Master RSS
UB

CRYPTOLOGIE

INTRODUCTION A LA SI
&
LA CRYPTOLOGIE

INTRODUCTION

- La continuité de l'activité de l'entreprise appelle celle de son système d'information. Cette continuité ne peut être assurée que par la mise en place de moyens de protection apportant un niveau de sécurité adapté aux enjeux spécifiques de l'entreprise.
- La sécurité des réseaux est devenue l'un des éléments clés de la continuité des SI de l'entreprise.

INTRODUCTION

- Comme toute composante critique, le réseau doit faire l'objet d'une politique de sécurité tenant compte de tous les besoins d'accès au réseau d'entreprise:
  - accès distants
  - échange des mails
  - commerce électronique
  - interconnexion des tierces parties
  - etc..

LA SÉCURITÉ INFORMATIQUE VISE GÉNÉRALEMENT CINQ PRINCIPAUX OBJECTIFS :

- L'**intégrité** c'est-à-dire garantir que les données sont bien celles que l'on croit être.
- La **confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées .
- La **disponibilité**, les services (ordinateurs, réseaux, périphériques, applications…) et les informations (données, fichiers…) doivent être accessibles aux personnes autorisées quand elles en ont besoin.
- La **non répudiation**, permettant de garantir qu'une transaction ne peut être niée.
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

PROBLÈMES DE SÉCURITÉ

Problèmes dus à des failles notamment dans les protocoles de communication

Toute information circulant sur Internet peut être capturée et enregistrée et/ou modifiée

Problème de confidentialité et d'intégrité

Toute personne peut falsifier son adresse IP (***spoofing***) ce qui engendre une fausse identification

Problème d'authentification

Aucune preuve n'est fournie par Internet quant à la participation dans un échange électronique

Problème d'absence de traçabilité

LES DIFFERENTS ASPECTS DE LA SECURITE

la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

- **La sécurité physique**, soit *la sécurité au niveau des infrastructures matérielles* : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels
- **La sécurité personnelle** **:**la sensibilisation des utilisateurs aux problèmes de sécurité

LES DIFFERENTS ASPECTS DE LA SECURITE

- **La sécurité logique:** c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- **La sécurité des communications:** technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
- **La sécurité procédurale:** sert de tampon entre les commandes juridiques et les livraisons technique

LES CAUSES DE L'INSECURITE

On distingue généralement deux types d'insécurités :

- **l'état actif d'insécurité**, c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur)
- **l'état passif d'insécurité**, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose

LES MENACES :

La menace est définie comme étant une violation potentielle de la sécurité. Nous distinguerons les types de menace suivants :

- **La menace accidentelle :** menace d'un dommage non intentionnel envers le SI. Cette menace peut découler d'une catastrophe naturelle (incendie, inondation, tremblement de terre,...), d'une erreur dans l'exploitation du SI (manipulation, saisie, ...) ou de pannes qu'elles soient matérielles ou de logicielles.

LES MENACES :

- **La menace intentionnelle** ou délibérée : par opposition à la précédente, elle est le fait d'un acte volontaire.
- **La menace active** : menace de modification non autorisée et délibérée de l'état du système. Si elle venait à se concrétiser le SI, ou ses informations, subiraient un dommage ou une altération bien réelle.
- **La menace passive** : menace de divulgation non autorisée des informations, sans que l'état du système soit modifié. Une écoute de ligne ou une lecture de fichier sont des exemples de menaces passives.

LES VULNÉRABILITÉS :

Les vulnérabilités : ce sont les failles de sécurité dans un ou plusieurs systèmes. Une vulnérabilité peut se définir comme une faiblesse ou une faille dans les procédures de sécurité, les contrôles administratifs, les contrôles internes d'un système, qui pourrait être exploitée pour obtenir un accès non autorisé à un SI, à un de ses services ou à des informations

Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

LES RISQUES :

Un risque est un danger, un inconvénient plus ou moins probable auquel on est exposé dans un système d'information. Il est généralement admis que le risque est une fonction de la menace, des vulnérabilités et des contre-mesures (ensemble de mesures adoptées pour contrer les menaces et les failles).

LES ATTAQUES:

Les attaques (exploits):elles représentent les moyens d'exploiter une vulnérabilité.

Les informations ou les systèmes d'informations d'une entreprise peuvent subir des dommages de plusieurs façons : certains intentionnels (malveillants), d'autres par accident. Ces événements seront appelés des « attaques ».

Il existe quatre catégories principales d'attaque :

- L'accès;
- La modification;
- Le déni de service;

POLITIQUE DE SÉCURITÉ

La politique de sécurité est l'expression de ces objectifs.

