Les concepts fondamentaux de la cryptographie

Nadia El Mrabet

GREYC−LMNO−Université de Caen, France

Ecole « Code et Cryptographie », ENSIAS de Rabat−MAROC,
Semaine du 8 au 14 mars 2010.

Plan de la présentation

Outline

Terminologie

Vocabulaire

On se placera dans la problématique d'un émetteur et d'un récepteur désirant s'envoyer un message sur un canal de transmission public (donc ouvert à la possibilité qu'une tierce personne intercepte le message).
Le but est de décrire et d'analyser des procédés (cela inclus leurs implémentations concrètes) permettant de transformer le message original, que l'on désignera par message clair (ou texte clair), en un message équivalent dont le contenu initial sera dissimulé (par la transformation).
Ce procédé sera appelé chiffrement (ou cryptage).

Terminologie

Vocabulaire

Une fois que le message est chiffré, il transite via un canal non sécurisé vers son destinataire.
Afin de déchiffrer le message, le destinataire doit lui faire subir l'opération inverse du chiffrement qui est le déchiffrement.
Cela permet d'assurer la confidentialité du message. On parlera alors de message chiffré.
En pratique, nous ne considérerons que des messages de type texte. Les méthodes que nous décrirons devront éventuellement être adaptées si l'on souhaite chiffrer du son ou/et de l'image, même si du point de vue de l'ordinateur ce sera une suite de nombres binaires.

Terminologie

Protocoles

Un système de chiffrement ou encore cryptosystème désignera la description d'un procédé de chiffrement/déchiffrement (la méthode, l'algorithme et son utilisation).
Nous parlerons

- de cryptographie pour désigner la conception de systèmes de chiffrements,
- et de cryptanalyse pour désigner la science et l'art de l'analyse d'un système de chiffrement, ce qui signifie en bref le « cassage » du système.

La cryptologie est la partie des mathématiques qui regroupent la cryptographie et la cryptanalyse.

Terminologie

Notations

Nous désignerons par M le message clair que l'on souhaite chiffrer et par C le message chiffré.
Nous noterons E l'opération de chiffrement et par D celle de déchiffrement.
Nous avons alors les égalités suivantes :

$$\begin{aligned} E(M) &= C, \\ D(C) &= M, \\ D(E(M)) &= M. \end{aligned}$$

Terminologie

Problème à résoudre

Voici les problèmes fondamentaux que doit résoudre la cryptographie :

- Authentification : il doit être possible pour le récepteur du message de garantir son origine. Une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre (usurpation d'identité),

Terminologie

Problème à résoudre

Voici les problèmes fondamentaux que doit résoudre la cryptographie :

- Authentification : il doit être possible pour le récepteur du message de garantir son origine. Une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre (usurpation d'identité),
- Intégrité : le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant sa transmission. Une tierce personne ne doit pas pouvoir substituer un message légitime (ayant pour origine l'émétteur) par un message frauduleux.

Terminologie

Problème à résoudre

Voici les problèmes fondamentaux que doit résoudre la cryptographie :

- Authentification : il doit être possible pour le récepteur du message de garantir son origine. Une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre (usurpation d'identité),
- Intégrité : le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant sa transmission. Une tierce personne ne doit pas pouvoir substituer un message légitime (ayant pour origine l'émétteur) par un message frauduleux.
- Non répudiation : un émetteur ne doit pas pouvoir nier l'envoi d'un message.

Ces trois contraintes sont très importantes du point de vue juridique.

Outline

Une page d'histoire

Chiffrements par substitution et transposition

Nous allons voir quelques systèmes rudimentaires de transformations (qui pour certains, ne sont pas vraiment des cryptosystèmes !), qui sont intéressants soit du point de vue historique, soit comme étude de cas.
Il s'agit des protocoles utilisés historiquement et qui ont mené à la cryptographie moderne.

Une page d'histoire

Chiffrements par substitution

Définition

Un « chiffrement par substitution » est un algorithme par lequel chaque caractère du message clair (écrit dans un alphabet donné) est substitué par un autre caractère dans le message chiffré (qui peut être écrit dans un alphabet différent de celui du message clair).

