Introduction à la cryptologie

Dr. Yousfi Souheib

Différents modèles de sécurité

Le protocole AAA :

Le contrôle d'accès se fait en 4 étapes :

1. Identification : Qui êtes-vous ?
2. Authentification : Prouvez-le !
3. Autorisation : Avez-vous les droits requis ?
4. Audit : Qu'avez-vous fait ?

Authentification : Prouver l'identité d'un individu :

1. Ce que vous savez (mot de passe, code PIN, etc.)
2. Ce que vous avez (carte magnétique, lecteur de carte, etc.)
3. Ce que vous êtes (empreintes digitales, réseau rétinien, etc.)

Remarque

L'authentification forte résultera de la combinaison de 2 de ces facteurs.

Definition

La cryptologie est la science du secret. Mécanismes qui permettent de rendre inintelligible la lecture d'un message. Elle se divise en deux disciplines :

- La cryptographie qui est l'étude des algorithmes permettant la protection d'informations (numériques). Ces algorithmes sont appelés cryptosystèmes.
- La cryptanalyse qui est l'étude du niveau de sécurité des cryptosystèmes fournis par les cryptographes. C'est l'art de casser ou attaquer les cryptosystèmes.

Période artisanale

La transposition

Une forme de transposition utilise le premier dispositif de cryptographie militaire connu, la scytale spartiate, remontant au Ve siècle avant J.-C. La scytale consiste en un bâton de bois autour duquel est entourée une bande de cuir ou de parchemin

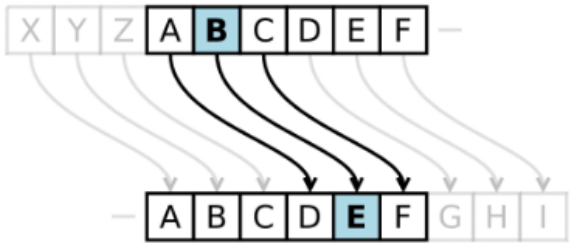
Fonctionnement

Après avoir enroulé la ceinture sur la scytale, le message était écrit en plaçant une lettre sur chaque circonvolution (axe).

Période artisanale

César

Le point de départ de la cryptographie par substitution générale. Son principe est un décalage des lettres de l'alphabet.



Fonctionnement

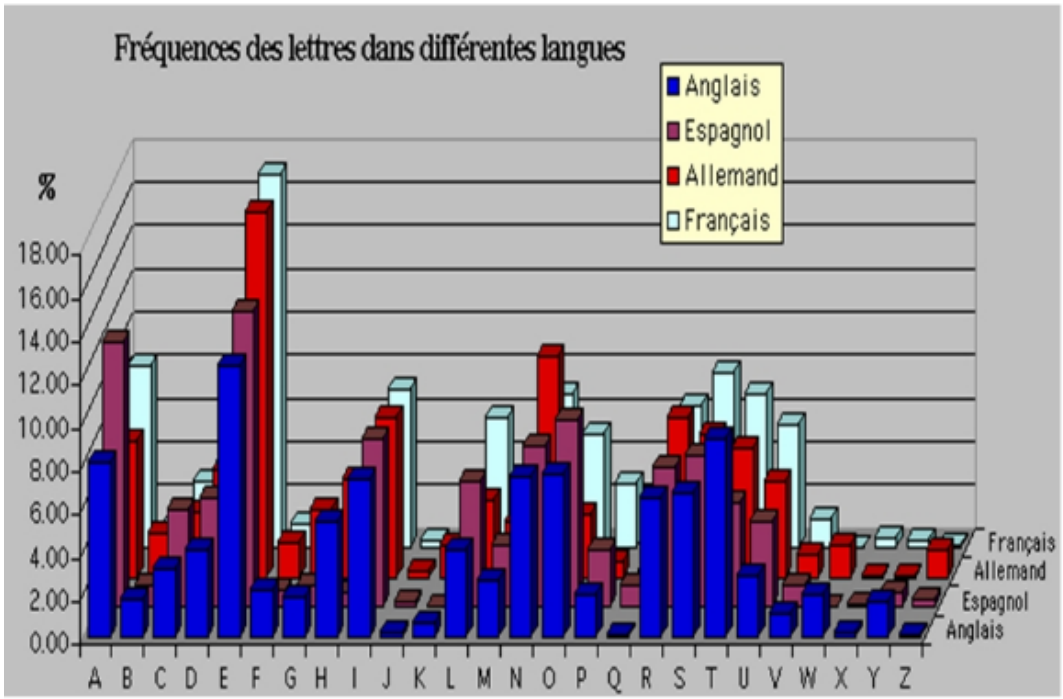
Pour le chiffrement, on aura la formule : $C = e(P) = (P + k) mod 26$
Pour le déchiffrement, il viendra : $P = d(C) = (C - k) mod 26$

Remarque

Si on connaît l'algorithme utilisé (ici César), la cryptanalyse par force brute est très facile. En effet, dans le cas du chiffre de César, seules 25 (!) clef sont possibles.

Analyse de fréquences

Lorsque la langue de départ et le cryptosystème sont connus, on peut exploiter les régularités du langage par le principe d'analyse de la fréquence d'une lettre pour un message chiffré suffisamment long pour avoir des moyennes significatives.



