

La cryptographie et ses secrets

Mathilde Herblot

herblot@math.univ-paris-diderot.fr

Université Paris Diderot

1^{er} mars 2017

Cartes à puce



- Confidentialité des données contenues sur les cartes
- Lecture sans contact
- Vérification de la validité de l'abonnement

Paiements en ligne, e-commerce

Récapitulatif et paiement de votre commande

https://secure.voyages-sncf.com/reservation/paiement

Accueil > Votre billet de train > Votre réservation pour PARIS - BOURG ST MAURICE

ACCUEIL | TRAIN | VOL, VOITURE | HÔTEL | SKI, SÉJOUR | BONS PLANS | VOYAZINE

Résultats | Panier | Coordonnées | Confirmation

RÉCAPITULATIF ET PAIEMENT DE VOTRE COMMANDE

PARIS ↔ BOURG ST MAURICE	1 Passager	138.00 €
Aller 08h38 PARIS GARE DE LYON 13h12 BOURG ST MAURICE 1 ^{er} Passager (26 à 59 ans) PLEIN TARIF LOISIR : Service d'échange et de remboursement gratuit jusqu'à la veille du départ, avec retenue de 10€ le jour du départ, non échangeable et non remboursable après départ.	TGV 0642 2 ^e classe	Samedi 26 Mars Voiture 7 - Place 87 Balle haute - Couloir - Duo côté à côté
Retour 09h15 BOURG ST MAURICE 14h23 PARIS GARE DE LYON 1 ^{er} Passager (26 à 59 ans) TOUJOURS PREMIER : OFFRE SPÉCIALE DE MARS : Billet non échangeable, non remboursable.	TGV 0642 2 ^e classe	Samedi 02 Avril Voiture 7 - Place 21 Balle basse - Couloir - Duo côté à côté

MODIFIEZ LE VOYAGE

VOS INFORMATIONS SAISIES À VÉRIFIER

Votre billet :
Vous avez choisi : **le retrait en Borne Libre Service**
Vous devrez retirer votre billet en Borne Libre Service avec la carte utilisée pour le paiement en ligne.
Veuillez noter que la carte American Express, une carte étrangère ou "sans puces" ne peut pas être utilisée pour un retrait en borne Libre Service.

Vos coordonnées

Terminé

INFORMATION LÉA
Pour vous garantir une transaction entièrement sécurisée, le site utilise le procédé de cryptage SSL et le système de sécurisation 3DS pour protéger toutes les données liées aux moyens de paiement.

Clé de voiture



TRES SECRET DEFENSE

Petit historique de la cryptographie

Plus vieil exemple connu : au XVI^e siècle avant J.-C., en Mésopotamie (Irak actuel), une tablette d'argile sur laquelle est gravée la recette secrète d'un potier.



Scytale



Chiffre de César

Méthode utilisée par Jules César dans ses correspondances secrètes.

Décalage des lettres de l'alphabet.

Par exemple, décalage de 4 : on remplace A par E, B par F, C par G...

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
				↓	↓																				
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

Décalage de E.

Combien de chiffrements différents possibles ?

Chiffre de César

Méthode utilisée par Jules César dans ses correspondances secrètes.

Décalage des lettres de l'alphabet.

Par exemple, décalage de 4 : on remplace A par E, B par F, C par G...

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
				↓	↓																				
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

Décalage de E.

Combien de chiffrements différents possibles ? 25

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

Remarque : il suffit de savoir comment une lettre de l'alphabet est transformée pour connaître les transformations de toutes les lettres.

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

Remarque : il suffit de savoir comment une lettre de l'alphabet est transformée pour connaître les transformations de toutes les lettres.

Nombre de S : 5

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

C'est le décalage de O. Décryptons :

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

C'est le décalage de O. Décryptons :

P

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

C'est le décalage de O. Décryptons :

P R

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

C'est le décalage de O. Décryptons :

P R E

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

C'est le décalage de O. Décryptons :

P R E M

Chiffre de César, à l'attaque !

Texte chiffré, décalage inconnu :

D F S A W S F A O F G R S I L A W Z Z S R W L G S D H

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

C'est le décalage de O. Décryptons :

P R E M I E R M A R S D E U X M I L L E D I X S E P T

Permutation

Au lieu de décaler l'alphabet, on peut mélanger complètement les lettres.

Par exemple :

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

On dit qu'on fait une *permutation* des lettres de l'alphabet.

Combien de tels chiffrements ?

Permutation

Au lieu de décaler l'alphabet, on peut mélanger complètement les lettres.

Par exemple :

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

↓ ↓

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

On dit qu'on fait une *permutation* des lettres de l'alphabet.