Elle indique l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place afin :

- d'empêcher (ou tout au moins freiner) la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;
- de détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;
- d'intervenir afin d'en limiter les conséquences et, le cas échéant, poursuivre l'auteur du délit.

POLITIQUE DE SÉCURITÉ

il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en œuvre se fait selon les **quatre étapes suivantes** :

- Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;

POLITIQUE DE SÉCURITÉ

- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;

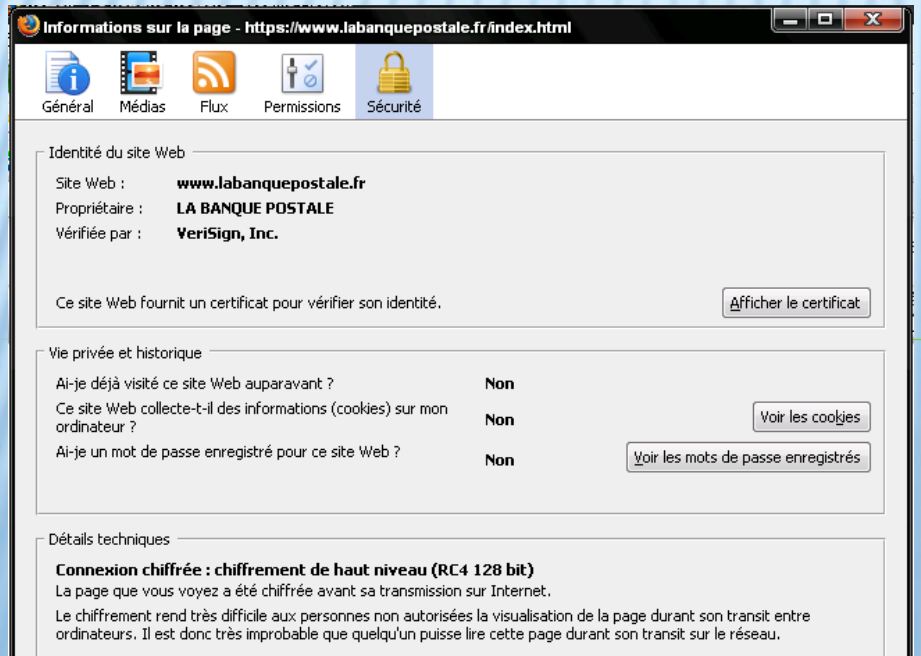
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

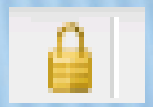
L'UTILISATION DE LA CRYPTOLOGIE NOUS GARANTIS:

- L'**intégrité.**
  - identification/signature
- La **confidentialité**.
  - chiffrement
- La **non répudiation**.
  - empreinte digitale
- L'**authentification**.
  - hachage/signature

Domaines d'application de la cryptographie:

- Internet:
  - Sites bancaires
  - Sites de vente en ligne
  - etc.





Domaines d'application de la cryptographie:

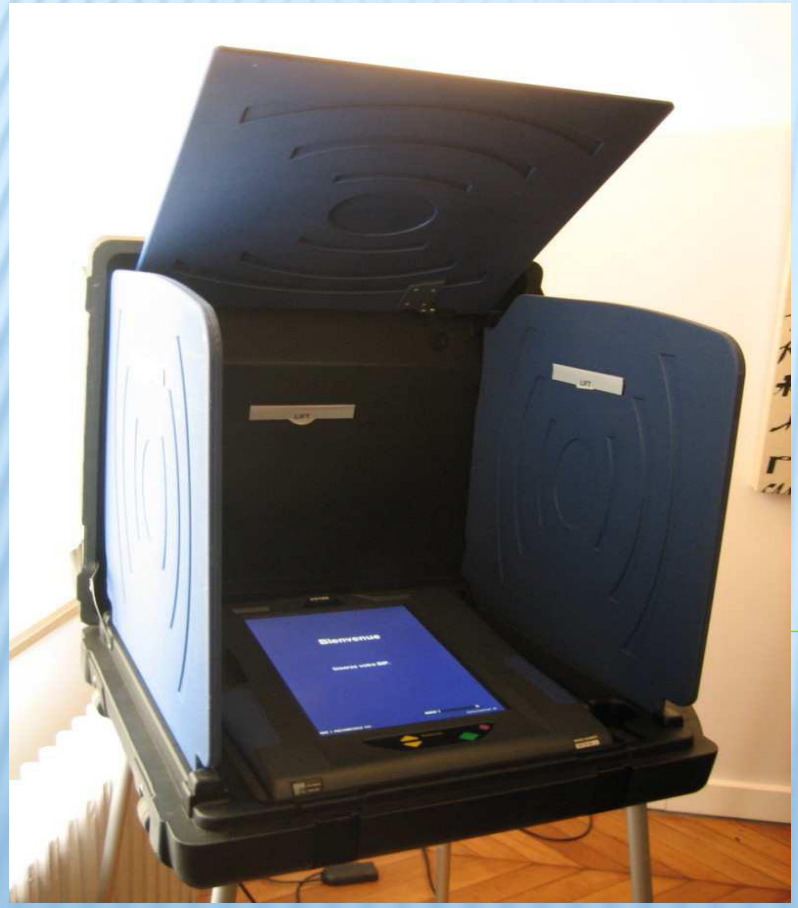
- Carte à puce : carte de paiement

Domaines d’application de la cryptographie:

- Carte à puce : carte vital

Domaines d'application de la cryptographie:

- Vote électronique
- Machines à voter
- Vote en ligne



DOMAINES D'APPLICATION DE LA CRYPTOGRAPHIE:

- Module de Sécurité HSM

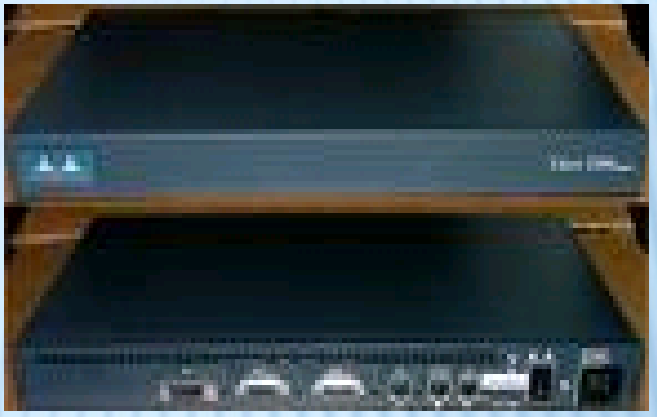
Le module HSM est un appareil infalsifiable qui offrant les fonctions cryptographiques nécessaires à la sécurisation des transactions sur les réseaux financiers.

DOMAINES D'APPLICATION DE LA CRYPTOGRAPHIE:

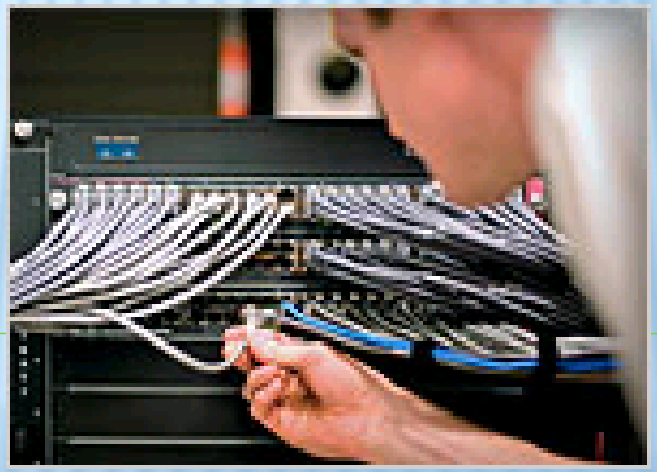
- Télécommunications
  - GSM
  - Wifi

DOMAINES D'APPLICATION DE LA CRYPTOGRAPHIE:

- Routeur Cisco
- IPSEC, VPN, AAA



- PIX Firewall
- IPSEC, VPN, AAA



LA CRYPTOLOGIE

CRYPTOLOGIE

- Du grec Kruptos = cacher et logos = science
- Science qui se divise en deux familles :

• Cryptographie : produire des messages secrets

• Cryptanalyse : percer les messages secrets

- L'origine de la cryptographie remonte à 4000 avant J.C en Egypte pharaonique.
- Longtemps réservée aux communications militaires et diplomatiques mais depuis s'est largement vulgarisée. . .

CRYPTOLOGIE

- Tous les algorithmes et protocoles inventés avant les années 70, ont été complètement cassées.
- On se réfère à cette période en parlant de période de la cryptographie classique ou artisane (art des codes secrets): 4000 ans avant J.C jusqu'en 1975/76.
- Dans les années 70, considérées comme le début de l'époque moderne, la cryptographie, devenue la science des codes secrets, s'est développée dans le monde civil surtout avec la prolifération des systèmes de communication et de nouveaux services des années 1990/2000: Internet, Commerce électronique.

CRYPTOLOGIE

- Cette nouvelle cryptographie est dite moderne par ce que entre autres:

❖toutes ses branches ont connues une modélisation mathématique plus cohérente

❖ elle a produit des outils (algorithmes, protocoles,...) qui restent encore robustes malgré le développement des techniques de cryptanalyse

❖ elle prend en charge presque totalement tous les besoins de sécurité dans un schémas de communication

❖ son application dans le monde civil a permis le développement de nouveaux métiers ou services: commerce électronique, e-banking, consultation de données personnelles sur internet,...

