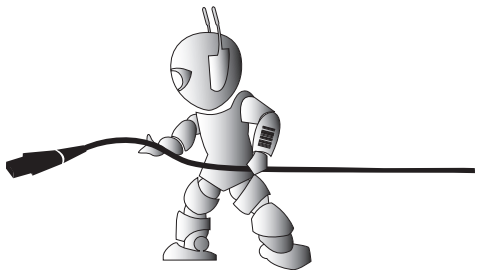
Chiffrement et authentification

Cryptographie moderne

Tuyêt Trâm DANG NGOC
<dntt@u-cergy.fr>

Université de Cergy-Pontoise

2012–2013



DÉPARTEMENT
Sciences Informatiques

Plan

DÉPARTEMENT
Sciences Informatiques

Cryptographie

- Confidentialité : s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé
- Intégrité : l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle
- Signature :
  - Authentification : procédure qui consiste à vérifier l'identité d'une entité (personne, ordinateur...)
  - Non-répudiation : assure que le message ne peut être remis en cause par l'un des partis.
  - Horodatage : certifier des heures et des dates de signature électronique et renforcer la fonction de non répudiation
- Certificat : carte d'identité numérique dont l'objet est d'identifier une entité physique ou non-physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique.
- Certification : processus d'attribution de certificat par un tiers de confiance

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Codage ASCII (American Standard Code for Information Interchange)

L'ASCII définit 128 caractères numérotés de 0 à 127 et codés en binaire de 0000000 à 1111111.
Sept bits suffisent donc pour représenter un caractère codé en ASCII.
Toutefois, les ordinateurs travaillant presque tous sur huit bits (un octet) depuis les années 1970, chaque caractère d'un texte en ASCII est stocké dans un octet dont le 8e bit est 0.

Code	Signif.
0	NUL
1	SOH
2	STX
3	ETX
4	EOT
5	ENQ
6	ACK
7	BEL
8	BS
9	HT
10	LF
11	VT
12	FF
13	CR
14	SO
15	SI
16	DLE
17	DC1
18	DC2
19	DC3
20	DC4
21	NAK
22	SYN
23	ETB
24	CAN
25	EM
26	SUB
27	ESC
28	FS
29	GS
30	RS

Code	Signification
31	US
32	SP
33	!
34	"
35	#
36	$
37	%
38	&
39	’
40	(
41	)
42	*
43	+
44	,
45	-
46	.
47	/
48	0
49	1
50	2
51	3
52	4
53	5
54	6
55	7
56	8
57	9
58	:
59	;
60	<

Code	Signif.
61	=
62	>
63	?
64	@
65	A
66	B
67	C
68	D
69	E
70	F
71	G
72	H
73	I
74	J
75	K
76	L
77	M
78	N
79	O
80	P
81	Q
82	R
83	S
84	T
85	U
86	V
87	W
88	X
89	Y
90	Z

Code	Signif.
91	[
92	\
93	]
94	^
95	_
96	‘
97	a
98	b
99	c
100	d
101	e
102	f
103	g
104	h
105	i
106	j
107	k
108	l
109	m
110	n
111	o
112	p
113	q
114	r
115	s
116	t
117	u
118	v
119	w
120	x

Code	Signif.
121	y
122	z
123	{
124	|
125	}
126	~
127	DEL

DÉPARTEMENT
Sciences Informatiques

Code dec.	Code bin.	Signif.
65	01000001	A
66	01000010	B
67	01000011	C
68	01000100	D
69	01000101	E
70	01000110	F
71	01000111	G
72	01001000	H
73	01001001	I
74	01001010	J
75	01001011	K
76	01001100	L
77	01001101	M
78	01001110	N
79	01001111	O
80	01010000	P
81	01010001	Q
82	01010010	R
83	01010011	S
84	01010100	T
85	01010101	U
86	01010110	V
87	01010111	W
88	01011000	X
89	01011001	Y
90	01011010	Z

C	R	Y	P	T	O
01000011	01010010	01011001	01010000	01010100	01001111

DÉPARTEMENT Sciences Informatiques

Chiffrement par transposition

Exemple : permutation de bit deux à deux

C	R	Y	P	T	O
1000011	1010010	1011001	1010000	1010100	1001111
0100101	1100001	0111001	1100000	0101011	0001111
%	a	9	‘	+	^O

- Transposition au sein d'une lettre ou avec les bits d'autres lettres.
- Inversible

DÉPARTEMENT
Sciences Informatiques

Chiffrement par substitution avec mot clef

Exemple : avec l'opérateur XOR

Opérateur XOR

Si les deux bits sont identiques, alors 0, sinon 1.

$0 \oplus 0 = 0\,;\ 0 \oplus 1 = 1\,;\ 1 \oplus 0 = 1\,;\ 1 \oplus 1 = 0$

```
Message en clair   :    C       R       Y       P       T       O
Message en ASCII   : 1000011 1010010 1011001 1010000 1010100 1001111
Clef : OTARIE      : 1001111 1010100 1000001 1010010 1001001 1000101
                     -----------------------------------------------
Texte chiffré (XOR): 0001100 0000110 0011000 0000010 0011101 0001010
```

- Inversible avec la clef

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Cryptographie symétrique

Cryptographie symétrique

Une même clef permettre de chiffrer et de déchiffrer un message et sur laquelle peut reposer toute la sécurité de la communication.

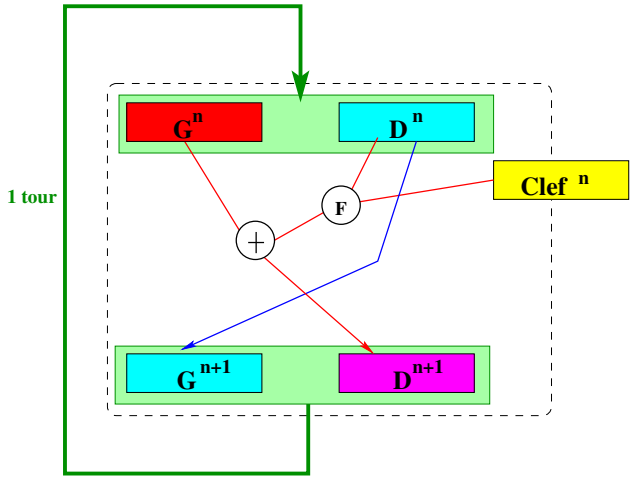
- Chiffrement par bloc (block cipher) : découpage des données en blocs de taille généralement fixe. Les blocs sont ensuite chiffrés les uns après les autres.
  Lucifer, DES, TDES, AES, Blowfish, Twofish
- Chiffrement par flot : traitement des données de longueur quelconque et dans découpe.
  A5/1 (GSM), A5/2, A5/3, RC4 (Wep), Py, E0 (bluetooth)

DÉPARTEMENT Sciences Informatiques

Principe du chiffrement par bloc

1. Remplacer les caractères par un code binaire (par exemple le code ASCII en base 2). On obtient ainsi une longue chaîne de 0 et de 1.
2. Découper cette chaîne en blocs de longueur donnée, par exemple 64 bits.
3. Chiffrer un bloc en l'"additionnant" bit par bit à une clef.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3. On appelle cela une ronde.
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

Schéma de Feistel



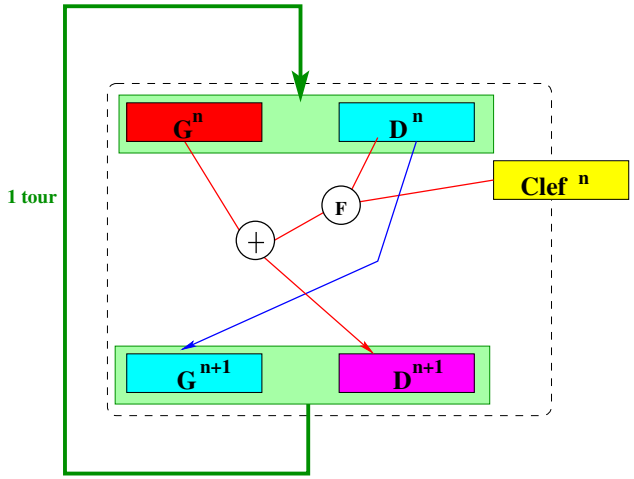
DÉPARTEMENT
Sciences Informatiques

Principe du chiffrement par bloc

La sécurité du chiffre repose sur :

- la taille de la clé
- la difficulté d'inverser la fonction F.