Une page d'histoire

Chiffrements par substitution

Définition

Un « chiffrement par substitution » est un algorithme par lequel chaque caractère du message clair (écrit dans un alphabet donné) est substitué par un autre caractère dans le message chiffré (qui peut être écrit dans un alphabet différent de celui du message clair).

En cryptographie classique, quatre types de chiffrement par substitution sont distingués :

- Substitution simple
- Substitution homophonique
- Substitution polygramique
- Substitution polyalphabétique

Une page d'histoire

Chiffrements par substitution

- Substitution simple : Un caractère du message clair est substituer par un caractère unique du message chiffré.

  Cela correspond le plus souvent à une permutation des caractères de l'alphabet des messages clairs.

Une page d'histoire

Chiffrements par substitution

- Substitution homophonique : Un caractère du message clair correspond à plusieurs caractères du message chiffré.

  Le principe est qu'à chaque caractère de l'alphabet des messages clairs est associé une liste de lettre dans l'alphabet des messages chiffrés (qui est en général beaucoup plus gros que celui pour les messages clairs), l'ensemble de ces listes formant une partition de l'alphabet des messages chiffrés.

  Par exemple on peut envoyer A vers un nombre de la liste $\{26, 40, 73, 58\}$, B vers un nombre parmi $\{12, 7, 26, 41\}$, etc. On choisit alors soit aléatoirement, soit suivant une « clef », les nombres associés aux caractères de l'alphabet des messages clairs.

Une page d'histoire

Chiffrements par substitution

- Substitution polygramique : le principe est de substituer des blocs de caractères, au lieu d'un seul caractère.

Une page d'histoire

Chiffrements par substitution

- Substitution polygramique : le principe est de substituer des blocs de caractères, au lieu d'un seul caractère.
- Substitution polyalphabétique : Il s'agit d'un ensemble de substitutions simples. Suivant la position du caractère dans le message clair, on applique une des substitutions simples. Ce sont des sortes de « permutations à paramètres ».

Une page d'histoire

Chiffrements par substitution

Le chiffrement de César entre dans la catégorie des « substitutions simples ».
Illustrons la méthode :
Par exemple décalage de trois lettres vers la droite :

E C O L E D H I V E R
devient
H F R O H L Y H U

ou d'une lettre vers la gauche :

E N S I A S
devien
D M R H Z R

Une page d'histoire

Chiffrements par substitution

Une autre méthode connue est $ROT13$ qui décale les caractères de 13 places vers la droite (i.e., A devient N), alors $M = ROT13(ROT13(M))$. Ces algorithmes sont facilement cassables.

Les substitutions homophoniques sont en général sensible aux attaques par messages clairs connus. Néanmoins, ces types de chiffrement sont faciles à casser à l'aide d'un ordinateur.

Une page d'histoire

Chiffrements par substitution

En fait, tous les chiffrements par substitutions sont cassables, en général par « analyse de fréquence » (cf. D. Kahn, « The codebreakers : The story of secret writing », Macmillan, 1967 et W. F. Friedman, « Elements of cryptanalysis », Aegan Park Press 1976).

Le point culminant de ces méthodes a été Enigma, la machine utilisée par les allemands durant la seconde guerre mondiale. Enigma : 1939–45, Allemagne.

Outline

Une page d'histoire

Chiffrements par transposition

Définition

Le « Chiffrement par transposition » consiste à appliquer une permutation des caractères sur le message clair en entier. De ce fait, le message chiffré est fait du même matériel que le message clair.

Ce type de chiffrement est de nouveau sensible à des attaques par analyse de fréquence de mots. Ces chiffrements sont en général cassables par les moyens de calculs actuels.
Nous les illustrons par l'exemple du XOR et du Masque Jetable (One-Time Pad).

Une page d'histoire

Chiffrements par transposition–XOR

Le principe du XOR est simple.

Le message est « XORÉ » bit à bit avec une clef donnée. Cette clef détermine la taille des blocs de bits.

Rappelons que le XOR correspond à l'addition dans $\mathbb{Z}/2\mathbb{Z}$.
L'opération est souvent désignée par par $\oplus$, et ses règles sont $0 \oplus 0 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$ et $1 \oplus 1 = 0$.
Si M est le message et K la clef, $C = M \oplus K$ et $M = C \oplus K$. C'est donc un « chiffrement » symétrique, mais il est facilement cassable.
$\Rightarrow$ Exercice : trouver un algorithme pour casser un chiffrement XOR.