PRINCIPE DE FONCTIONNEMENT DE LA CRYPTOGRAPHIE

Définitions utiles

- **Message clair** : Le message originel que Mr Ndiaye veut envoyer à Mme Anne sans que personne d'autre que Anne ne puisse le lire
- **Clé.** Données (Nombre très grand) utilisé par un algorithme de cryptage pour chiffrer et déchiffrer des données
- **Chiffrer** : transformer un message clair en un message codé qui n'est pas compréhensible sans avoir la clé de déchiffrement.
- **Déchiffrer** : retrouver le message original **AVEC** la clé de déchiffrement.

Définitions utiles

- **Décrypter** : retrouver le message original **SANS** la clé de déchiffrement.

- **Algorithme de cryptage.** Algorithme: une procédure bien définie qui:

• d'abord prend en entrée une valeur, une donnée (élément ou partie d'un ensemble)
• ensuite exécute une suite finie de règles ou d'opérations (de calculs,...)
• enfin donne un résultat.

NB Il arrive qu'on considère une fonction (application) mathématique comme un algorithme.

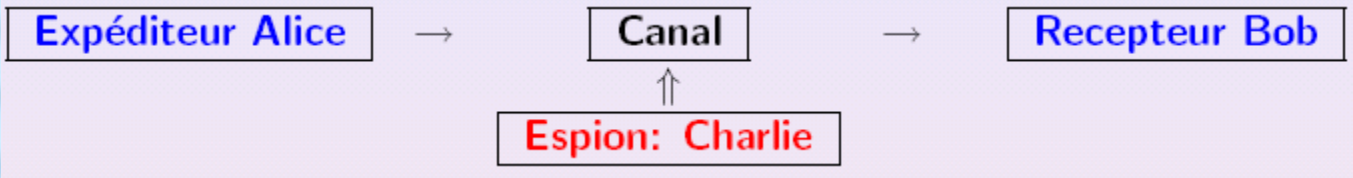
- **Protocole** : Description de l'ensemble du système : algorithmes de cryptage et décryptage, choix et utilisation des clés...

Définitions utiles

- **Information** élément de connaissance: texte, son, image, vidéo,...
- **Traiter/manipuler** une information: lire, écrire/modifier, effacer une information
- **Canal:** moyen de transmission permettant de convoyer une information entre deux partenaires d'une communication; par exemple ligne téléphonique, fibre optique, moyen de communication sans fils,...

Définitions utiles

Dans l'étude des codes secrets (cryptographie) on considère le scenario de communication suivant:



- **Entités**: quelqu'un (= personne) ou quelque chose (= machine,...) capable d'envoyer, de recevoir ou de traiter/manipuler une information. Dans la pratique, c'est l'un des partenaires d'une communication. Par exemple Alice, Bob et Charlie sont des entités.

Définitions utiles

- **Espion/adversaire/ennemie/attaquant:** entité malveillante cherchant a agir illégalement sur un canal de communication dans le but de nuire: violer la confidentialité des données, intercepter et modifier les données, usurper l'identité d'une entité légitime, etc.

- **Canal non sûr**: canal dans lequel un espion peut réaliser avec succès ses forfaits

Exemples des cryptosystèmes

Exemple1: Algosym1

Soit "M = **Mon premier cours de crypto**" et f la transformation "f = **Inverser l'ordre des lettres**" Alors

$f(M)$ = **OTPYRCEDSRUOCRIEMERPNOM**

$f =$ algorithme de chiffrement;

$M =$ texte claire

$M' = f(M) =$ texte chiffré ou cryptogramme;

$f^{-1} = f$; $f^{-1} =$ algorithme de déchiffrement

$f^{-1} \circ f(M) = M \Rightarrow$ texte déchiffré

$\Rightarrow$ **Inconvénient de cet algorithme?** Si on connait f, on peut chiffrer et déchiffrer donc f n'est pas un bon algorithme!

Exemples des cryptosystèmes

Considérons l'algorithme qui déplace chaque lettres de K positions vers la droite dans l'ordre alphabétique puis inverser l'ordre des lettres.

REMARQUE: dans cet exemple, les fonctions de chiffrement et de déchiffrement sont paramètres. Le paramètre K est appelé **clé**. Ainsi, on peut rendre publique l'algorithme et quand deux entités veulent communiquer, ils choisissent leur clé k qui restera secrète.

L'ensemble des valeurs possibles du paramètre k est appelé espace des clés.

