Masque jetable

- Principe du tel. Rouge entre URSS et USA
- Soit M un message binaire=b1b2b3...bl (avec l le nombre de bits du message)
- Soit K=k1k2k3...kl une suite de bits impossibles à prédire (on utilise une suite tirée aléatoirement)
- Pour obtenir le message chiffré, on fait un où exclusif entre chaque bit du message et celui de la clef
  - $c_i = b_i$ XOR k_i

Masque jetable

- Table du XOR: 0 XOR 0=0, 1 XOR 0 = 0 XOR 1 = 1 et 1 XOR 1 = 0
- Avantages du masque jetable:
  - Simple à mettre en oeuvre, rapide
  - Sûr si la clef est imprévisible
- Défauts :
  - Transport de la clef: les deux extrémités doivent l'avoir mais pas l'espion. Le transfert sûr de la clef est aussi difficile que celui du message.
  - La génération de la clef qui ne peut être réutilisée d'un message à un autre

Masque jetable

- Connaissant le message et sa version chiffrée, on peut en déduire facilement la clef K
- C= M XOR K
- K = M XOR C
- Conséquence: il faut une nouvelle clef pour chaque message
- Méthode du masque jetable ou « One Time Pad »

Principes de Kerckhoffs

- Auguste Kerckhoffs (Hollande, 1883)
  - Seule une donnée de petite taille (clef) doit suffire à assurer la sécurité
  - La sécurité d'un mécanisme ne doit pas reposer sur son caractère secret
- Il est beaucoup plus facile de garder secret un clef connue d'une personne qu'un procédé mis au point par plusieurs personnes.

L'ère scientifique:

- 1976: Diffie et Hellman découvrent la crypographie à clef publique en mettant au point un algorithme d'échange de clefs ne supposant aucun échange de secret préalable
- 1977: DES (standard américain de chiffrement symétrique)
- 1978: Rivest, Shamir et Alderman (re)découvrent RSA (système dechiffrement à clef publique)

algorithme de chiffrement symétrique (à clefs privées)

- Chiffrement symétrique:
  - la même clef sert au chiffrement et au déchiffrement
  - C'est le principe du coffre fort:
    - Akira et Barack connaissent tous deux la combinaison du coffre fort :
      - Akira dépose un message dans le coffre fort en utilisant la combinaison : elle chiffre le message avec la clef partagée
      - Barack récupère le message en ouvrant le coffre avec la même combinaison: il déchiffre le message avec la clef partagée
      - Si une autre personne réussit à avoir la combinaison, il peut lui aussi ouvrir le coffre et lire ou déposer des messages: elle peut chiffrer de nouveaux messages ou déchiffrer les messages transmis

Chiffrement symétrique

- les algo classiques sont rapides
- Pb:
  - comme faire en sorte que Bob et Alice connaissent la clef ?
  - Problème loin d'être négligeable qui se coûtait des sommes importantes aux services secrets du monde entier pour diffuser et renouveler les clefs secrètes envoyées à leur agents :
    - Renouveler suffisamment souvent les clefs
    - Avoir une clefs spécifique pour chaque contexte/agent pour éviter les conséquences de la récupération d'une clef par l'ennemi

algorithme de chiffrement

- chiffrement asymétrique:
  - Chaque participant x
    - a une clef publique Px qu'il peut diffuser à tous
    - A une clef secrète Qx qu'il doit être seul à connaître
  - Le chiffrement se fait avec la clef publique
  - Le déchiffrement se fait avec la clef privée
  - Principe de la boîte aux lettres :
    - Alice peut déposer des messages dans la boîte aux lettres: elle chiffre un message avec la clef publique
    - Bob est le seul à avoir la clef de la boîte aux lettre et donc le seul à pouvoir lire les messages qui y ont été déposés: il est seul à pouvoir déchiffrer des messages avec la clef privée.
  - Exemple: si Alice veut envoyer un message à Bob
    - Elle chiffre le message avec la clef publique de Bob
    - Bob reçoit le message chiffré et le déchiffre avec sa clef privée
  - les algo classiques sont lents

algorithmes classiques

- symétriques:
  - DES (1976): standard américain (1977), clef de 56 bits sur des blocs de 64 bits. dépassé de nos jours.
  - triple DES (1978): variante, triple application de DES, clefs entre 128 et 192 bits sur des blocs de 64 bits.
  - RC2, RC4, RC5 (1994) et RC6:
  - IDEA (1992): clef 128 bits sur des blocs de 64 bits
  - blowfish: clef 32 à 448 bits sur des blocs de 64 bits. Algo très analysé,considéré comme solide. utilisation libre.
  - AES (1998): clefs 128, 192 ou 256 bits sur blocs de 128 bits. standard américain. utilisation libre.

algorithmes classiques

- asymétriques:
  - RSA s'appuyant sur la factorisation de nombres premiers
  - Diffie-Hellman et El Gamal s'appuyant sur le calcul des logarithmiques discrets
  - des algorithmes nouveaux s'appuyant sur les courbes elliptiques

Système hybrides

- On génère une clef de session Ks
- On utilise un chiffrement à clef publique pour la transmettre à son correspondant
- On chiffre le reste de la communication avec un algorithme symétrique (donc rapide) utilisant la clef Ks

L'espion

- L'espion est un personnage classique de la cryptographie. Le but initial de la cryptographie était de protéger des communications de ses actions :
  - Il peut vouloir écouter et déchiffrer un message
  - Il peut vouloir déchiffrer tous les messages échangés entre Ahmed et Bernard
  - Il peut vouloir modifier les messages entre Arthur et Bérénice (on parle alors d'écoute active)

L'espion (2)

- Il peut se faire passer pour Anas auprès de Bérénice: on parle d'usurpation d'identité
- Il peut se faire passer pour Alex auprès de Bertrand et pour Bertrand auprès d'Alex : attaque « Man In the Middle »
- Bertrand peut refuser de reconnaître être l'auteur d'un message (reconnaissance de dette, ...) qu'il a pourtant envoyé à Aïcha.