Période artisanale

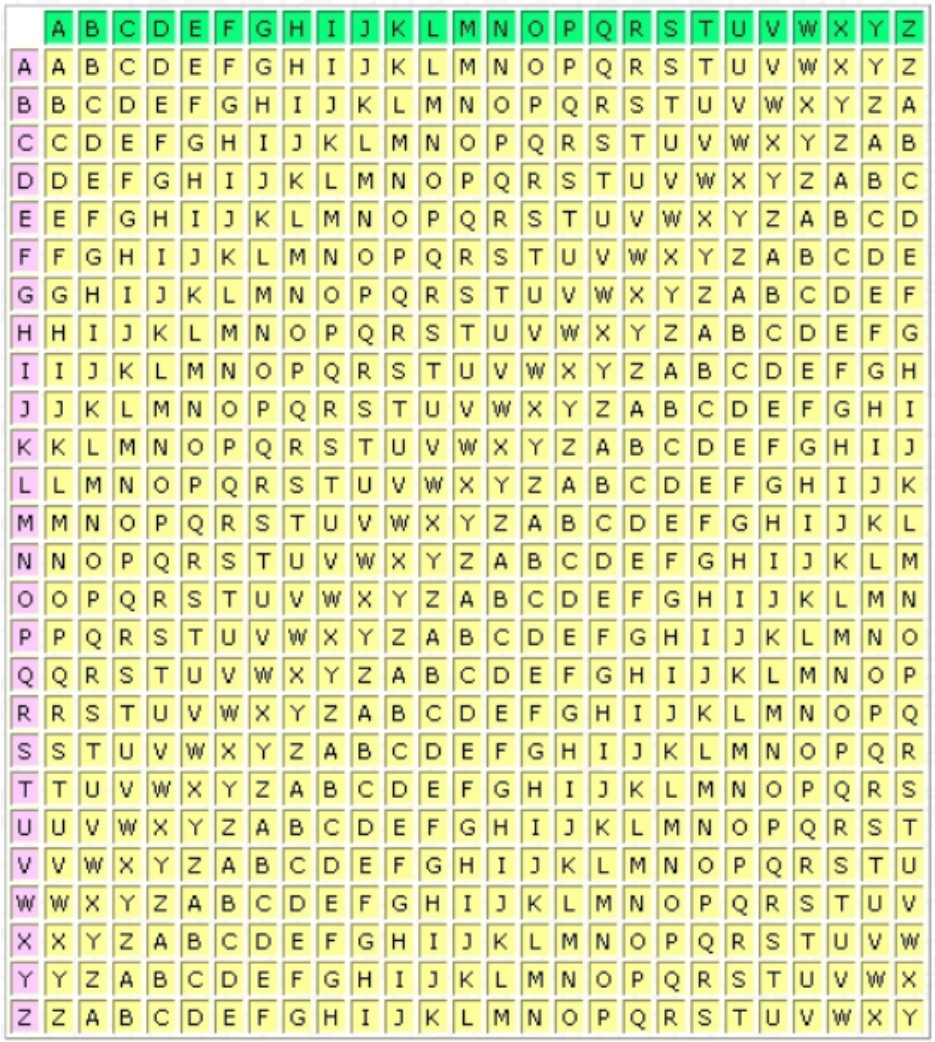
Cryptosystème de Vigenère (1586)

C'est une amélioration décisive du cryptosystème de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On parle du carré de Vigenère.

Avantage

La grande force du cryptosystème de Vigenère est que la même lettre sera chiffrée de différentes manières d'où perte de la fréquence des lettres, ce qui rend inutilisable l'analyse de fréquence classique.

Période artisanale
Cryptosystème de Vigenère



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

Fonctionnement Mathématique

La clef $k = (k_1, k_2, ..., k_s) \in (\mathbb{Z}/26\mathbb{Z})^s$, si on considère un message $m = (a_1, a_2, ..., a_n, ...)$, son chiffré est :
$c = (a_1 + k_1, ..., a_s + k_s, a_{s+1} + k_1, ..., a_{2s} + k_s, a_{2s+1} + k_1, ...)$.
Le déchiffrement s'effectue suivant le même principe, puisque le clair m est obtenu à partir du chiffré $c = (b_1, b_2, ...)$ par soustraction de la clef : $m = (b_1 - k_1, ..., b_s - k_s, b_{s+1} - k_1, ..., b_{2s} - k_s, b_{2s+1} - k_1, ...)$.

Exemple

- Si la clef est « coco » et le message « montreal », la clef est répétée pour être de même longueur que le message 'cococococo'
- 'c' utilisé pour 'm' donne 'o' ; 'o' utilisé pour 'o' donne 'c' ; 'c' utilisé pour 'n' donne 'p' ; et ainsi de suite.

Exemple

Soit la phrase "tours est une superbe ville", on veut la chiffrer avec le mot clef "SUPINFO". On commence par répéter en boucle la clef « au dessus » du texte.

clé	S	U	P	I	N	F	O	S	U	P	I	N	F	O	S	U	P	I	N	F	O	S	U
clair	t	o	u	r	s	e	s	t	u	n	e	s	u	p	e	r	b	e	v	i	l	l	e
chiffré																							

Exemple

Pour déchiffrer un message, le destinataire fera la même chose, mais à l'envers.