Exemples des cryptosystèmes

- En cryptographie, pour les systèmes de chiffrement on utilise que des algorithmes qui fonctionnent avec des clés.
- Déjà, depuis la fin du 19eme siècle, Kerckoffs avait énoncé, un principe fondamental en cryptographie (dans son article sur la cryptographie militaire) qui rendait fondamental le rôle de la clé.

Principe de Kerchkoffs

La sécurité d'un code cryptographique ne doit pas reposer sur le secret de l'algorithme mais sur celui des clés utilisées

- D'ailleurs, en cryptographie académique, on suppose toujours que l'algorithme est connu de tous. Cela permet aux spécialistes de le tester afin de mettre en évidence ses faiblesses et de l'améliorer en conséquence ou lui trouver un successeur (=Cryptanalyse).

Exemples des cryptosystèmes

Algorithme secret

- Chaque expéditeur / destniatire doit créer son propre algorithme et s'assurer tout seul que son algo est costaud;
- un plus petit nombre d'utilisateurs = une plus petite motivation à casser l'algo sauf si les messages chiffrés ont une très grande valeur;
- Indisponible pour autres utilisateurs ou autres pays;
- Généralement l'algoritme est implémenté en version embarquée au lieu de logiciel
- La cryptanalyse doit inclure la récupération de l'algorithme;
- Très utilisé dans l'industrie militaire (cryptographie embarquée)

Exemples des cryptosystèmes

Algorithme publié

- Démocratiser l'accées aux algorithmes de cryptographie;
- L'utilisateur est dispensé de devoir créer son propre algorithme et il fait confiance à l'algo adopté par tous;
- Il est plus facile de fabriquer et garder des clés (grands nombres) que de concevoir des algorithmes;
- La seule manière fiable dévaluer la sécurité du code en permettant à la communauté scientifique mondiale de le tester pour trouver les faiblesses (involontaires) et les trappes cachées par les constructeurs;
- Grand nombre de réalisations = prix réduits + performence élevée
- Implémentation logicielle contre solution embarquée
- Standardisation locale et internationale

Exemples des cryptosystèmes

Modélisation des systèmes de chiffrement

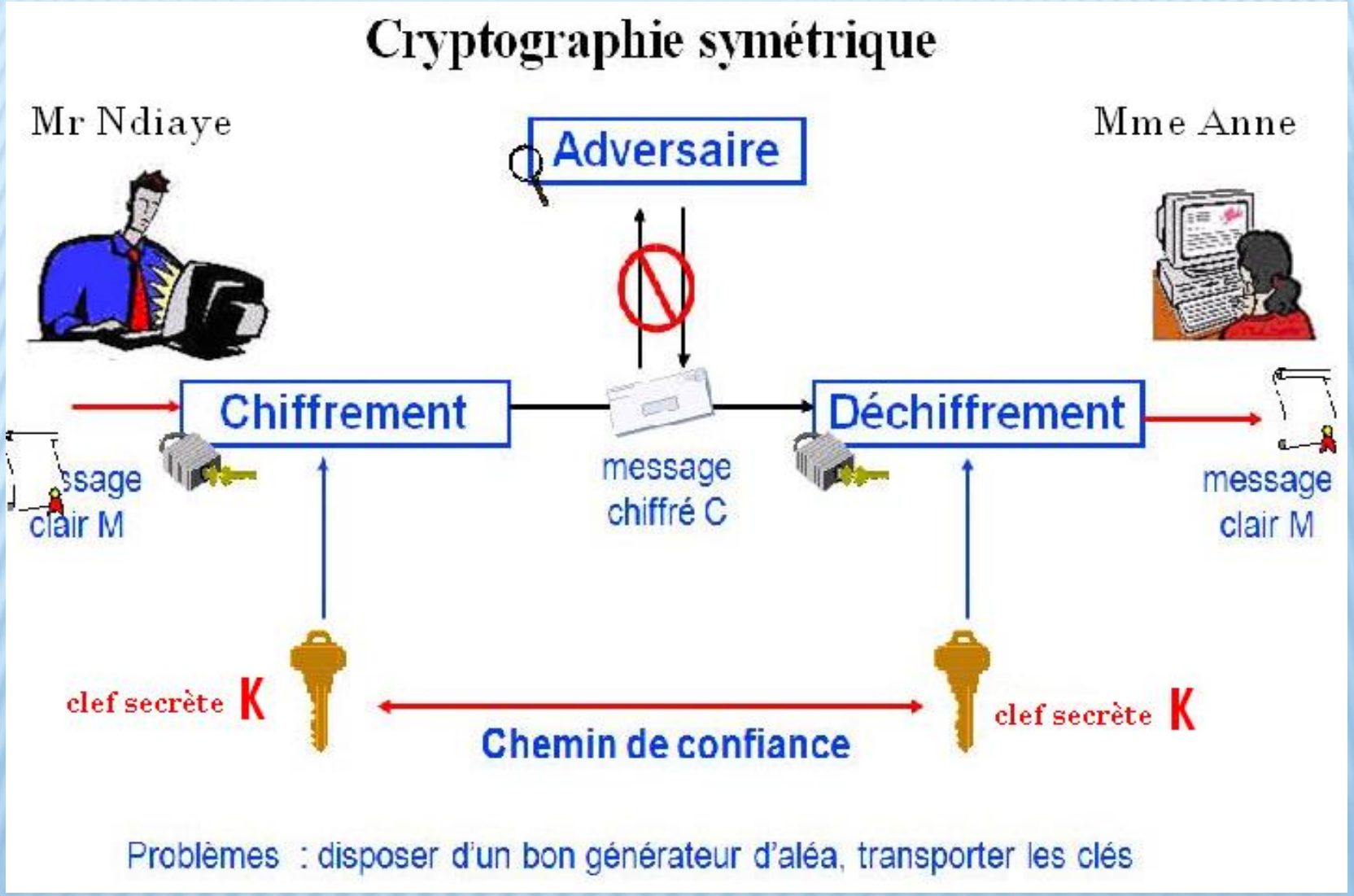
Un système de cryptographie est composé d'un quintuplet $(\mathcal{P}, \mathcal{C}, C_k, D_{k'}, \mathcal{K})$ où:

- $\mathcal{P}$ est un ensemble appelé espace des textes clairs
- $\mathcal{C}$ est un ensemble appelé espace des textes chiffrés
- $\mathcal{K}$ est un ensemble appelé espace des clés
- $Gen_{\mathcal{K}}$ un algorithme de génération de clés (=les éléments de $\mathcal{K}$);
- $C_k : \mathcal{P} \rightarrow \mathcal{C}$ est une fonction inversible à gauche appelée fonction de chiffrement et qui dépend d'un parametre k appelé clé.
- $D_{k'} : \mathcal{C} \rightarrow \mathcal{P}$ est la fonction inverse gauche de C_k (i.e $D_{k'} \circ C_k(m) = m, \forall m \in \mathcal{P}$) et est appelée fonction de déchiffrement (dépendant de la clé k') .

CRYPTOGRAPHIE

SYMETRIQUE ASYMETRIQUE HYBRIDE

CRYPTOGRAPHIE SYMÉTRIQUE : PRINCIPES



LES PROTOCOLES SYMÉTRIQUE

D.E.S. (Data Encryption Standard)

- **Histoire** : crée par IBM. Standard du NIST (National Institute of Standards and Technology) depuis 1976 : norme FIPS 46-3
- **Bloc** : codage par blocs de 64bits
- **Clé** : 64 bits avec 8 bits de parité donc 56 bits effectifs
- **Spécificités** : plusieurs applications augmentent la sûreté

LES PROTOCOLES SYMÉTRIQUE

I.D.E.A (International Data Encryption Algorithm)

- **Histoire** : développé par Lai et Massey en 1992
- **Bloc** : codage par blocs de 64bits
- **Clé** : clé de 128 bits
- **Spécificités** : utilise trois structures différentes pour une généralisation des diagrammes de Feistel

LES PROTOCOLES SYMÉTRIQUE

A.ES (Advanced Encryption Standard)

Histoire : crée par J. Daemen et V. Rijmen. Remplace D.E.S. comme standard du NIST depuis 2000

- **Bloc** : codage par blocs de 64bits
- **Clé** : clé de 128, 192 ou 256 bits
- **Spécificités** : résistance à toutes les attaques connues ; très grande rapidité pour le cryptage et décryptage ; utilise des méthodes de substitution-permutation.

Cryptographie Symétrique

- **Principe :**

  la même clé sert à chiffrer et déchiffrer le message.

- **Avantage :**

  Chiffrement et déchiffrement du message rapide.

- **Inconvénient :**

  on est obligé de donner la clé au destinataire du message « codé ».

Risque d'interception de la clé !