Schéma de Feistel



DÉPARTEMENT
Sciences Informatiques

Algorithmes de chiffrement par bloc basé sur un réseau de Feistel

Algorithme	Concepteur	Date	Taille du bloc	Taille de la clef	Nombre de cycles
Lucifer	Feistel (IBM)	1971	32/48/128	48/64/128	16
DES	IBM	1975 (std 1977)	64	56	16
Triple-DES	Tuchman (IBM)	1999	64	168/112	3x16
G-DES	I. Schaumuller-Bicht	1981	32n (256)	56	16
DES-X	Rivest	1984	64	184	16
ICE		1997	64	64	16
Blowfish	B.Schneier	1993	64	32-448	16
Twofish		2000	128	128/192/256	16

DÉPARTEMENT
Sciences Informatiques

Advanced Encryption Standard (AES)

Algorithme	Concepteur	Date	Taille du bloc	Taille de la clef	Nombre de cycles
AES	J. Daemen, V.Rijmen	2000	128	128/192/256	10/12/14

DÉPARTEMENT
Sciences Informatiques

Algorithme AES

Chaque bloc de 128 bits (16 octets) est transformé en une matrice de 4x4 octets (après permutation). Puis :

1. SubBytes : substitution de chaque élément (S-box)
2. ShiftRows : décalage des lignes (en fonction du numéro de ligne)
3. MixColumns : transformation linéaire de chaque colonne (multiplication par un polynome)
4. AddRoundKey : XOR avec une matrice dérivée d'une sous-partie de la clef

Plus rapide et sécurisé que DES.

DÉPARTEMENT Sciences Informatiques

Algorithme IDEA

Algorithme	Concepteur	Date	Taille du bloc	Taille de la clef	Nombre de cycles
IDEA	X. Lai, J. Massey	1991	64	128	$8 + 1/2$

DÉPARTEMENT
Sciences Informatiques

Principe du chiffrement par flot

Un chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper.

- Chiffrement du message M avec la clé K : $M \oplus K = C$
- Déchiffrement du message C avec la clé K :
  $C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M$

Hardware	Software
HC-128	F-FCSR-H v2
Rabbit	Grain v1
Salsa20/12	MICKEY v2
Sosemanuk	Trivium

(source : http ://fr.wikipedia.org/wiki/Chiffrement_par_flot)

DÉPARTEMENT Sciences Informatiques

Chiffrement symétrique : synthèse

Une unique clé secrète partagée entre les 2 parties qui sert pour le chiffrement et le déchiffrement du message

Algorithmes utilisant ce système :

- RC2, RC4
- DES, TDES, D-DES, DES-x
- Blowfish, Twofish
- IDEA,
- AES

Avantage :

- Rapide

Inconvénients :

- Il faut autant de clefs que de couples de correspondants
- La non-répudiation n'est pas assurée. Mon correspondant possédant la même clé que moi, il peut fabriquer un message en usurpant mon identité
- Transmission de clef ?

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Clef

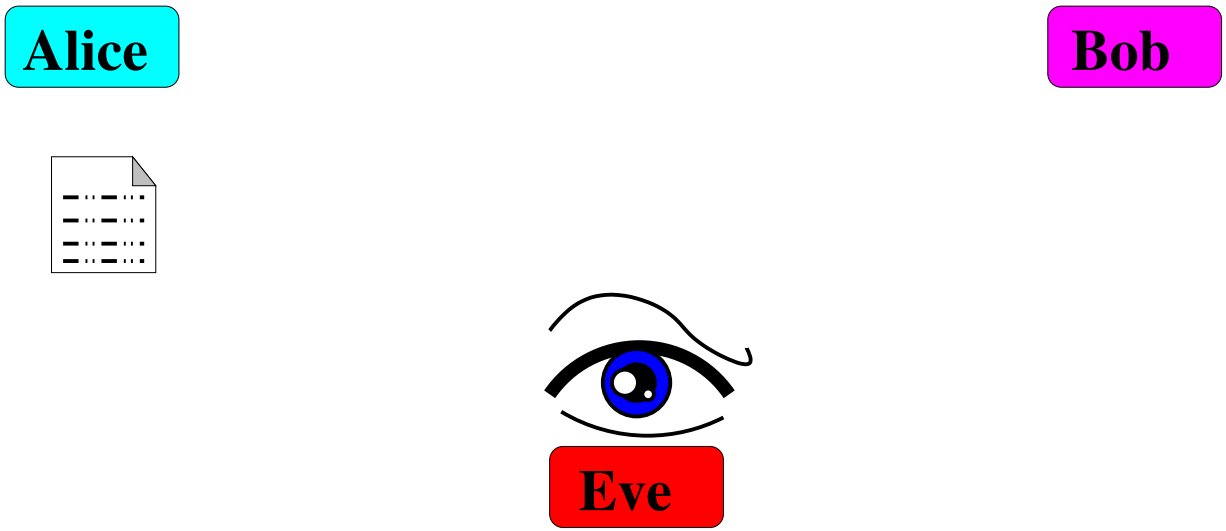
La sécurité d'un système de cryptement ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clef.

Problème : Comment distribuer la clef ?

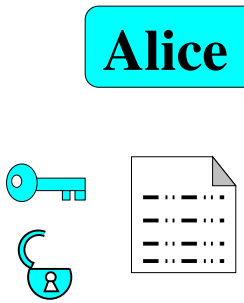
- Steganographie : dangereux
- rencontre physique (pas toujours faisable...)