Une page d'histoire

Chiffrements par transposition–Masque Jetable

Définition

Le Masque jetable (One–Time Pad) est une sorte de « chiffrement jetable » que l'on utilise qu'une seule fois. Ce chiffrement est souvent appelé « chiffrement Vernam » (en référence à Gilbert Vernam).

Il est robuste et l'on peut prouver qu'il est sure, mais il est difficile a déployer.

Le principe : ce n'est rien d'autre qu'une longue liste aléatoire de caractère que l'on utilise qu'une seule fois. Le chiffrement se fait en opérant une addition modulo 26 du message clair avec le « masque jetable » (aussi appelé oneŰtime pad). Le récepteur ayant les mêmes masques jetables, il lui est possible de déchiffrer les messages.

Une page d'histoire

Chiffrements par transposition–Masque Jetable

Par exemple, si le message est ONE TIME PAD et que la suite de caractères sur le pad est TBFRGFARFMGQ. Alors le message chiffré sera IPKLPSFHGQ. En effet,

$$\mathrm{O}(15) + \mathrm{T}\ (20) = \mathrm{I}(9) \bmod 26,\ \mathrm{N}(14)+\mathrm{B}(2) = \mathrm{P}(16) \bmod 26, \vdots$$

Le problème de cette méthode est qu'elle nécessite une grande quantité de donnée aléatoire (et non pseudo–aléatoires), ce qui est difficile à fournir. Notons que le principe du masque jetable est en fait utilisé dans les chiffrement à flots.

Outline

Terminologie

Algorithme et clefs

Un algorithme de cryptographie (ou encore méthode cryptographique) désigne les fonctions mathématiques utilisées pour le chiffrement et le déchiffrement. Ces fonctions peuvent aussi être regroupées au sein d'une seule fonction (ou algorithme).
Si initialement, la sécurité d'un cryptosystème reposait entièrement sur le fait que l'algorithme de cryptographie était tenu secret, ce n'est que vers la fin du 19ième siècle qu'a été reconnu le fait que **la sécurite ne devait pas reposer sur la méthode cryptographique**.
Les articles d'Auguste Kerckhoffs (« La cryptographie militaire », Journal des sciences militaires, vol. IX, pp. 5 Ű- 38, Janvier 1883, pp. 161 -Ű 191, Février 1883) sont les précurseurs des fondements de la cryptographie moderne.

Terminologie

Les règles de Kerckhoffs

Voici, **texto**, les six règles de Kerckhoffs pour la conception de « cryptosystème militaire » :

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

Terminologie

Les règles de Kerckhoffs

Voici, **texto**, les six règles de Kerckhoffs pour la conception de « cryptosystème militaire » :

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

Terminologie

Les règles de Kerckhoffs

Voici, **texto**, les six règles de Kerckhoffs pour la conception de « cryptosystème militaire » :

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

Terminologie

Les règles de Kerckhoffs

Voici, **texto**, les six règles de Kerckhoffs pour la conception de « cryptosystème militaire » :

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;

Terminologie

Les règles de Kerckhoffs

Voici, **texto**, les six règles de Kerckhoffs pour la conception de « cryptosystème militaire » :

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

Terminologie

Les règles de Kerckhoffs

Voici, **texto**, les six règles de Kerckhoffs pour la conception de « cryptosystème militaire » :

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Terminologie

La cryptographie à clé publique

En pratique, le respect des règles de Kerckhoffs impose que la méthode cryptographique intègre des clefs pour le chiffrement ou le déchiffrement.
Nous noterons alors les fonctions E et D par E_{K1} et D_{K2}, ou E_K et D_K si les clefs sont identiques.
En général le nombre de clefs possibles est trés grand.

Terminologie

La cryptographie à clé publique

En pratique, le respect des règles de Kerckhoffs impose que la méthode cryptographique intègre des clefs pour le chiffrement ou le déchiffrement.
Nous noterons alors les fonctions E et D par E_{K1} et D_{K2}, ou E_K et D_K si les clefs sont identiques.
En général le nombre de clefs possibles est trés grand.
Nous parlerons d'espace des clefs pour désigner l'ensemble de toutes les clefs possibles.
Du point de vue mathématique, le cryptosystème représente la méthode cryptographique, l'espace des clefs ainsi que les ensembles de tous les messages clairs et chiffrés possibles.