Période artisanale

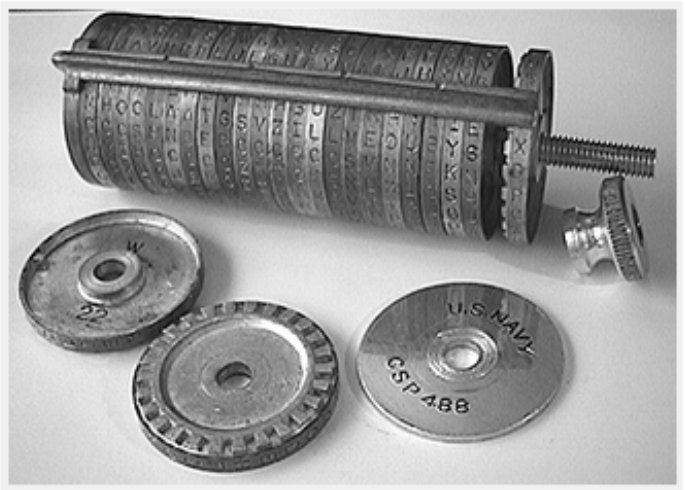
clé	S	U	P	I	N	F	O	S	U	P	I	N	F	O	S	U	P	I	N	F	O	S	U
clair	t	o	u	r	s	e	s	t	u	n	e	s	u	p	e	r	b	e	v	i	l	l	e
chiffré	L	I	J	Z	F	J	G	L	O	C	M	F	Z	D	W	L	Q	M	I	N	Z	D	Y

Exemple

Ce cryptosystème fut longtemps considéré comme incassable.Il l'est d'ailleurs si l'on utilise une clef aussi longue que le texte à chiffrer, et que l'on change de clef à chaque message. Cette méthode est appelée masque jetable et fut élaborée par Vernam en 1917. Son inviolabilité a été démontrée par Shannon en 1949.

Le cylindre de Jefferson (1800)

Le mécanisme est composé d'une série de disques pivotant autour d'un axe, et sur lesquels sont inscrits des alphabets désordonnés. Pour chiffrer un message, on fait tourner les disques de façon à ce qu'il apparaisse sur une ligne du cylindre. Le message chiffré sera alors le contenu de la ligne suivante. Ici, la clef est l'ordre dans lequel les disques sont insérés sur l'axe. Chaque disque étant identifié par un numéro, la clef est donc un nombre.

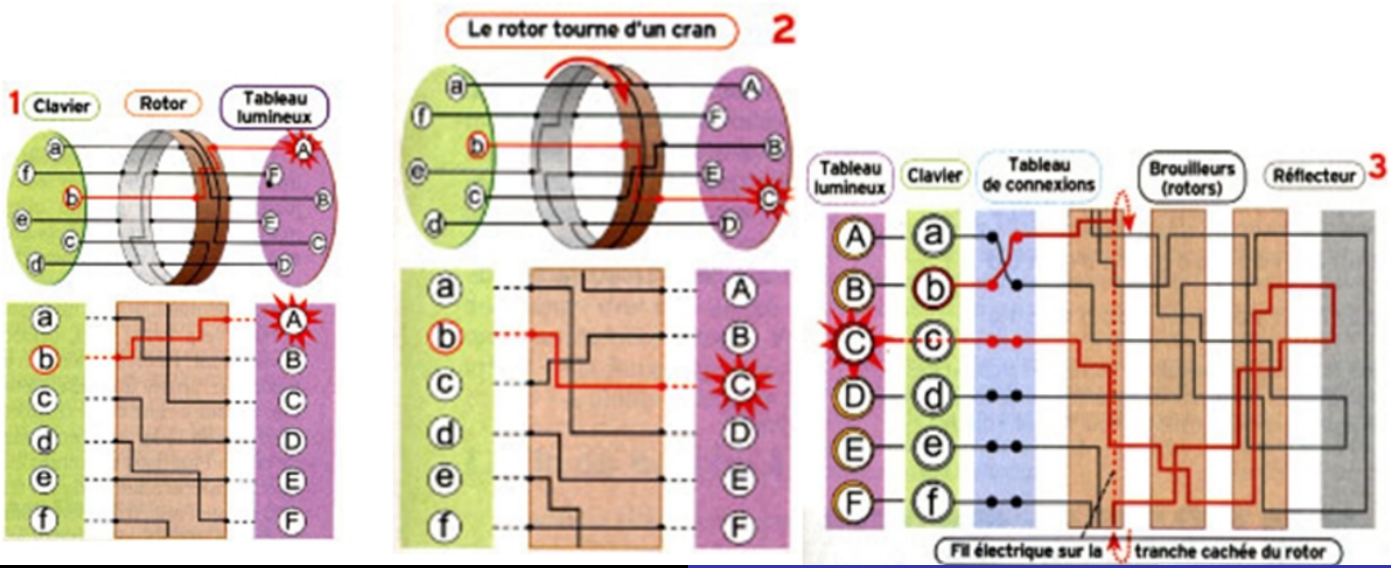


Le cylindre de Jefferson (1800)

Le destinataire du message possède les mêmes cylindres que l'expéditeur. Après qu'il ait ordonné les disques selon la clef, reconstitue sur une ligne le message chiffré. Il n'aura plus ensuite qu'à lire le texte intelligible sur la ligne précédente. C'est la première introduction de la mécanique en cryptographie. Ce chiffre fut vite abandonné, avant d'être réutilisé par l'armée américaine un siècle plus tard.