Combien de tels chiffrements ?

$$26 \times 25 \times 24 \times \cdots \times 2 \times 1 \simeq 4 \cdot 10^{26} = 400\,000\,000\,000\,000\,000\,000\,000\,000$$

Permutation

Au lieu de décaler l'alphabet, on peut mélanger complètement les lettres.

Par exemple :

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

On dit qu'on fait une *permutation* des lettres de l'alphabet.

Combien de tels chiffrements ?

$$26 \times 25 \times 24 \times \dots \times 2 \times 1 \simeq 4 \cdot 10^{26} = 400\,000\,000\,000\,000\,000\,000\,000\,000$$

Mais on sait comment l'attaquer !

Chiffre de Vigenère



Blaise de Vigenère
(1523-1596)

Clé : un « mot », par exemple : MATHS.
On la répète suffisamment de fois pour recouvrir le message clair.

C E C I E S T T R E S S E C R E T
M A T H S M A T H S M A T H S M A

Chiffre de Vigenère



Blaise de Vigenère
(1523-1596)

Clé : un « mot », par exemple : MATHS.
On la répète suffisamment de fois pour recouvrir le message clair.

```
C E C I E S T T R E S S E C R E T  
M A T H S M A T H S M A T H S M A  
O E V P W E T M Y W E S X J J Q T
```

Chiffre de Vigenère

Clé : un « mot », par exemple : MATHS.
On la répète suffisamment de fois pour recouvrir le message clair.

C E C I E S T T R E S S E C R E T
M A T H S M A T H S M A T H S M A
O E V P W E T M Y W E S X J J Q T

Avantages :

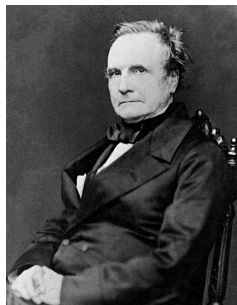
- une même lettre n'est pas toujours chiffrée de la même façon.
- la cryptanalyse fréquentielle ne marche pas.

Considéré comme sûr pendant 300 ans.



Blaise de Vigenère
(1523-1596)

Charles Babbage

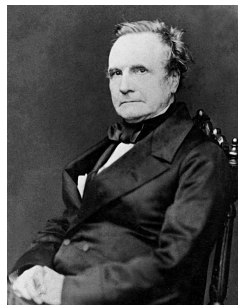


Charles Babbage
(1791-1871)

Idée : On cherche des séquences de lettres qui se répètent plusieurs fois dans le chiffré :

- hasard ?
- même (bout de) mot chiffré avec le même morceau de clé ?

Charles Babbage



Charles Babbage
(1791-1871)

Idée : On cherche des séquences de lettres qui se répètent plusieurs fois dans le chiffré :

- hasard ?
- même (bout de) mot chiffré avec le même morceau de clé ?

Dans le deuxième cas, cela signifie que la distance qui sépare ces deux *occurrences* du même (bout de) mot est un multiple de la longueur de la clé !

Exemple

KETVI YGPNU FNZIE EWPUY PFNUF NJVFD JSEPE JHPSR KYSDF UOAXD
ERVIG PUESF LOKOO SBNII OAUVR KPMEM JGTSS AODEK WUCPN MKYOF
SVIZI YOUJQ AIEEM JCGXW OVTLK XPUDI EFIUL FQAXJ VMEJS VESAJ
UTUYU EMBTN IPRJF MUHFR OFDKP FDVDA ZMPNF TTXEE IDBLK QFNUT
TATJD FGOXX IEVSE AWFMF OTKRB NHMEZ ISRFM EJYDA UJOTR FPSPD
AMUAV DUTIG FFUDG YDUOF SUVUE TJNUR JLTFN YYJVS BIZHF GSBVK
WEAOH EXWQO VSLKW DLBTS KWTUQ FROIV RFT

Exemple

KETVI YGP **NU FN** ZIE EWPUY PF **NUF N** JVFD JSEPE JHPSR KYSDF
UOAXD ERVIG PUESF LOKOO SBNII OAUVR KPMEM JGTSS AODEK WUCPN
MKYOF SVIZI YOUJQ AIEEM JCGXW OVTLK XPUDI EFIUL FQAXJ VMEJS
VESAJ UTUYU EMBTN IPRJF MUHFR OFDKP FDVDA ZMPNF TTXEE IDBLK
QFNUT TATJD FGOXX IEVSE AWFMF OTKRB NHMEZ ISRFM EJYDA UJOTR
FPSPD AMUAV DUTIG FFUDG YDUOF SUVUE TJNUR JLTFN YYJVS BIZHF
GSBVK WEAOH EXWQO VSLKW DLBTS KWTUQ FROIV RFT