DÉPARTEMENT Sciences Informatiques

Principe de Diffie-Hellman-Merkle

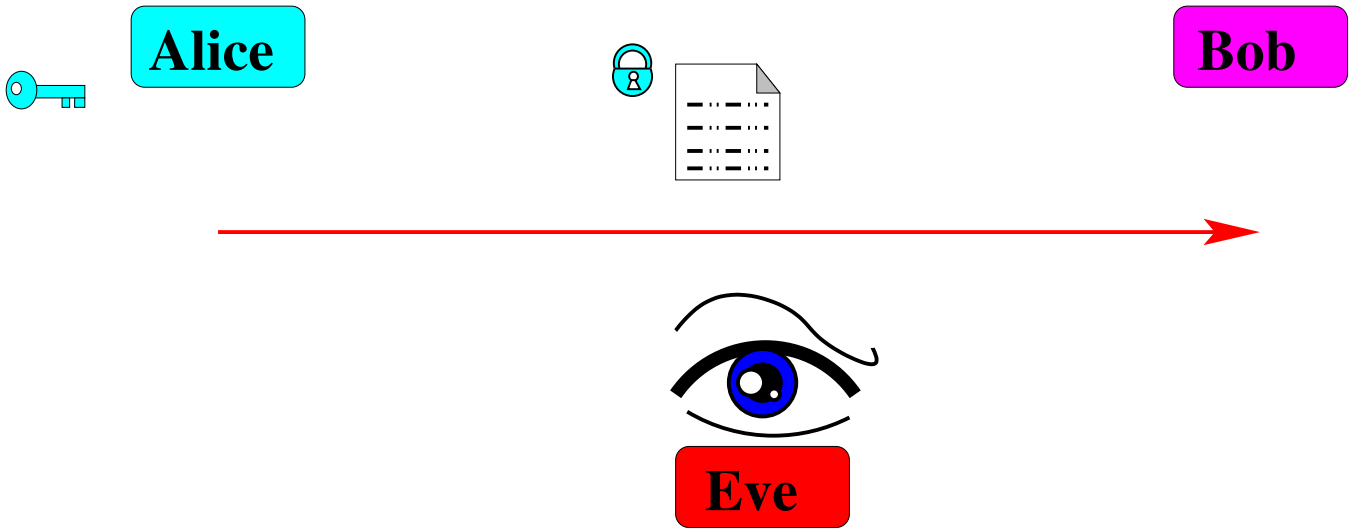


Principe de Diffie-Hellman-Merkle



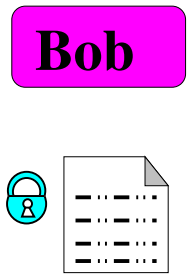
DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle



DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle

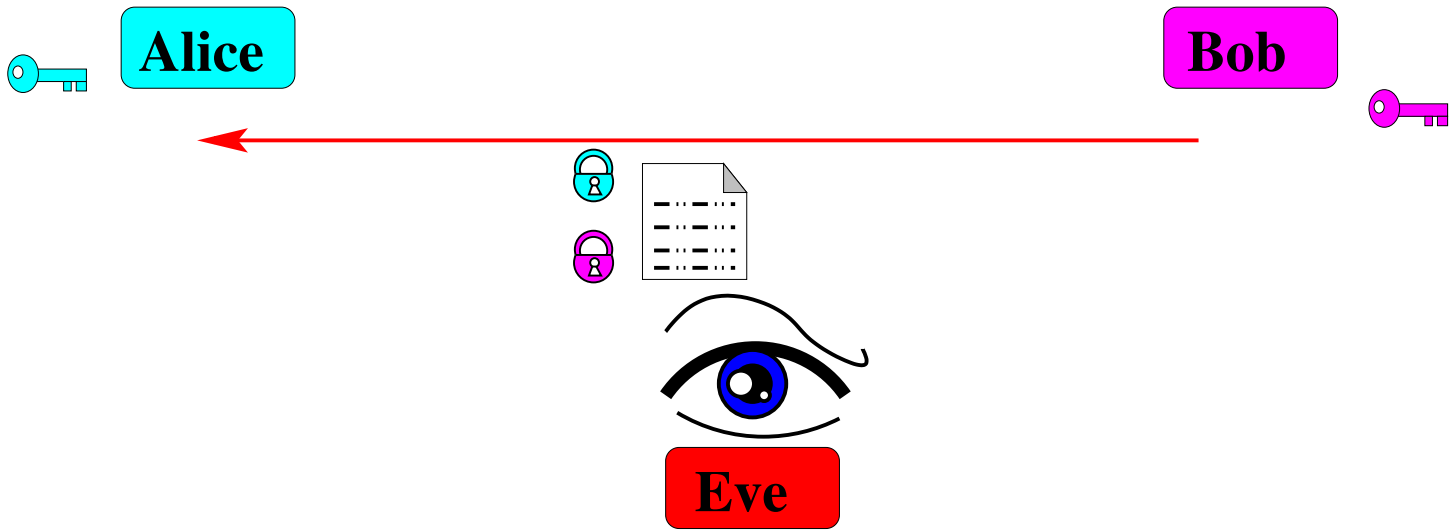


DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle

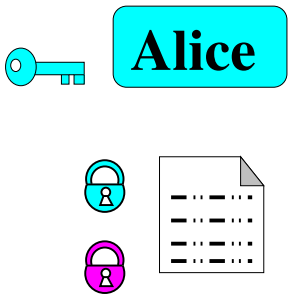
DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle

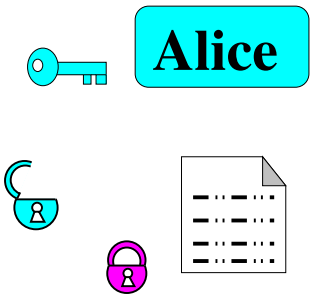


DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle

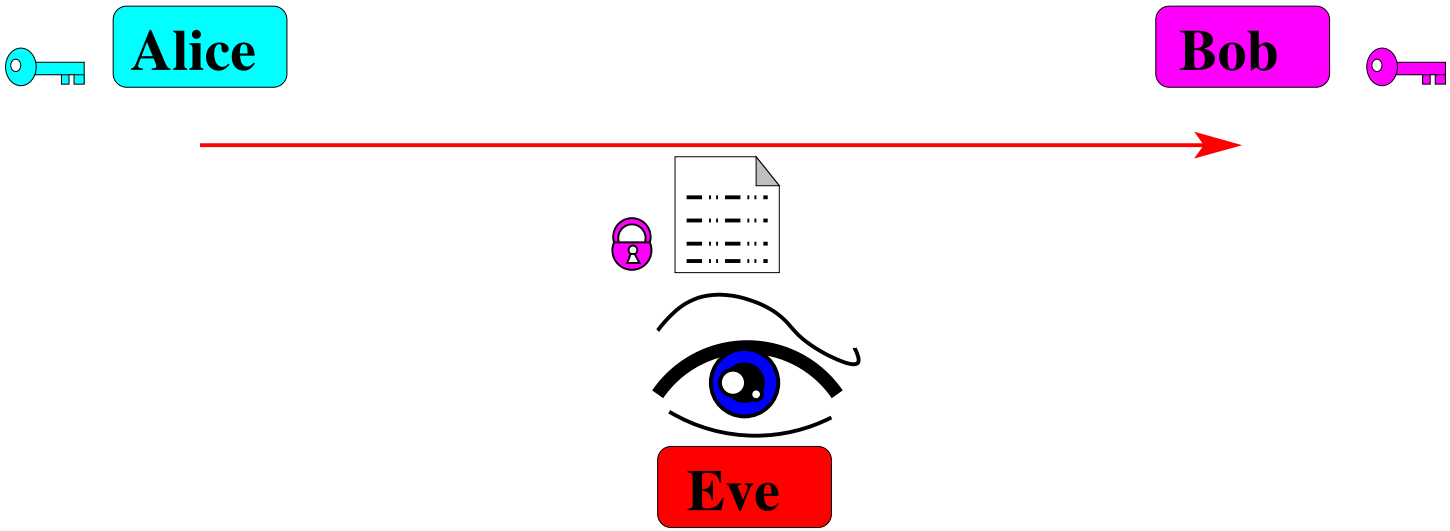


Principe de Diffie-Hellman-Merkle



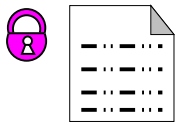
DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle



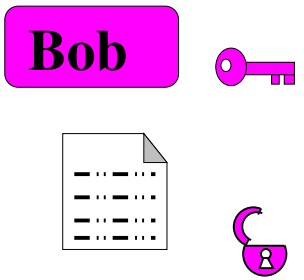
DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle

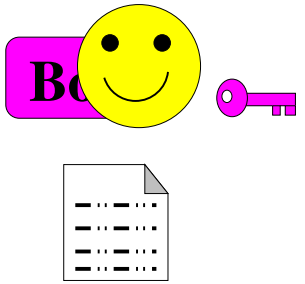


DÉPARTEMENT
Sciences Informatiques

Principe de Diffie-Hellman-Merkle



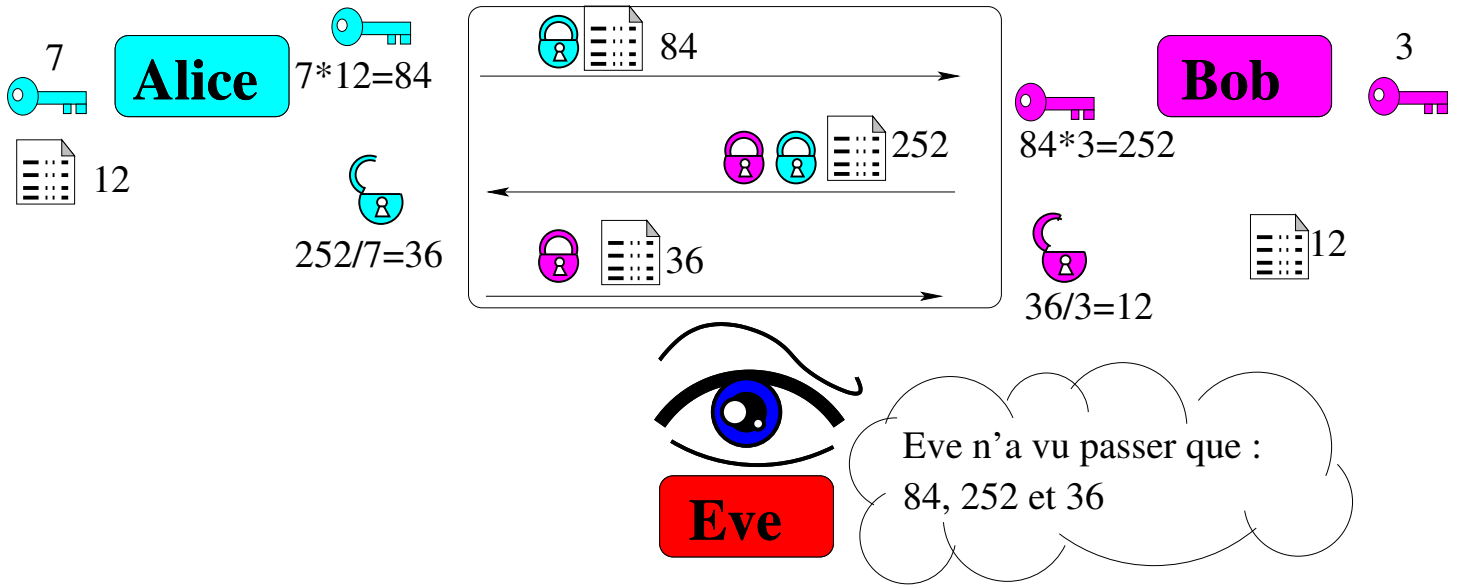
Principe de Diffie-Hellman-Merkle



DÉPARTEMENT
Sciences Informatiques

Recherche de fonctions mathématiques

Soit la fonction de chiffrement $f(x) = x \times A \times B$ où A et B sont les clefs secrètes respectives de Alice et de Bob.



Critique de cette méthode :

- Bob peut retrouver la clef secrète de Alice (en faisant $252/(12 \times 3)$.
- Alice peut retrouver la clef secrète de Bob (en faisant $252/(12 \times 7)$.
- Si Eve connait l'algorithme (et donc la fonction f), elle peut déduire la clef secrète de A et de B et donc x.

$\Rightarrow$ Décompositions en nombres premiers

$\Rightarrow$ Calcul des PGCD et PPCM

DÉPARTEMENT Sciences Informatiques

Recherche de fonctions mathématiques

Recherche d'une fonction à sens unique

- faciles à appliquer
- mais difficilement inversible

$$Y^x(modP)$$

(Rappel : le modulo, noté aussi $[P]$ (ou en programmation % P), est le reste de la division entière par P)

DÉPARTEMENT
Sciences Informatiques

Echange de Diffie-Hellman-Merkle

Alice et Bob conviennent de Y et P, la fonction est donc $f(x) = Y^x(modP)$

Alice

- Alice choisit un nombre secret : A
- Alice calcule $\alpha = f(A) = Y^A(modP)$
- Alice envoie α à Bob
- Alice calcule $\beta^A(modP)$

Bob

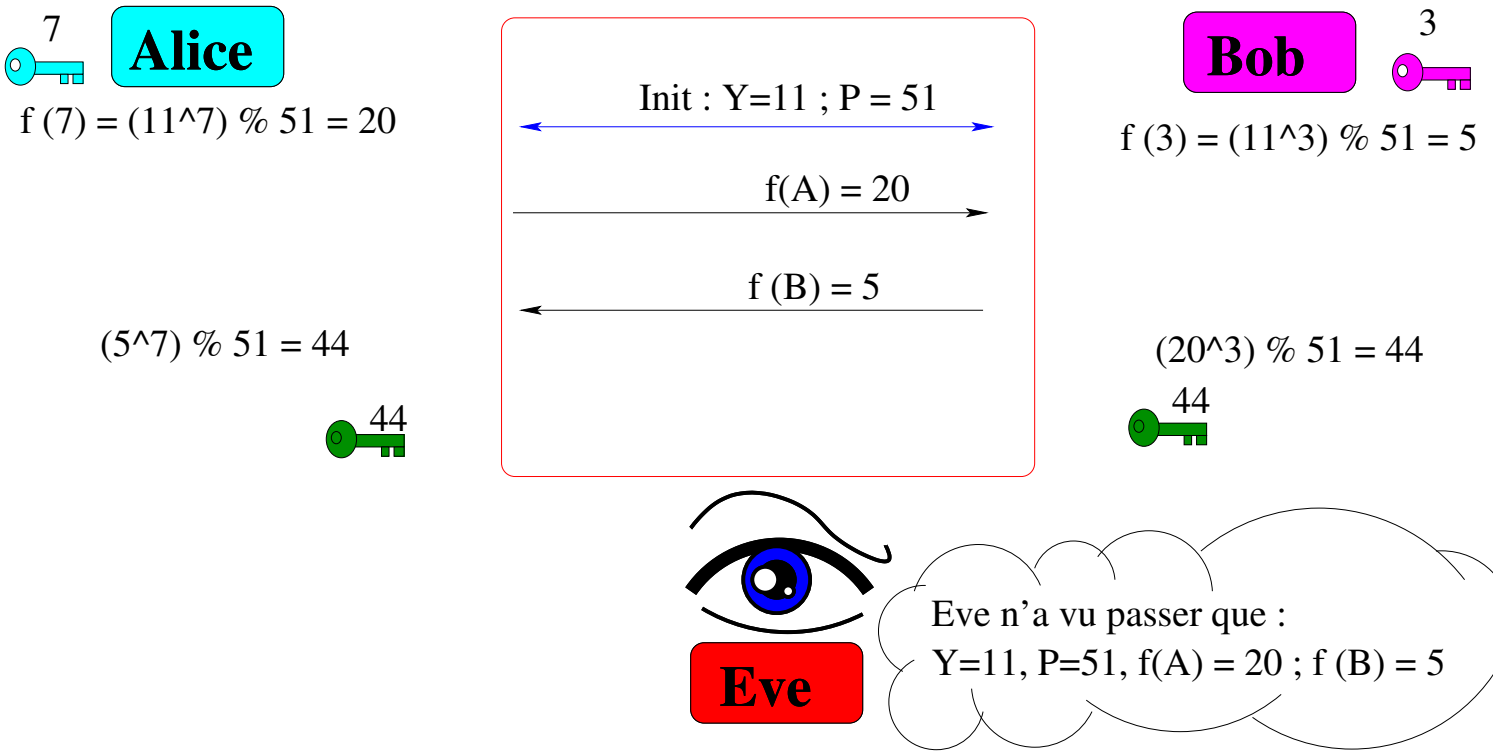
- Bob choisit un nombre secret : B
- Bob calcule $\beta = f(B) = Y^B(modP)$
- Bob envoie β à Alice
- Bob calcule $\alpha^B(modP)$