Cryptographie Symetrique

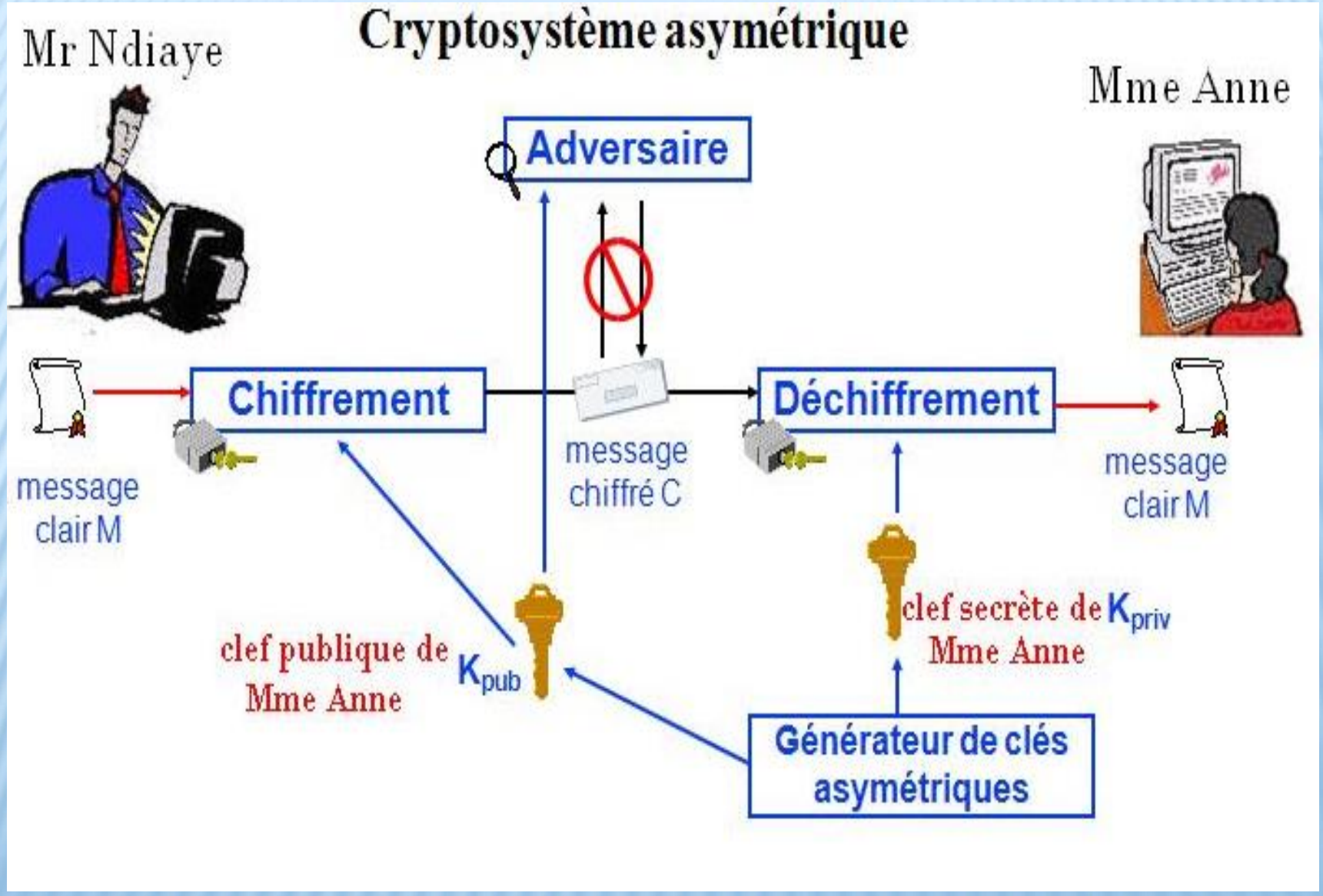
UN EXEMPLE : LES CODES CÉSAR

- Principe : décalage de l'alphabet.
- Exemple : le code Avocat (A vaut K)
  - Lors du chiffrement, on décale chaque lettre du message de 10 lettres dans l'ordre alphabétique.
  - Opération inverse lors du déchiffrement.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	…
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	…

Exemple : chiffrement et déchiffrement de : « Le message »

CRYPTOGRAPHIE ASYMÉTRIQUE : PRINCIPES



LES PROTOCOLES ASYMÉTRIQUE

R.S.A (Rivest Shamir Adleman)

- **Histoire** : Publié en 1977 par Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman. Le premier système à clé publique solide à avoir été inventé
- **Clé** : clé de 128, 192 , 256, 512, 1024, 2048 bits
- **Spécificités** : le RSA est fondé sur la difficulté de factoriser des grands nombres.