Outline

Les deux grandes familles de cryptosystèmes

Les cryptosystèmes symétriques

Chiffrement symétrique

Le terme de cryptosystème symétrique s'applique lorsque les clefs de chiffrement et déchiffrement peuvent se déduire (en temps polynômial) l'une de l'autre.
En pratique la clef utilisée pour le déchiffrement est identique à celle utilisée pour le chiffrement.

Les deux grandes familles de cryptosystèmes

Les cryptosystèmes symétriques

Chiffrement symétrique

Le terme de cryptosystème symétrique s'applique lorsque les clefs de chiffrement et déchiffrement peuvent se déduire (en temps polynômial) l'une de l'autre.
En pratique la clef utilisée pour le déchiffrement est identique à celle utilisée pour le chiffrement.

$\Rightarrow$ Le défaut pratique de ce type de système est que l'émetteur et le récepteur doivent avoir la même clef afin de communiquer, ce qui implique une transmission de clef et donc l'existence d'un canal sure (même si la sureté de se canal ne doit être garanti que pour un moment bref).

Les deux grandes familles de cryptosystèmes

Les cryptosystèmes symétriques

Chiffrement symétrique

Le terme de cryptosystème symétrique s'applique lorsque les clefs de chiffrement et déchiffrement peuvent se déduire (en temps polynômial) l'une de l'autre.
En pratique la clef utilisée pour le déchiffrement est identique à celle utilisée pour le chiffrement.

$\Rightarrow$ Le défaut pratique de ce type de système est que l'émetteur et le récepteur doivent avoir la même clef afin de communiquer, ce qui implique une transmission de clef et donc l'existence d'un canal sure (même si la sureté de se canal ne doit être garanti que pour un moment bref).
$\Rightarrow$ L'avantage est que le chiffrement est très rapide.

Exemples

les plus connus : DES, triple Ű DES, AES, RC4, masque jetable.

Les deux grandes familles de cryptosystèmes

Les cryptosystèmes symétriques

Il existe deux catégories de chiffrement symétrique (noter que maintenant l'expression a un sens, puisque chiffrement et déchiffrement sont des algorithmes similaires) :

- Chiffrements par flots [stream ciphers] : ce sont des systèmes de chiffrement qui opèrent sur le message clair par bit (ou quelquefois par petit groupement de bits).
- Chiffrements par blocs [block ciphers] : ce sont des systèmes de chiffrement qui opèrent sur le message clair par « grand » groupes de bits (e.g., 64 bits).

Moralement les systèmes par flots opèrent sur les caractères, alors que ceux par blocs opèrent sur les mots.

Outline

Les deux grandes familles de cryptosystèmes

Les cryptosystèmes asymétriques

Chiffrement asymétrique (a.k.a. « à clef public »)

Ce sont des algorithmes dont la clef de chiffrement est différente de la clef de déchiffrement (i.e., l'algorithme de déchiffrement ne se déduit pas, en temps polynômial, de l'algorithme de chiffrement).

De ce fait, il est possible de rendre public la clef de chiffrement. La clef de déchiffrement est alors appelée la clef privée.

Représentation

Le principe se représente par l'image des boîtes et cadenas.

Les deux grandes familles de cryptosystèmes

Les cryptosystèmes asymétriques

Le principe de la cryptographie à clef public a été introduit par Whitfield Diffie et Martin Hellman en 1976 (aussi introduit séparément par Ralph Merkle).
Utilise une fonction à sens unique (clé publique) avec trappe (clé privée).
$\Rightarrow$ Cela permet de résoudre les problèmes de la cryptographie symétrique.
Inconvénient : 100 à 1000 fois plus lent que le chiffrement symétrique. En pratique on mélange les deux (SSL, SSH, PGP par exemple).

Outline

Cryptanalyse

Définition

La cryptanalyse s'oppose, en quelque sorte, à la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de se passer de cette dernière ; et retrouver le message caché sans connaitre la clé privée de l'algorithme.

Cryptanalyse

Définition

La cryptanalyse s'oppose, en quelque sorte, à la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de se passer de cette dernière ; et retrouver le message caché sans connaitre la clé privée de l'algorithme.