Alice et Bob ont obtenu le même nombre : $k = \beta^A(modP) = \alpha^B(modP)$ qui servira de clef (pour DES par exemple).

Même si Eve avait intercepté Y, P, α et β, elle ne peut pas trouver k.

DÉPARTEMENT Sciences Informatiques

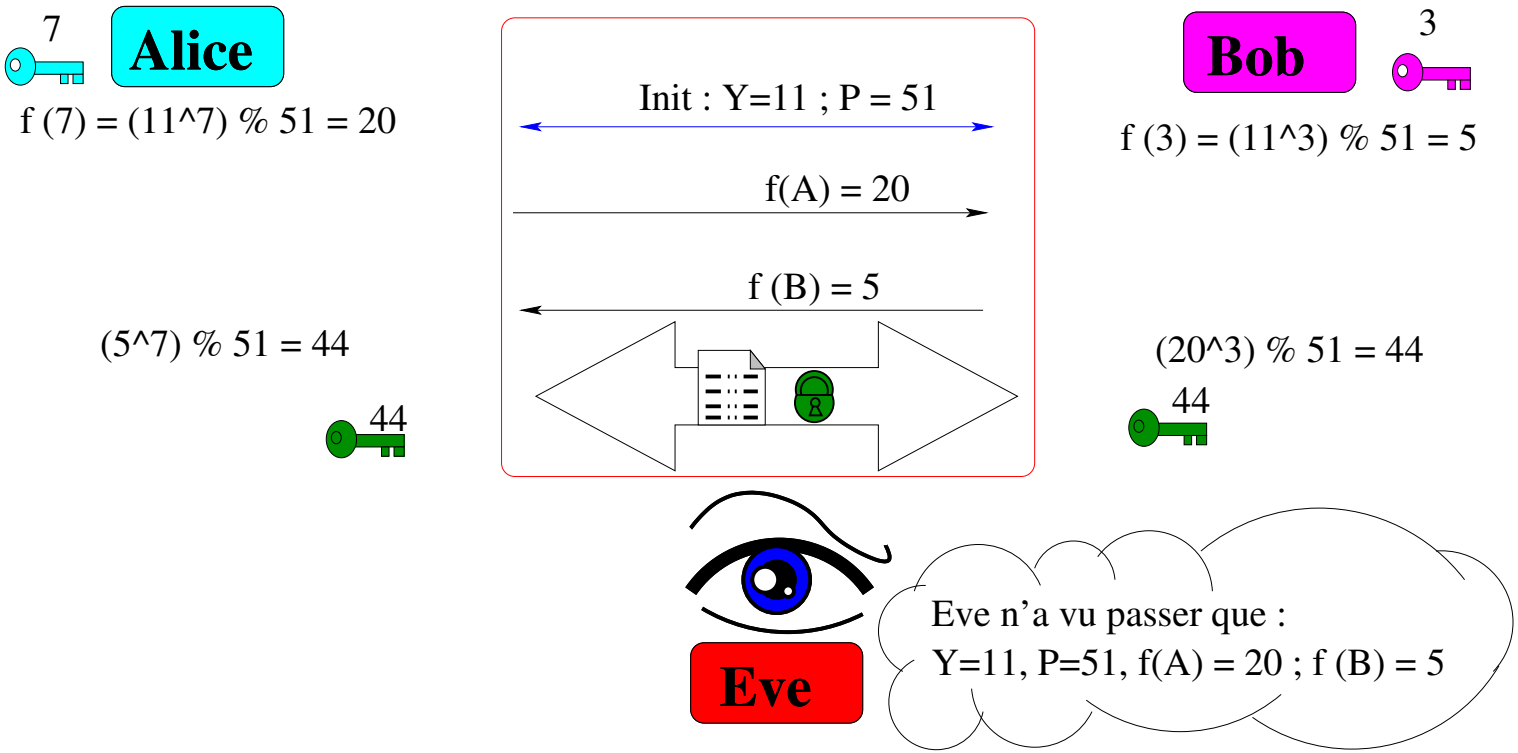
Diffie-Hellman-Merkle



La clef générée sera ensuite utilisée avec un chiffrement à clef symétrique (par exemple DES).

DÉPARTEMENT Sciences Informatiques

Diffie-Hellman-Merkle



La clef générée sera ensuite utilisée avec un chiffrement à clef symétrique (par exemple DES).

DÉPARTEMENT Sciences Informatiques

Synthèse : Diffie-Hellman-Merkle

- 2 partis peuvent convenir d'une clef sans se rencontrer
- ... de manière sûre (même s'ils sont sur écoute).

La clef générée sera ensuite utilisée avec DES par exemple. (DES utilise une clef symétrique : même clef pour chiffrer et déchiffrer)
Inconvénient :

- Nécessite un certain nombre d'échanges synchronisés (Alice et Bob doivent être présents tous les deux au moment de l'établissement de la clef).
  $\Rightarrow$ peu pratique pour les e-mails
  $\Rightarrow$ peu pratique pour le commerce électronique

DÉPARTEMENT Sciences Informatiques

Echange de Rivest-Shamir-Adleman

- Alice choisit deux nombres premiers p et q et les garde secrets.
- Alice calcule $n = p \times q$ (module de chiffrement)
- Alice choisit un e tel que $e + (p-1) \times (q-1)$ soit un nombre premier relatif
- Alice diffuse (n, e), cette paire s'appelle Clef publique
- Alice calcule (et garde secrète) d telle que :
  $e \times d = 1(mod((p-1)(q-1)))$. Le couple (n, d) est appelé clef privée.

DÉPARTEMENT
Sciences Informatiques

RSA créer une paire de clef

Il faut générer e, d, et n.

- Prendre deux nombres premiers p et q (de taille à peu près égale). Calculer $n = pq$.
- Prendre un nombre e qui n'a aucun facteur en commun avec $(p-1)(q-1)$.
- Calculer d tel que $e \times dmod(p-1)(q-1) = 1$, c-à-d d est le modulo inverse de e dans $Z/(p-1)(q-1)Z$: $d = e^{-1} mod((p-1)(q-1))$.
- (e, n) sera la clef publique et (d, n) la clef privée.