Services s'appuyant sur de la cryptographie

- Confidentialité
- Intégrité
- Authentification:
- Non répudiation

Confidentialité

- protection des données contre une divulgation non autorisée
- 2 moyens techniques complémentaires
  - protéger l'accès aux données (implique authentification et contrôle d'accès). Ex.: authentification windows + ACL NTFS
  - les chiffrer
- intégrité, confidentialité : des contraintes opposées
  - intégrité : multiplier les sauvegardes notamment hors site
  - confidentialité: limiter les lieux de stockage pour faciliter le contrôle d'accès

Intégrité

- certifier que les données n'ont pas été altérées de façon intentionnelle ou accidentelle
- la modification peut avoir lieu
  - lors du transfert des données (corruption, écoute active)
  - lors du stockage des données
  - lors de leur traitement (bogues des logiciels applicatifs, des OS).
- Implications:
  - légales, plantage des applications et perte d'activité
  - perte d'image

Identification et authentification

- **identification**: définir l'identité de l'utilisateur
- **authentification**: permet de vérifier l'identité fournie (authentification simple vs authentification forte)
  - via un élément que l'utilisateur connait (mot de passe, ...)
  - via un élément que l'utilisateur possède (carte à puce, certificat, ...)
  - via biometrie
- Authentification forte : l'authentification utilise 2 méthodes de nature différente
    - Exemple : la carte bancaire (une carte que l'on a et un code que l'on connait)

authentification

- élément clef pour assurer :
  - la confidentialité et l'intégrité des données via un contrôle d'accès: seules les personnes identifiées, authentifiées et habilités à le faire peuvent accèder/modifier les données
  - la non-répudiation et l'imputabilité (preuve d'une transaction, ...)
- Authentification unique (SSO: Single Sign On)
  - l'utilisateur s'authentifie une fois
  - il a accès à toutes les ressources du réseau
  - cf partie technique (keberos, ...)

non répudiation

- **non répudiation** : ne pouvoir nier qu'un événement a eu lieu
- **imputabilité**: on sait qui a réalisé une action
- **traçabilité**: mémoriser des événements imputables
- **auditabilité**: pouvoir réaliser une analyse ultérieure d'un événement. Ex.: en cas d'intrusion.
- moyens: utilisation de journaux
  - de taille limitée
  - éventuellement hors site (intrusion)

Signature électronique

- Définition: la *signature électronique* a pour objectif de permettre à une personne d'attacher son identité à un message.
- Problèmes:
  - Le message doit être protégé contre les modifications sinon que certifie-t-on en le signant ?
  - La signature ne doit pas pouvoir être utilisée pour signer un autre message

Signature électronique: exemple à ne pas suivre

- Supposons que signer se résume à ajouter son nom à la fin d'un fichier
  - Tout le monde peut imiter une telle signature (pb de non répudiation)
  - Le document signé peut-être modifié (ajoutons un zéro sur la somme citée dans un chèque et changeons le bénéficiaire)
  - Ajouter de l'information à la fin d'un fichier peut le corrompre

Signature:

- Elle se décompose en deux parties:
  - Un procédé de signature: permet d'obtenir les données signées.
    - Ne doit pouvoir être appliqué que par le signataire.
    - Utilise en général un secret détenu par le signataire
  - Un procédé de vérification: à partir d'un texte signé et de l'identité du signataire, le procédé de vérification doit confirmer que le texte signé a bien été signé par le signataire désigné
    - doit pouvoir se faire sans secret détenu par le signataire.
- Signature et confidentialité sont deux services distincts qui sont parfois intégrés dans un même système.

Chiffrement symétriques

- clef de chiffrement = clef de déchiffrement
- Chiffrements par bloc:
  - DES (1977), blocs de 64 bits, clefs de 56 bits
  - IDEA (Lai Massey 1991), blocs de 64 bits, clefs de 128 bits
  - Rinjdael (Rinmen, Daemen, 1997): blocs de 128 ou 256 bits, clefs de 128, 192 ou 256 bits
  - AES, blocs de 128 bits, clefs de 128, 256 bits
- Chiffrement en continu d'un flux
  - RC4: chiffrement octets par octets
  - Pseudo-Vernam: XOR entre le flux et la sortie d'un générateur aléatoire

Principes de conception

- Problème :
  - On connaît de nombreux systèmes faibles (cesar, substitution, vigenere, ...)
  - comment construire des systèmes sûrs et plus efficaces que le masque jetable

Principes de conception

- Claude Shannon, 1949, « Communication Theory of Secrecy Systems »
  - Confusion: la relation entre le texte clair et le message chiffré doit être impossible à établir. Ca doit notamment être le cas pour les propriétés statistiques de l'un et de l'autre
  - Diffusion: un bit de clef ou de texte clair doit influencer de nombreux bits du texte chiffré.