique (empreinte digitale, iris, visage, voix...) au moyen d'une fonction cryptographique à sens unique qui crée une clé ou paire de clés de chiffrement biométrique.

Avantages :

- rétro-ingénierie irréalisable
- possibilité d'avoir plusieurs pseudo-identifiants par individu et de les gérer tel un certificat d'infrastructure de clé publique (PKI)
- précision de comparaison similaire à celle de la biométrie classique
- technologie économique
- combinaison de différents modes de reconnaissances biométriques (empreintes digitales, iris, voix, visage...) possible.
- chaque pseudo-identifiant est indépendant de tous les autres et le chiffrement biométrique résout les problèmes de respect de la vie privée liés à la biométrie classique.

⇒ technologie récente (2008 !)

- 1 Wifi
- 2 Carte à puce
- 3 Marquage d'étiquettes
- 4 Biométrie
- 5 Tatouage (watermarking - filigrane)**
- 6 Crédits

Tatouage (watermarking - filigrane)

Application de la stéganographie : tatouage électronique.

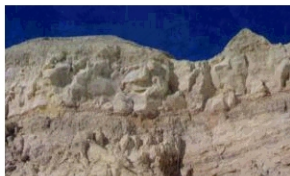
- cacher des données dans un document : correspondance secrète.
- marquer de façon indélébile un document : protection de droits d'auteurs

Contraintes d'un algorithme de tatouage (ex. fichier image) :

- respecter la qualité de l'image
- être robuste : résister aux transformations (compression, filtre, découpage, impression/numérisation)
- résister aux attaques : impossibilité de supprimer le tatouage
- garantir avec une bonne probabilité que le document est tatoué ou non et si oui, à qui appartient le tatouage.

Exemple de tatouage

Pour chaque pixel de la première image, et pour chaque couleur R,G,B de cette image, on remplace les 4 bits de poids faible par les 4 bits de poids fort correspondants dans la seconde image :



Images obtenues de l'application

<http://www.bibmath.net/crypto/stegano/cacheimage.php3>

- 1 Wifi
- 2 Carte à puce
- 3 Marquage d'étiquettes
- 4 Biométrie
- 5 Tatouage (watermarking - filigrane)
- 6 **Crédits**

- <http://www.bibmath.net/crypto/moderne/cb.php3>
- <http://ditwww.epfl.ch/SIC/SA/SPIP/Publications/spip.php?ar>
- RFID et la sécurité par Gildas Avoine
- Supports de cours de Jean-Louis Lanet