La machine ENIGMA (1918)

Cette machine ressemble à une machine à écrire. À chaque lettre tapée, une impulsion électrique est émise, parcourt divers circuits dépendants de la position de rotors, et éclaire finalement une ampoule correspondant à la lettre chiffrée. Entre chaque lettre, la position des rotors changent, modifiant ainsi la substitution opérée. La clef de chiffrement de cette machine est la position initiale des rotors. Le nombre de clefs est gigantesque.



La machine ENIGMA

À partir de 1926, les différents secteurs de l'armée allemande vont s'équiper en machines ENIGMA. Environ 100 000 exemplaires seront ainsi utilisés. Les services secrets britanniques créeront pendant la deuxième guerre une cellule chargée de déchiffrer les messages issues de machines ENIGMA. La réussite de cette opération, la plus vaste de l'histoire de la cryptanalyse, permit selon les historiens d'écourter la guerre d'environ deux ans. Le mathématicien Alan Turing (1912-1954) dirigea cette cellule depuis Bletchley Park.

Période artisanale

Résumé

Tous les algorithmes présentés dans les parties précédentes étaient symétriques :

- scytale : on utilise des bâtons de même diamètre pour chiffrer et déchiffrer.
- chiffre de César : le décalage est de k lettres que ça soit pour chiffrer ou déchiffrer.
- chiffre de Vigenère : on utilise le même mot clef pour chiffrer et déchiffrer.
- machine Enigma : la position des rotors est la même lors du chiffrement ou du déchiffrement.

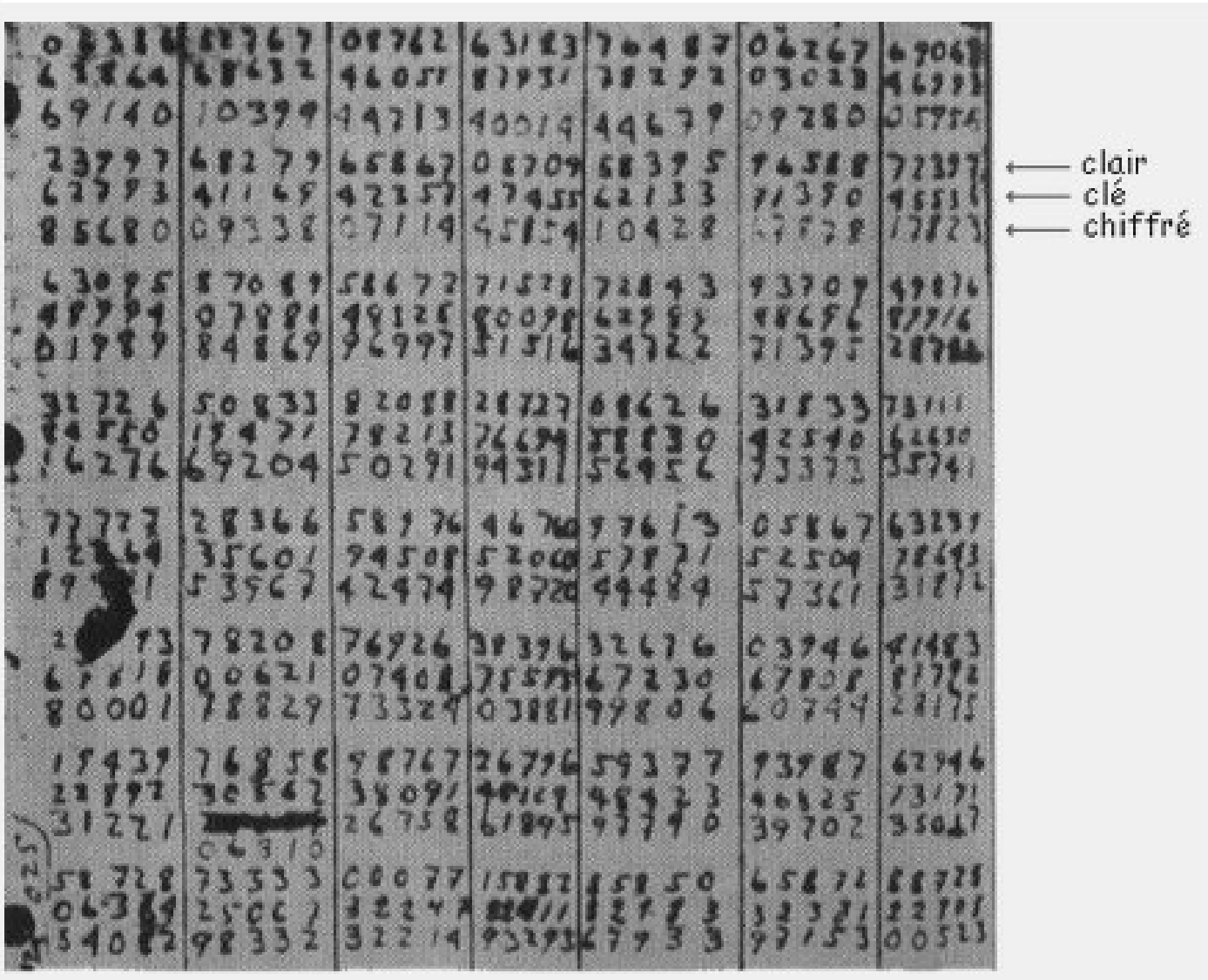
Remarque :

- En 1970, les échanges de clefs dans les grosses banques américaines se font à travers un courtier. Mais la logistique devenait ingérable.