Séquence	Distance	Décomposition
NUFN	14	2×7

Exemple

KETVI YGP **NU FN Z** IE E WPUY PF **NUF N** JVFD JSEPE JHPSR KYSDF
UOAXD ERVIG PUESF LOKOO SBNII OAUVR KPM **EM J** GTSS AODEK
WUCPN MKYOF SVIZI YOUJQ A IE **EM J** CGXW OVTLK XPUDI EFIUL
FQAXJ V **MEJ** S VESAJ UTUYU EMBTN IPRJF MUH **FR O** FDKP FDVDA
ZMPNF TTXEE IDBLK QFNUT TATJD FGOXX IEVSE AWFMF OTKRB NHMEZ
ISRF **M EJ** YDA UJOTR FPSPD AMUAV DUTIG FFUDG YDUOF SUVUE
TJNUR JLTFN YYJVS BIZHF GSBVK WEAOH EXWQO VSLKW DLBTS KWTUQ
FRO IV RFT

Séquence	Distance	Décomposition
NUFN	14	2×7
EMJ	35	5×7
FRO	157	157
IEE	98	2×7^2
MEJ	93	3×31

Exemple

Séquence	Distance	Décomposition
NUFN	14	2×7
EMJ	35	5×7
FRO	157	157
IEE	98	2×7^2
MEJ	93	3×31

clé de longueur 7 ?

- 1 On garde une lettre sur 7 en partant de la première :
KPEFFJSDUOOMSUOYEWPUVSUPFFPEFJIFBSDFUGDUJJFEQDTV
Lettre la plus fréquente : F
- 2 On garde une lettre sur 7 en partant de la deuxième :
ENENDHDEEOAEACFOEOULMAERRDNINDEMNRAPAFUELVGAOLUR
Lettre la plus fréquente : E
- 3 TUWUJPFRRSSUMOPSUMVDFEJMJOVFDUFVVFHFUSVFOTTSSOVBQF
Lettres les plus fréquentes : F, S, U
- 4 VFPFSSUVFBVJDNVJJTIQJUBFFDTBTGSOMMJPDUFJFBBHSTFT
Lettre la plus fréquente : F
- 5 INUNEROILNRGEMIQCLEASTTMDATLTOETEEODUDSNNIVELSR
Lettres les plus fréquentes : E, N
- 6 ZYZJPKAGOIKTKKZAGKFXVUNUKZXXKAXAKZJTATGUUYZKXKKO
Lettre la plus fréquente : K
- 7 GIPVEYXPKIPSWYIIXXIJEYIHPMEQTXWRIYRMIYVRYHWWWI
Lettre la plus fréquente : I

- ① On garde une lettre sur 7 en partant de la première :
 KPEFFJSDUOOMSUOYEWPUVSUPFFPEFJIFBSDFUGDUJJFEQDTV
 Lettre la plus fréquente : F → Première lettre de la clé : B
- ② On garde une lettre sur 7 en partant de la deuxième :
 ENENDHDEEOAEACFOEOULMAERRDNINDEMNRAPAFUELVGAOLUR
 Lettre la plus fréquente : E → Deuxième lettre de la clé : A
- ③ TUWUJPFRRSSUMOPSUMVDFEJMJOVFDUFVHFHUSVFOTTSSOVQBQF
 Lettres les plus fréquentes : F, S, U → 3^e lettre de la clé : B ? O? Q?
- ④ VFPFSSUVFBVJDNVJJTIQJUBFFDTBTGSOMMJPDUFJFBBHSTFT
 Lettre la plus fréquente : F → Quatrième lettre de la clé : B
- ⑤ INUNEROILNRGEMIQCLEASTTMDATLTOETEEODUDSNNIVELSR
 Lettres les plus fréquentes : E, N → 5^e lettre de la clé : A ? J?
- ⑥ ZYZJPKAGOIKTKKZAGKFXVUNUKZXXKAXAKZJTATGUUYZKXKKO
 Lettre la plus fréquente : K → Septième lettre de la clé : G
- ⑦ GIPVEYXPKIPSWYIIXXIJEYIHPMEQTXWRIYRMIYVRYHWWWI
 Lettre la plus fréquente : I → Septième lettre de la clé : E

Lettres les plus fréquentes : F, S, U → 3^e lettre de la clé : B ? O? Q?

Si la lettre est O, le décalage est le suivant :

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
				↓				↓										↓							
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

Peu probable !

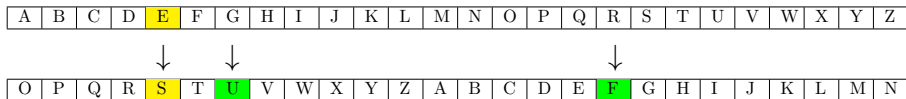
Si la lettre est Q, le décalage est le suivant :

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
				↓																					
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

Peu probable !