DÉPARTEMENT Sciences Informatiques

RSA : Exemple

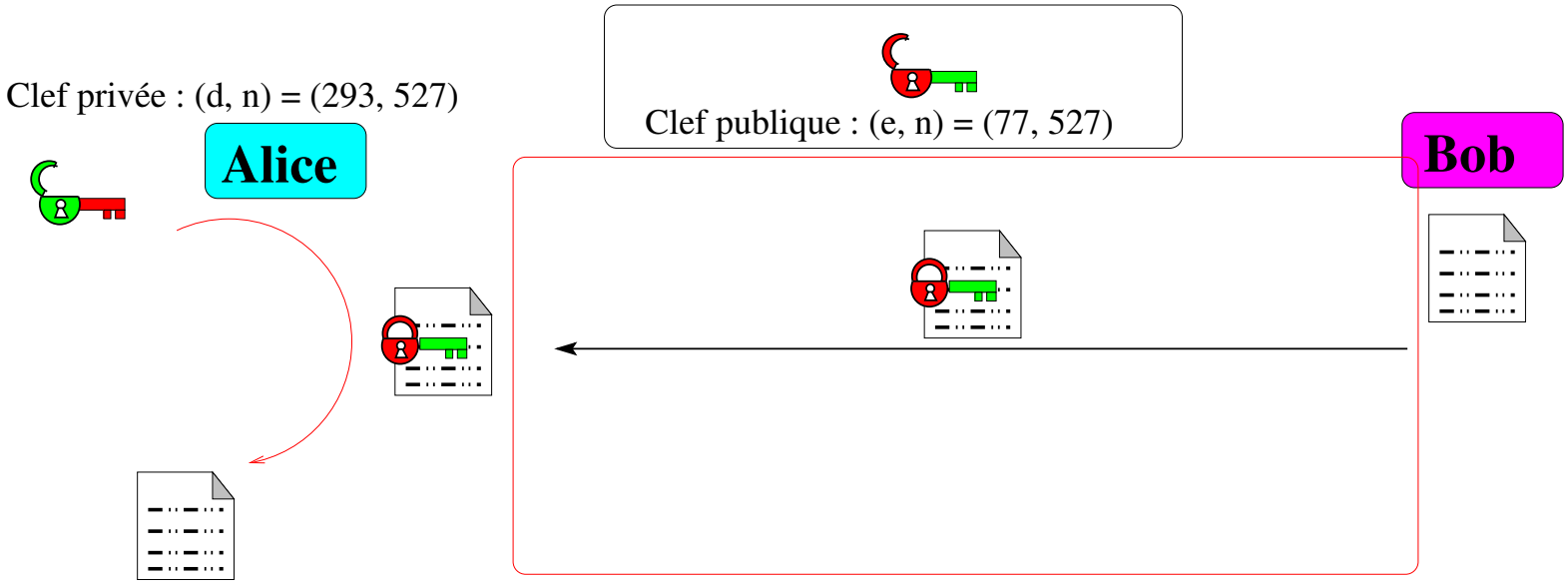
- Soit $p = 17$ et $q = 31$; $n = p \times q = 17 \times 31 = 527$
- On doit choisir un e quelconque tel que e n'ai aucun facteur en commun avec $(p-1)(q-1) = (17-1)(31-1) = 480$. Comme $480 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 5$, on prendra par exemple $e = 77$.
- On calcule $d = e^{-1} mod (p-1)(q-1) = 77^{-1} mod (480) = 293$.

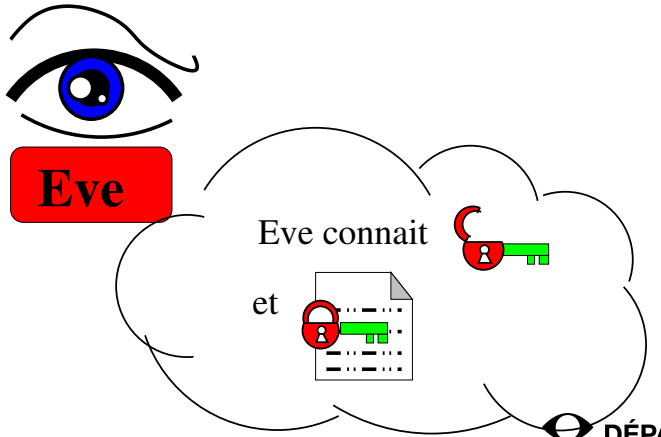
On a au final :

- la clef publique (=pour encrypter) : $(e, n) = (77, 527)$
- la clef privée (=pour décrypter) : $(d, n) = (293, 527)$

DÉPARTEMENT Sciences Informatiques

Rivest-Shamir-Adleman





DÉPARTEMENT
Sciences Informatiques

Chiffrement/Déchiffrement avec RSA

Pour chiffrer un message en clair en un message chiffré.

- Convertir le message en suite de nombre (ASCII, rang dans l'alphabet, etc.)
- Couper cette suite en blocs qui formera un nombre M.
- Convertir chaque nombre M en un nombre C chiffré selon la formule :

$$C = M^e (mod N)$$

Pour déchiffrer :

- Prendre chaque chiffre C, puis appliquer :

$$M = C^d (mod N)$$

- Convertir chaque nombre C en caractères formant le message

DÉPARTEMENT Sciences Informatiques

Chiffrement/Déchiffrement avec RSA : Exemple

Soit le mot à chiffrer : TRI

- ASCII (décimal) : 84 82 73
- ASCII (binaire) : 1000011 1000011 1000011
- Par bloc de 6 : 100001 110000 111000 011000
- Conversion décimale : 33 48 56 24

La représentation **codée** du mot TRI est 33 48 56 24
(code connu : algo, taille des blocs et table ASCII connue).

Chiffrement de 33 48 56 24.

- $C = M^e (mod N)$:
  - $33 * *77\%527 = 407$
  - $48 * *77\%527 = 362$
  - $56 * *77\%527 = 377$
  - $24 * *77\%527 = 261$

Message chiffré : 407, 362, 377, 261.

Utiliser un calculateur à entier long.

Déchiffrement de 407, 362, 377, 261.

- $M = C^d (mod N)$:
  - $407 * *293\%527 = 33$
  - $362 * *293\%527 = 48$
  - $377 * *293\%527 = 56$
  - $261 * *293\%527 = 24$

Message déchiffré : 33 48 56 24.

DÉPARTEMENT Sciences Informatiques

Nombres premiers

$n = p \times q$. Si p et q premiers et suffisamment grand, alors connaissant n, il est très difficile de retrouver p et q.

Ordre d'idées :

- Jusqu'au nombre 10000000000000000000000 il y a 19253203916068039689 23 nombres premiers.
- 16 juin 2009, le plus grand nombre premier $2^{42643801} - 1$ (presque 13 millions de chiffres) calculé (116.000 PC developpant à eux tous une puissance de 40 TFlop/seconde.)

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157

163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317

331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499

503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683

691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883

887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063

1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231

1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427

1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553 1559 1567 1571

DÉPARTEMENT Sciences Informatiques

Chiffrement asymétrique : synthèse

Les deux clefs sont fabriqués ensemble et :

- la connaissance d'une des clefs ne permet pas de déduire l'autre
- ce qui est chiffré avec une clef ne peut être déchiffré que par l'autre clef

On choisit ensuite arbitrairement de rendre une des ces clef publique et garder l'autre privée.
Ensuite

- Clé publique : Sert à chiffrer le message
- Clé privée : Sert à déchiffrer le message

Mais dans certains cas (signature) on chiffrera un message avec la clef privée qui ne pourra être déchiffrée que par la clef publique.

DÉPARTEMENT Sciences Informatiques

Chiffrement asymétrique : synthèse (2)

Algorithmes utilisant ce système :

- Diffie-Helmann-Merkle
- RSA
- DSA, ElGamal

Avantage :

- pas besoin de se transmettre les clés au départ par un autre vecteur de transmission.