Applications diplomatiques

La cryptologie a depuis toujours été utilisée à des fins diplomatiques et militaires. Citons par exemple le fameux téléphone rouge, ligne reliant le Kremlin et la maison blanche où le procédé utilisé était celui ancestral de Vigenère. Les précautions optimales étaient prises, c'est-à-dire que la clef était à usage unique et aussi longue que le texte à chiffrer. Dans ces conditions le chiffre de Vigenère est démontré incassable. Vu le problème déjà évoqué de l'échange des clefs, l'utilisation de ce téléphone rouge fut cependant limitée à des communications de la plus haute importance. Fidel Castro et Ernesto Guevara utilisèrent ce même procédé dans les années soixante.

Message chiffré échangé par Castro et Guevara



Partie I
Le chiffrement symétrique

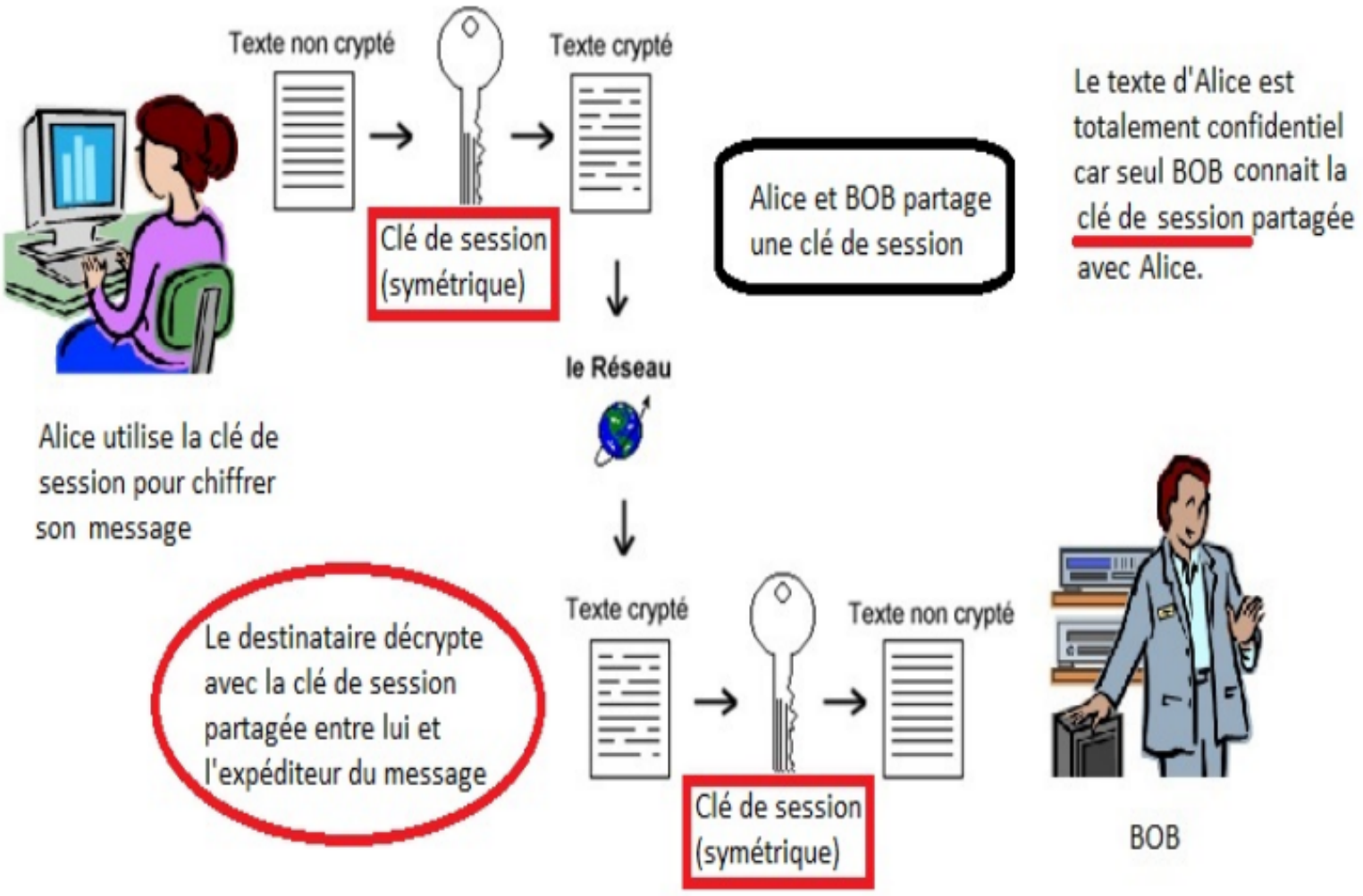
Le chiffrement symétrique

Definition

Les systèmes traditionnels de chiffrement symétrique utilisent une clef partagée entre émetteur et destinataire

- Si la clef unique est découverte, toutes les communications sont compromises.
- Permet de fournir la confidentialité.
- Avantage
  - Rapide
- Inconvénients
  - Il faut autant de clefs que de couples de correspondants (2-> 1 clef,...,n-> n(n-1)/2 clefs)
  - La non-répudiation n'est pas assurée. mon correspondant possédant la même clef que moi peut fabriquer un message en usurpant mon identité
  - Distribution de clefs : dans le cas d'un canal non sécurisé.