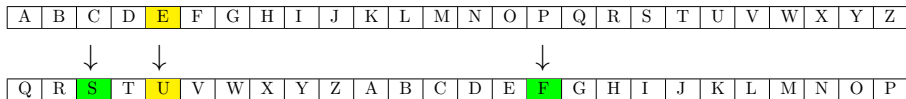
Lettres les plus fréquentes : F, S, U → 3^e lettre de la clé : B ? O? Q?

Si la lettre est O, le décalage est le suivant :



Peu probable !

Si la lettre est Q, le décalage est le suivant :



Peu probable !

La lettre de la clé est sûrement B

Lettres les plus fréquentes : F, S, U → 3^e lettre de la clé : B ? O? Q?

Si la lettre est O, le décalage est le suivant :

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
				↓				↓										↓							
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

Peu probable !

Si la lettre est Q, le décalage est le suivant :

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
				↓																					
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

Peu probable !

La lettre de la clé est sûrement B

De même, pour la 5^e lettre de la clé, la plus probable est le A.

La clé est donc BABBAGE et le message clair :

Je suis contente de vous l'entendre dire. J'ai horreur de tout ce qui altère l'ignorance naturelle. L'ignorance est comme un fruit exotique délicat, vous le touchez et le parfum disparaît. Toute la théorie moderne de l'éducation est radicalement stupide. Fort heureusement, en Angleterre, l'éducation ne produit aucun effet d'aucune sorte. Sinon il s'ensuivrait de graves dangers pour les classes supérieures.

Oscar Wilde, *L'Importance d'être Constant*

Enigma, seconde guerre mondiale



Substitution polyalphabétique,
système asynchrone.

Grands principes de la cryptographie moderne

- La sécurité ne doit pas reposer sur le secret de la méthode, mais sur le secret de la clé utilisée.
- Il n'y a pas de relation simple entre le clair et le chiffré.
- La modification d'une lettre du clair doit modifier l'ensemble du chiffré.

J'ai tout compris !

Je veux me connecter pour la première fois à Facebook. Je prends rendez-vous avec Mark Zuckerberg, pour que nous échangions une clé secrète.

J'ai tout compris !

Je veux me connecter pour la première fois à Facebook. Je prends rendez-vous avec Mark Zuckerberg, pour que nous échangions une clé secrète.

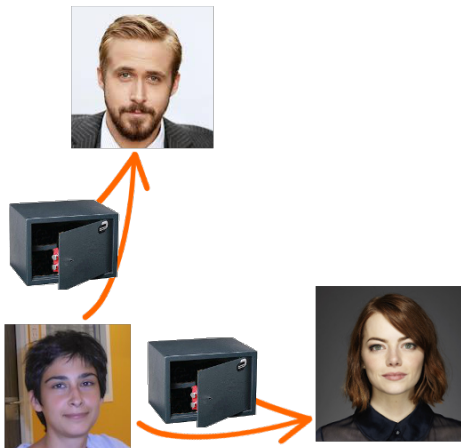
...

Est-il possible d'échanger des messages chiffrés sans échanger de clé ?

La cryptographie à clé publique

Ryan Gosling et Emma Stone veulent m'envoyer des messages secrets.

- Ils me demandent de leur envoyer un coffre-fort dont je suis la seule à avoir la clé.



La cryptographie à clé publique

Ryan Gosling et Emma Stone veulent m'envoyer des messages secrets.

- Ils me demandent de leur envoyer un coffre-fort dont je suis la seule à avoir la clé.
- Ils mettent leur message dedans et ferment le coffre.

La cryptographie à clé publique

Ryan Gosling et Emma Stone veulent m'envoyer des messages secrets.

- Ils me demandent de leur envoyer un coffre-fort dont je suis la seule à avoir la clé.
- Ils mettent leur message dedans et ferment le coffre.
- Ils me renvoient les coffres.

La cryptographie à clé publique

Ryan Gosling et Emma Stone veulent m'envoyer des messages secrets.

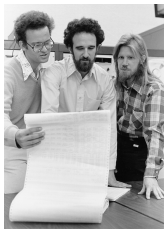
- Ils me demandent de leur envoyer un coffre-fort dont je suis la seule à avoir la clé.
- Ils mettent leur message dedans et ferment le coffre.
- Ils me renvoient les coffres.
- J'ouvre les coffres avec ma clé (secrète).



Principe mathématique de la cryptographie à clé publique

Le « coffre » est une fonction, qui transforme le message clair en le message chiffré. Elle doit être :

- facile à calculer (chiffrer le message, fermer le coffre)
- difficile à inverser (dur de retrouver le message pour un intrus, coffre dur à percer)
- facile à inverser pour une personne qui a une information supplémentaire (une clé, secrète).



Cette idée a été formulée par Merkle, Hellman, Diffie en 1975

Merci pour votre attention !