Inconvénient :

- Lent !

DÉPARTEMENT Sciences Informatiques

RSA

RSA : breveté par le MIT de 1983 à 2000 (brevet expiré) En 2008, c'est le système à clef publique le plus utilisé (carte bancaire française, de nombreux sites web commerciaux...).

Combinaison du chiffrement symétrique et asymétrique

- Chiffrement symétrique : Rapide mais problème d'échanges de clefs
- Chiffrement asymétrique synchrone : pas de problèmes d'échange de clefs mais nécessite la présence simultanée des deux partis
- Chiffrement asymétrique asynchrone : pas de problèmes d'échange de clefs, pas de présence simultanée des deux partis requise, mais lent

Idée :

- utiliser le chiffrement asymétrique (RSA, DSA, etc...) pour générer une clef de session. Puis utiliser le chiffrement symétrique (DES, IDEA, ...) pour chiffrer/déchiffrer les messages à l'aide de cette clef de session.

$\Rightarrow$ PGP

DÉPARTEMENT Sciences Informatiques

Confidentialité

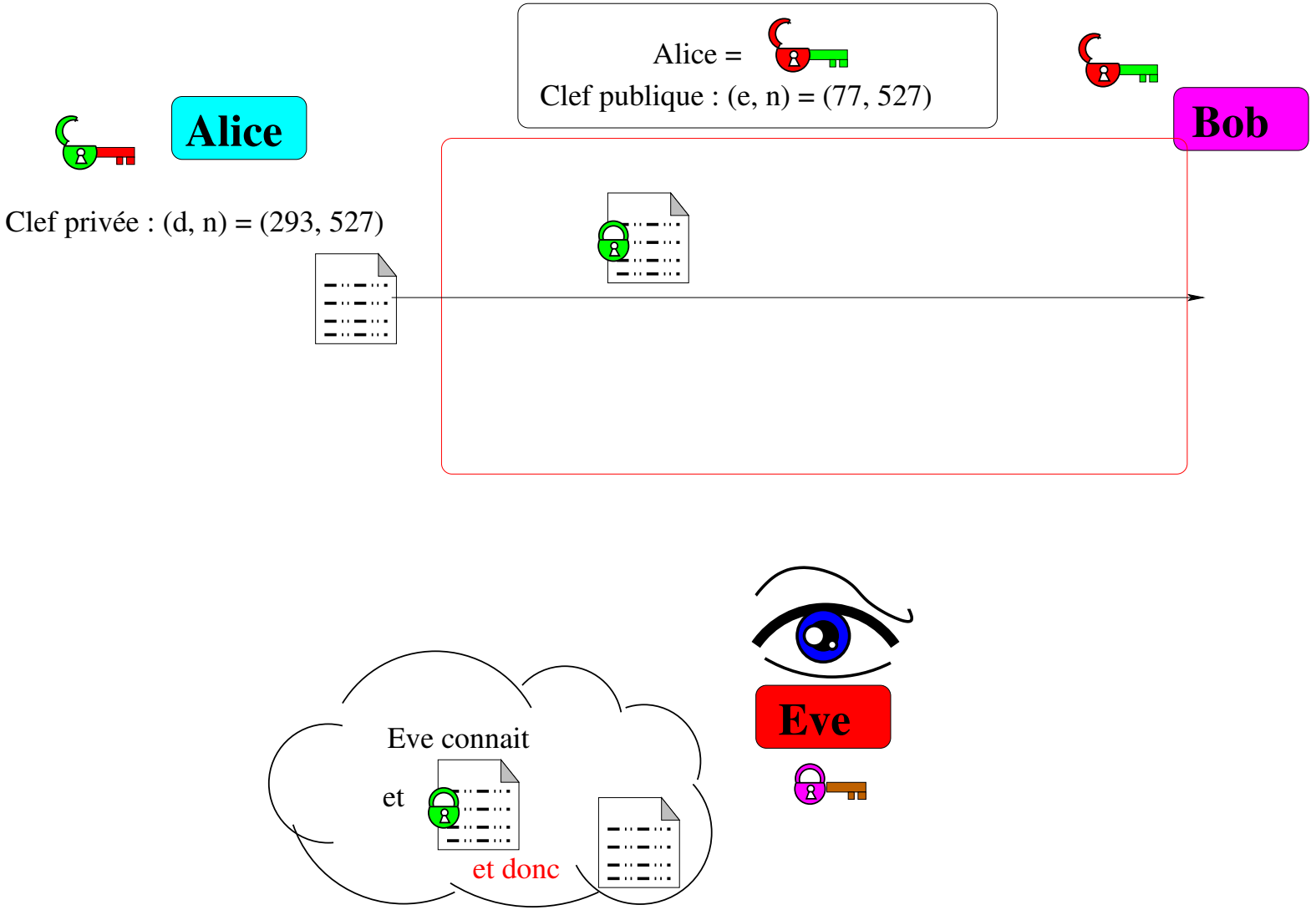
Assurer la confidentialité

1. Utiliser le chiffrement asymétrique (RSA) pour générer une clef de session.
2. Puis utiliser le chiffrement symétrique (DES, IDEA, AES) pour chiffrer/déchiffrer les messages à l'aide de cette clef de session.