Le chiffrement symétrique



Le chiffrement symétrique

- Les systèmes à clef secrète sont insuffisants à deux points de vue :
  - Distribution des clefs : comment avoir en général des communications sûres sans faire confiance à un KDC.
  - Signatures numériques : comment vérifier qu'un message provient bien de l'émetteur prétendu.

Partie II
Le chiffrement asymétrique

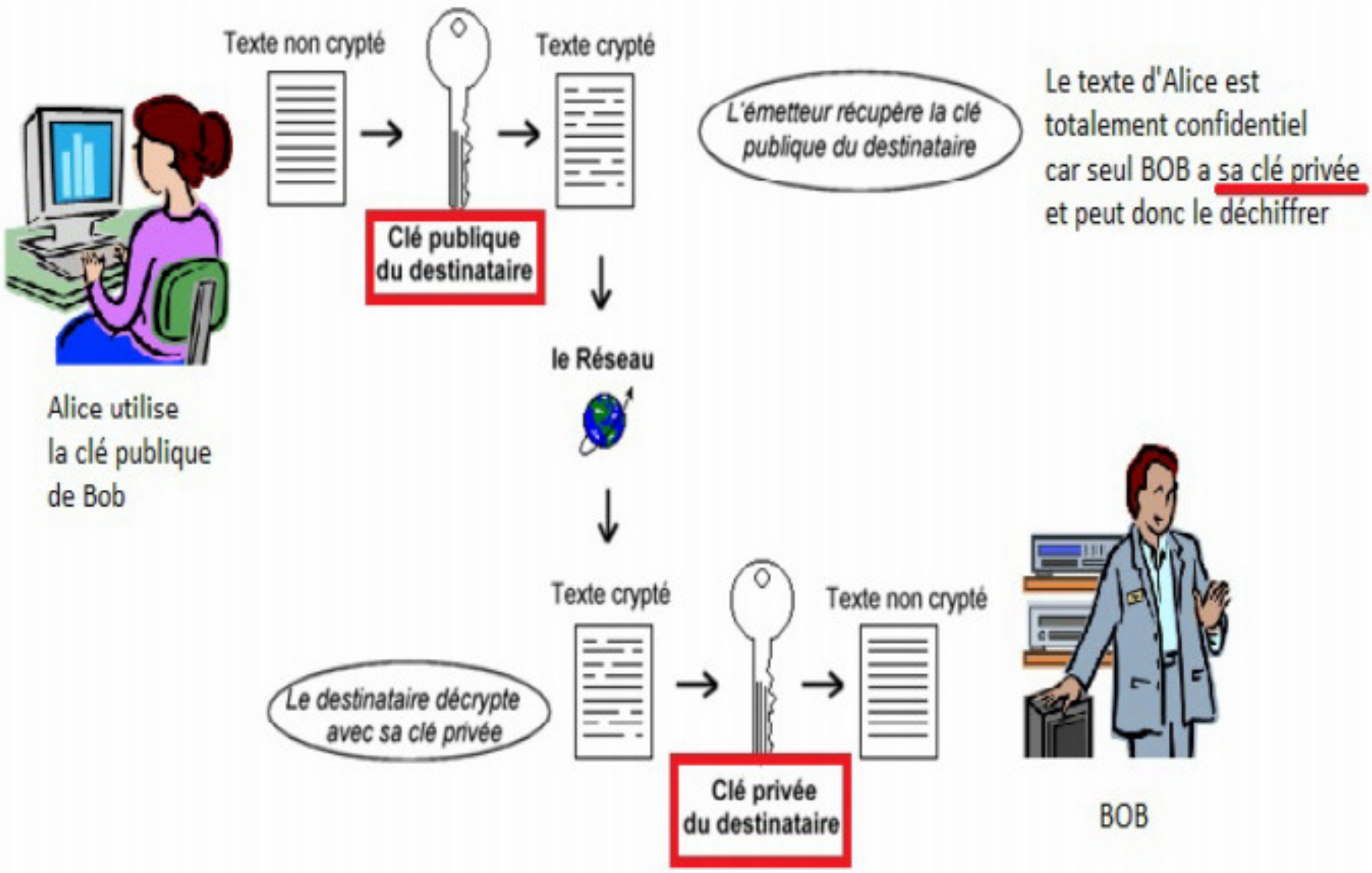
Le chiffrement asymétrique

Definition

Le chiffrement est dit asymétrique car le fonctionnement est différent entre émetteur et destinataire. Il utilise deux clefs : l'une est publique (dans un annuaire, par exemple) l'autre est secrète ou privée (jamais transmise).