LES PROTOCOLES ASYMÉTRIQUE

Taher Elgamal

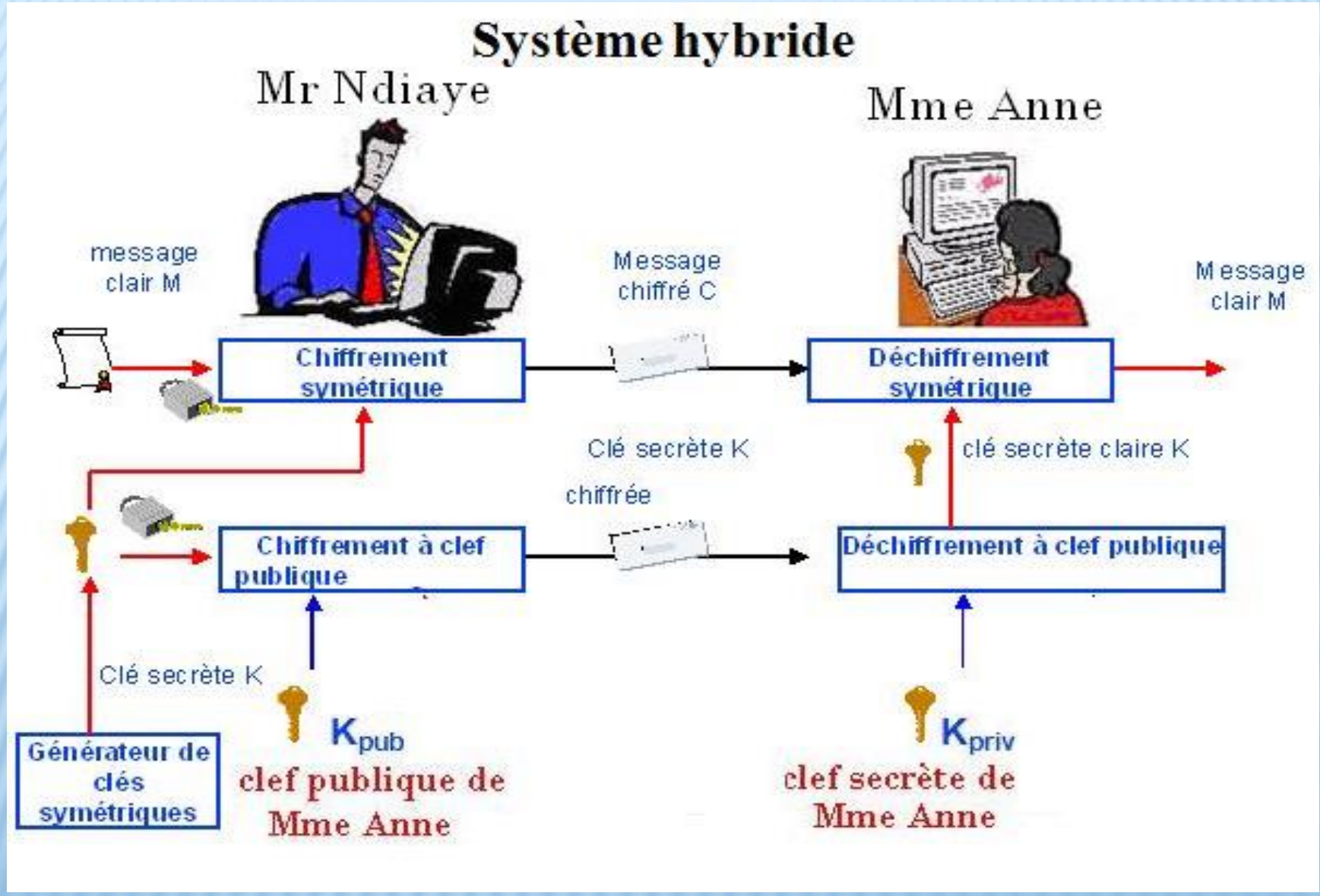
- **Histoire** : Publié en 1985 par **Taher Elgamal**
- **Clé** : clé de 128, 192 , 256, 512, 1024, bits
- **Spécificités** : la sécurité du cryptosystème Elgamal repose, comme le protocole de Diffie et Hellman, sur la difficulté de calculer le logarithme discret.

CRYPTOGRAPHIE HYBRIDE

La **cryptographie hybride** fait appel aux deux grandes familles de systèmes cryptographiques : la cryptographie asymétrique et la cryptographie symétrique

La cryptographie asymétrique est intrinsèquement lente de par les calculs complexes qui y sont associés alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, on doit transmettre les clés de manière sécurisée (sur un canal authentifié)

CRYPTOGRAPHIE HYBRIDE : PRINCIPES



LES PROTOCOLES HYBRIDE

Pretty **G**ood **P**rivacy (ou **PGP**)

- **Histoire** : Publié en 1991 par **Philip Zimmermann**
- **Clé** : clé de 128, 192 , 256, 512, 1024, bits
- **Spécificités** : la sécurité repose sur la rapidité des cryptosystèmes symétriques et la résistance des cryptosystèmes asymétriques