Il existe quatre types d'attaques générales :

- Attaque par analyse demessages chiffrés [Ciphertext−only attack],
- Attaque par message clair connu [Known−plaintext attack],
- Attaque à texte (clair ou chiffré) choisi [Choosen−plaintext ou Choosen−ciphertext attack],
- Attaque adaptative à texte (clair ou chiffré) choisi [Adaptative−Choosen−plaintext ou Adaptative−Choosen−ciphertext attack].

Cryptanalyse

Attaque par analyse de messages chiffrés

Attaque par analyse demessages chiffrés [Ciphertext−only attack]

:

Dans le cadre de cette attaque, le cryptanalyste dispose d'une série de messages chiffrés, éventuellement chiffré avec la même clef.
Le but est de trouver le message clair pour un grand nombre de messages chiffrés, voir de déterminer la clef (ou les clefs).

Mathématiquement : L'attaquant connait C_i sachant que $C_i = E_K(M_i)$ pour $i = 1, \ldots, N$, il veut en déduire M_{N+1} connaissant C_{N+1}.

Cryptanalyse

Attaque par message clair connu

Attaque par message clair connu [Known−plaintext attack] :

Cette attaque est aussi appelée attaque par message clair/message chiffré.
Le cryptanalyste possède un ensemble de messages clairs et de messages chiffrés correspondants.
Le problème est alors de retrouver la clef à partir de ces données ou un algorithme pour déchiffré n'importe quel autre message (probablement chiffré avec la même clef).

Mathématiquement : L'attaquant connait des paires (M_i, C_i) fixées avec $C_i = E_K(M_i)$ pour $i = 1, \ldots, N$, et l'on veut en déduire soit M_{N+1} connaissant C_{N+1}, soit K.
$\Rightarrow$ Noter que dans le cas de cryptosystème à clef public, le cryptanaliste peut fabriquer autant de pair clair/chiffré qu'il veut.

Cryptanalyse

Attaque à texte choisi

Attaque à texte (clair ou chiffré) choisi [Choosen−plaintext ou Choosen−ciphertext attack] :

Le cryptanalyste peut soit choisir des messages clairs et leurs équivalents chiffrés (attaque à message claire choisi), soit choisir des messages chiffrés et leurs équivalents clairs.
C'est l'une des attaques les plus dangereuses, car le cryptanalyste peut choisir des formatages particuliers de textes, permettant d'obtenir des informations supplémentaires sur la clef.

Mathématiquement : L'attaquant a la possibilité de fabriquer des paires (C_i, M_i) sachant que $C_i = E_K(M_i)$ (ou $M_i = D_K(C_i)$) pour $i = 1, \ldots, N$, et il veut en déduire soit M_{N+1} connaissant C_{N+1}, soit K.
A titre d'illustration, la vulnérabilité dans SSL (protocole RSA PKCS#1) qui a été trouvé en 1998 était du type « Attaque à texte choisi ».

Cryptanalyse

Attaque adaptative à texte choisi

Attaque adaptative à texte (clair ou chiffré) choisi [Adaptative−Choosen−plaintext ou Adaptative−Choosen−ciphertext attack] :

Cette attaque est un cas spécial du précédent, où le cryptanalyste peut fabriquer la paire (C_{i+1}, M_{i+1}) en fonction du résultat obtenu à l'étape i.

Outline

Sécurité des algorithmes

Classification

En 1994, Lars Knudsen a proposé une classification du « cassage » d'un cryptosystème (cela peut s'appliquer au procédé général ou bien une implémentation particulière du procédé cryptographique).

Sécurité des algorithmes

Classification

Cette classification est la suivante, et est utile en pratique pour l'évaluation de cryptosystèmes :

1. « Total break » : on est capable de trouver la clef K tel que $C = D_K(M)$.

Sécurité des algorithmes

Classification

Cette classification est la suivante, et est utile en pratique pour l'évaluation de cryptosystèmes :

1. « Total break » : on est capable de trouver la clef K tel que $C = D_K(M)$.
2. « Déduction globale » : l'attaquant est capable de trouver un algorithme alternatif pour le déchiffrement sans connaissance de la clef (i.e., l'algorithme produit $D_K(C)$ sans connaissance de K).