- Les méthodes utilisées ne sont plus substitution ou transposition mais des aspects complexes de la théorie des nombres et autres problèmes dits NP-complets.
- La clef publique, que tout le monde peut connaître, sert à chiffrer les messages et vérifier les signatures.
- La clef privée, connue de son seul propriétaire, est utilisée pour déchiffrer les messages chiffrés avec la clef publique correspondante et créer des signatures.
- La clef utilisée pour chiffrer les messages ou vérifier les signatures ne peut pas déchiffrer les messages ni créer des signatures.

Le chiffrement asymétrique



Le chiffrement asymétrique

- Trois catégories :
  - Chiffrement/Déchiffrement : L'émetteur chiffre son message en utilisant le clef publique du récepteur : Confidentialité.
  - Signature numérique : L'émetteur signe son propre message en utilisant sa clef privée : Authentification.
  - Échange de clefs : Deux partenaires peuvent s'échanger des clefs de session.
- Il y a une énorme différence de complexité entre le chiffrement simple et le déchiffrement difficile.
- Le problème du déchiffrement est connu, il est difficile à résoudre à cause du coût des calculs.
- Les méthodes utilisées travaillent sur des grands nombres (plusieurs centaines de chiffres).

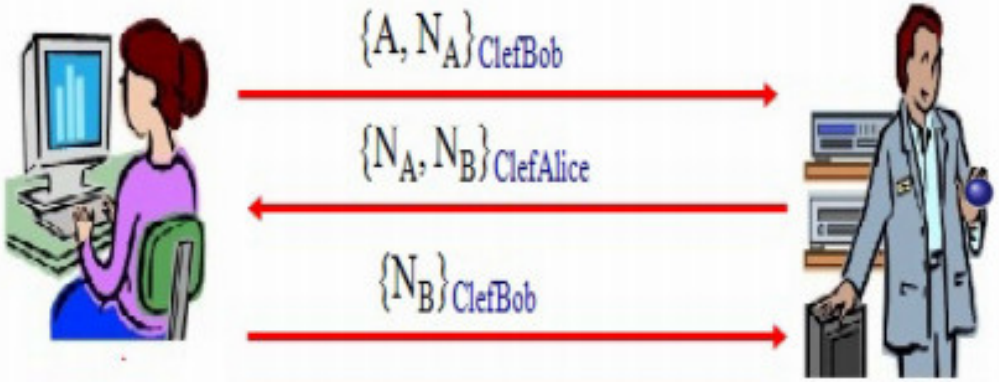
Le chiffrement asymétrique

- En 1976, Whitfield Diffie et Martin Hellman publient "new directions in cryptography", un article dans lequel ils décrivent un protocole afin de s'échanger secrètement une clef de chiffrement. C'est une avancée majeure car la communication des clefs a toujours été un problème fondamental. Dans cet article ils introduisent également le concept de clef publique.
- En 1977, Ronald Rivest, Adi Shamir et Leonard Max Adleman mettent au point le R.S.A., qui deviendra vite l'algorithme le plus sécurisé au monde.
- En 1991 Philip Zimmermann développe le logiciel P.G.P., Pretty Good Privacy. Il s'agit d'un freeware destiné principalement aux particuliers afin qu'ils chiffrent leur emails.
- Les dernières recherches en cryptologie se portent sur ce que l'on appelle la cryptographie quantique. L'échange de clefs se ferait par un canal quantique, où une information interceptée et lue par un tiers y introduit des erreurs. On peut donc détecter si une clef a été interceptée ou pas.

Le chiffrement asymétrique

Le protocole de Needham-Schroeder à clef publique (1978) :