Sécurité des algorithmes

Classification

Cette classification est la suivante, et est utile en pratique pour l'évaluation de cryptosystèmes :

1. « Total break » : on est capable de trouver la clef K tel que $C = D_K(M)$.
2. « Déduction globale » : l'attaquant est capable de trouver un algorithme alternatif pour le déchiffrement sans connaissance de la clef (i.e., l'algorithme produit $D_K(C)$ sans connaissance de K).
3. « Déduction locale » (cassage ou craquage d'une instance) : l'attaquant est capable de trouver le message clair à partir du message chiffré.

Sécurité des algorithmes

Classification

Cette classification est la suivante, et est utile en pratique pour l'évaluation de cryptosystèmes :

1. « Total break » : on est capable de trouver la clef K tel que $C = D_K(M)$.
2. « Déduction globale » : l'attaquant est capable de trouver un algorithme alternatif pour le déchiffrement sans connaissance de la clef (i.e., l'algorithme produit $D_K(C)$ sans connaissance de K).
3. « Déduction locale » (cassage ou craquage d'une instance) : l'attaquant est capable de trouver le message clair à partir du message chiffré.
4. « Déduction partielle » : l'attaquant est capable d'obtenir une information partielle sur la clef ou le message clair. Par exemple, cela peut être la connaissance de quelques bits de la clef.

Sécurité des algorithmes

Terminologie

Un algorithme est dit inconditionnellement sure, si quel que soit le nombre de messages chiffrés à la disposition du cryptanalyste, il n'y a pas assez d'information pour déduire le message clair.
En pratique, les cryptographes s'intéressent aux systèmes qui sont difficiles à casser, même s'ils disposent d'une grande puissance de calcul, il s'agit des algorithmes calculatoirement sures.
La complexité du craquage de l'algorithme s'exprime alors par le nombre d'opérations nécessaire pour le craquer.
Actuellement un algorithme nécessitant au moins 2^{80} opérations (élémentaires) est considéré sure (avec une raisonnable marge pour le futur). Néanmoins, ce chiffre à tendance à être ré−évaluer à la hausse (disons 2^{85}...).

Outline

Cryptographie vs stéganographie

La stéganographie est l'art de cacher un message dans un autre message, et cela sans être vu.
En soit le message n'est pas transformer (bien qu'il pourrait l'être).
Si l'attaquant connait la recette du « déguisement » il peut retrouver facilement le message, a moins que ce dernier ait lui aussi été chiffré.

Cryptographie vs stéganographie

La stéganographie est l'art de cacher un message dans un autre message, et cela sans être vu.
En soit le message n'est pas transformer (bien qu'il pourrait l'être).
Si l'attaquant connait la recette du « déguisement » il peut retrouver facilement le message, a moins que ce dernier ait lui aussi été chiffré.
Actuellement, la méthode la plus répandu de stéganographie se fait via les images :
pour cela on remplace le bit le moins significatif pour chaque octet de l'image (qui en général encode une couleur) par un bit du message a stéganographier. Ce type de modification est quasiment imperceptible pour un oeil humain.

Cryptographie vs stéganographie

La stéganographie est l'art de cacher un message dans un autre message, et cela sans être vu.
En soit le message n'est pas transformer (bien qu'il pourrait l'être).
Si l'attaquant connait la recette du « déguisement » il peut retrouver facilement le message, a moins que ce dernier ait lui aussi été chiffré.
Actuellement, la méthode la plus répandu de stéganographie se fait via les images :
pour cela on remplace le bit le moins significatif pour chaque octet de l'image (qui en général encode une couleur) par un bit du message a stéganographier. Ce type de modification est quasiment imperceptible pour un oeil humain.
Par exemple, dans un album d'une trentaine de photos numériques au format 1024×768, on peut y cacher un livre de 300 pages.

Où trouver de la cryptographie ?

Partout !

- Armée (et plus généralement sécurité au niveau des états),
- Système bancaire,
- Internet (achats, identification, déclaration d'impôts),
- Téléphones portables, clefs électroniques (e.g., voitures)
- TV payante,
- Cartes d'identités électroniques, cartes de santé,
- Vote électronique,
- DVD, HD Ű DVD, Blue Ray, audio numérique (certains formats, e.g., WMA, AAC),
- Consoles de jeux vidéos (e.g., Xbox, Xbox360).