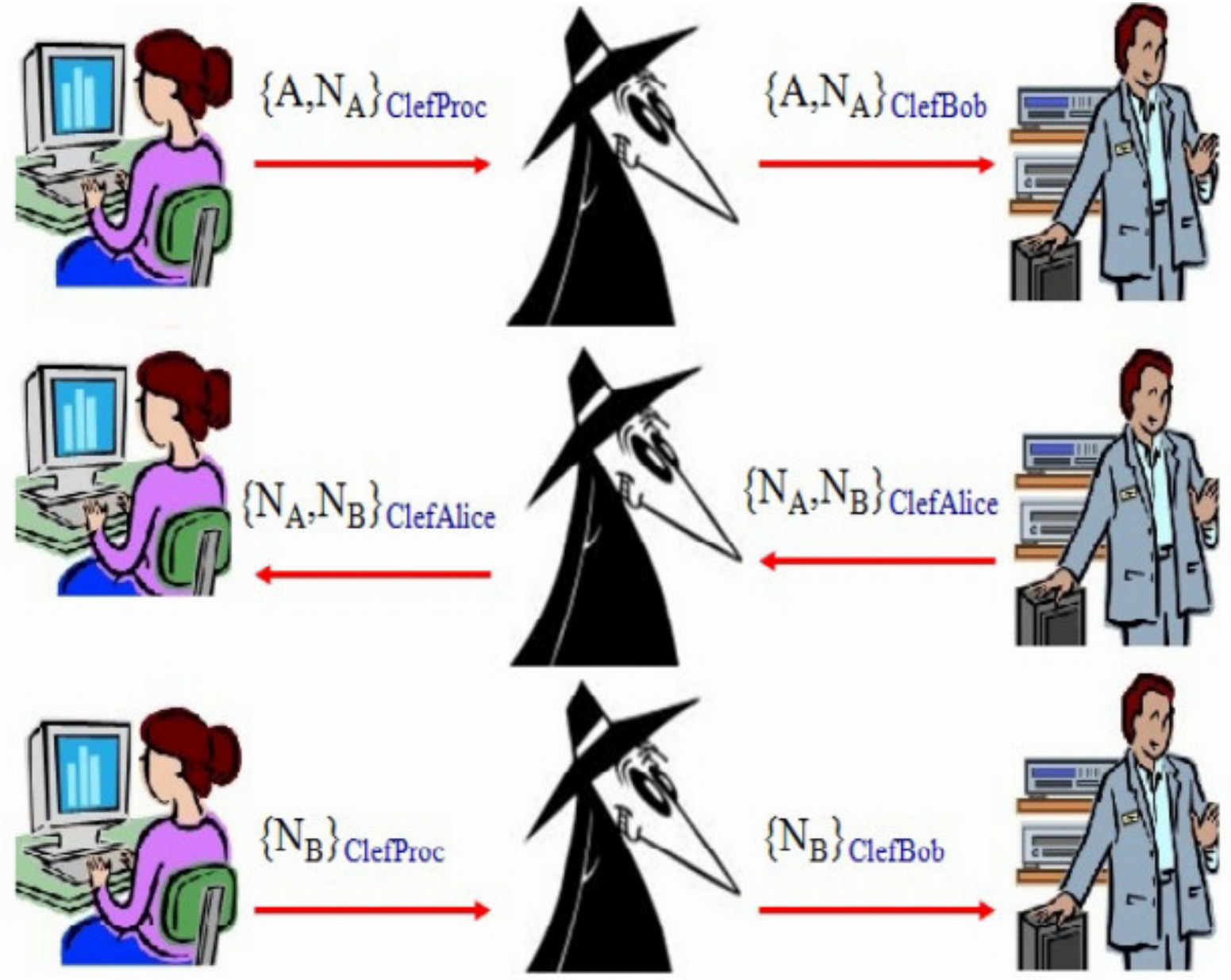
- Protocole d'authentification (prouvé l'un et l'autre leurs identités respectives dans un réseau non sûr).
- Longtemps utilisé par les CB.
- Il a fallu 17 ans pour imaginer et ce rendre compte que l'étude des protocoles cryptographiques est un vrai challenge. Gaven Low a exhibé l'attaque MIM.



- Est-ce que N_B est secret entre Alice et Bob ?

Lorsque Bob reçoit le message de Alice, est-ce que le message provient réellement d'Alice ?

Le chiffrement asymétrique



Comparaison Chiff. Symétrique VS Chiff. Asymétrique

- La première différence notable entre les deux systèmes est que dans l'un on a la contrainte importante de devoir procéder à un échange de clef, et que dans l'autre non.
- Les algorithmes asymétriques seront également plus lents et nécessiteront des ressources matérielles bien plus puissantes, qu'un particulier ne pourra par exemple pas avoir. En pratique, ils seront donc essentiellement destinés à des organisations gouvernementales ou à de grosses entreprises.

Cryptographie symétrique	Cryptographie asymétrique
Problème majeur d'échange des clés	Pas de clés à échanger
Relative simplicité d'implémentation	Relative complexité d'implémentation
Pas trop coûteux en ressources matérielles	Très coûteux en ressources matérielles
Relativement rapide	Très lent

Comparaison Chiff. Symétrique VS Chiff. Asymétrique

Nb personnes	Nb clés secrètes	Nb clés publiques ET privées
2	1	4
3	3	6
4	6	8
5	10	10
10	45	20
15	105	30
20	190	40
50	1225	100
100	4950	200
500	124 750	1 000
1 000	499 500	2 000
10 000	49 995 000	20 000
n	n(n-1)/2	2n

SYMMETRIC

ASYMMETRIC

Sécurité des cartes bancaires I

La sécurisation des transactions monétaires déclenchées par l'usage d'une carte bancaire est triple :

1. Utilisation d'un code confidentiel de 4 chiffres à taper par le possesseur de la carte.
2. Authentification hors ligne (signature R.S.A.) : chaque carte a une V.S. (Valeur de Signature) nombre calculé lors de sa fabrication à partir des informations personnelles du propriétaire. Ce calcul s'effectue à l'aide d'un algorithme R.S.A. et de la clef secrète du groupement des cartes bancaires. Déchiffré à l'aide de la clef publique du groupement, il est alors comparé aux informations personnelles du propriétaire. Normalement seul le groupement a pu calculer cette V.S. car le calcul nécessite la connaissance de leur clef secrète. Ici hors ligne signifie sans appel à un centre de paiement.

Sécurité des cartes bancaires II

La troisième étape de la sécurisation des transactions monétaires déclenchées par l'usage d'une carte bancaire est :

3. Authentification en ligne (par D.E.S.) : le centre de paiement envoie à la carte une valeur aléatoire. Celle-ci chiffre cette valeur à l'aide d'une clef secrète contenue dans sa puce et de l'algorithme D.E.S. Le centre de paiement fait ce même calcul et compare les deux valeurs. A noter que cela nécessite que le centre de paiement connaisse les clefs secrètes de toutes les cartes bancaires. Ici en ligne signifie avec appel à un centre de paiement.