DÉPARTEMENT
Sciences Informatiques

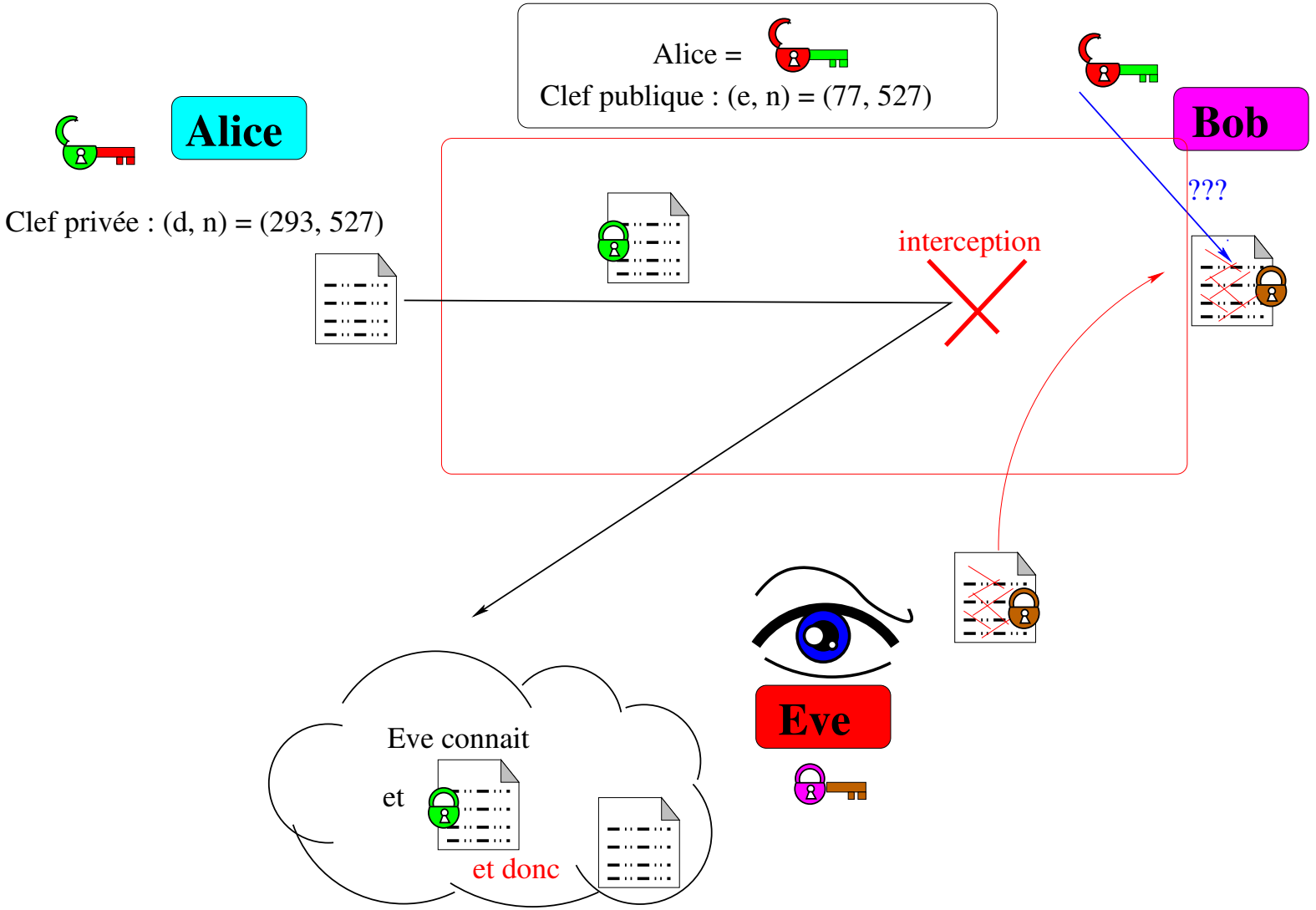
DÉPARTEMENT
Sciences Informatiques

Rivest-Shamir-Adleman



Un un message chiffré avec la clef privée ne peut être déchiffrée que par la

Rivest-Shamir-Adleman



Un un message chiffré avec la clef privée ne peut être déchiffrée que par la

- La personne à qui j'envoie un message crypté est-elle bien celle à laquelle je pense ?
- La personne qui m'envoie un message crypté est-elle bien celle à qui je pense ?

Terminologie

- Prouveur : Celui qui s'identifie, qui prétend être
- Vérifieur : Fournisseur du service
- Challenge : Le Vérifieur va lancer un challenge au prouveur que ce dernier doit réaliser

DÉPARTEMENT
Sciences Informatiques

Challenge

On vérifie que

$$D_{prive}(C_{public}(message)) = D_{public}(C_{prive}(message))$$

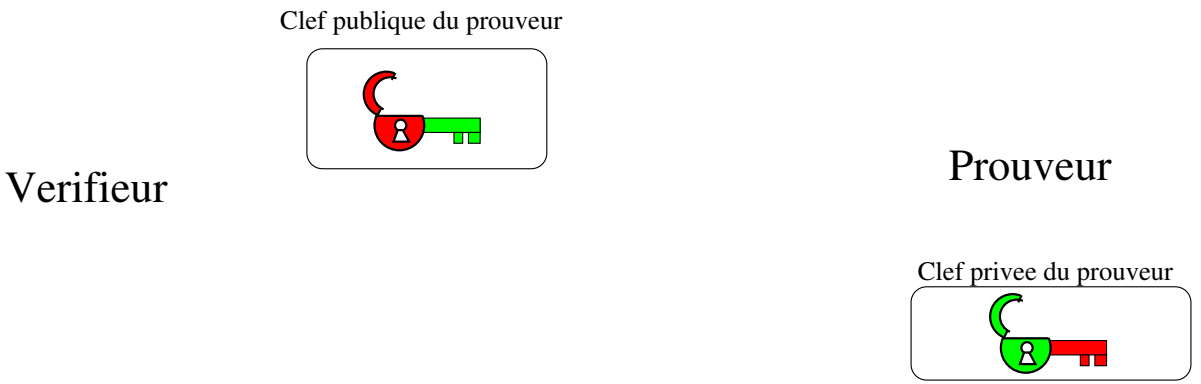
- Le texte est totalement confidentiel car le destinataire est le seul a avoir la clé privée
- On est sûr de l'identité de l'émetteur car il est le seul à pouvoir chiffrer un message avec cette clé privée

DÉPARTEMENT Sciences Informatiques

Challenge

On vérifie que

$$D_{prive}(C_{public}(message)) = D_{public}(C_{prive}(message))$$

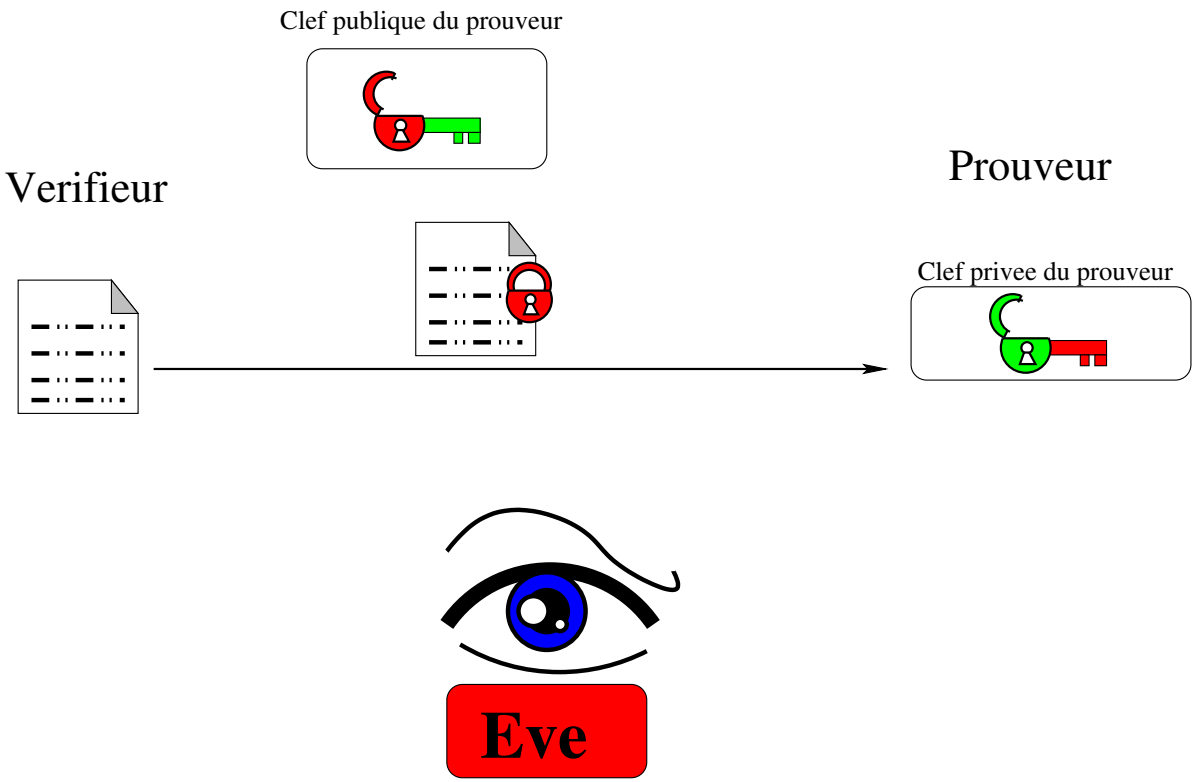


- Le texte est totalement confidentiel car le destinataire est le seul a avoir la clé privée

Challenge

On vérifie que

$$D_{prive}(C_{public}(message)) = D_{public}(C_{prive}(message))$$

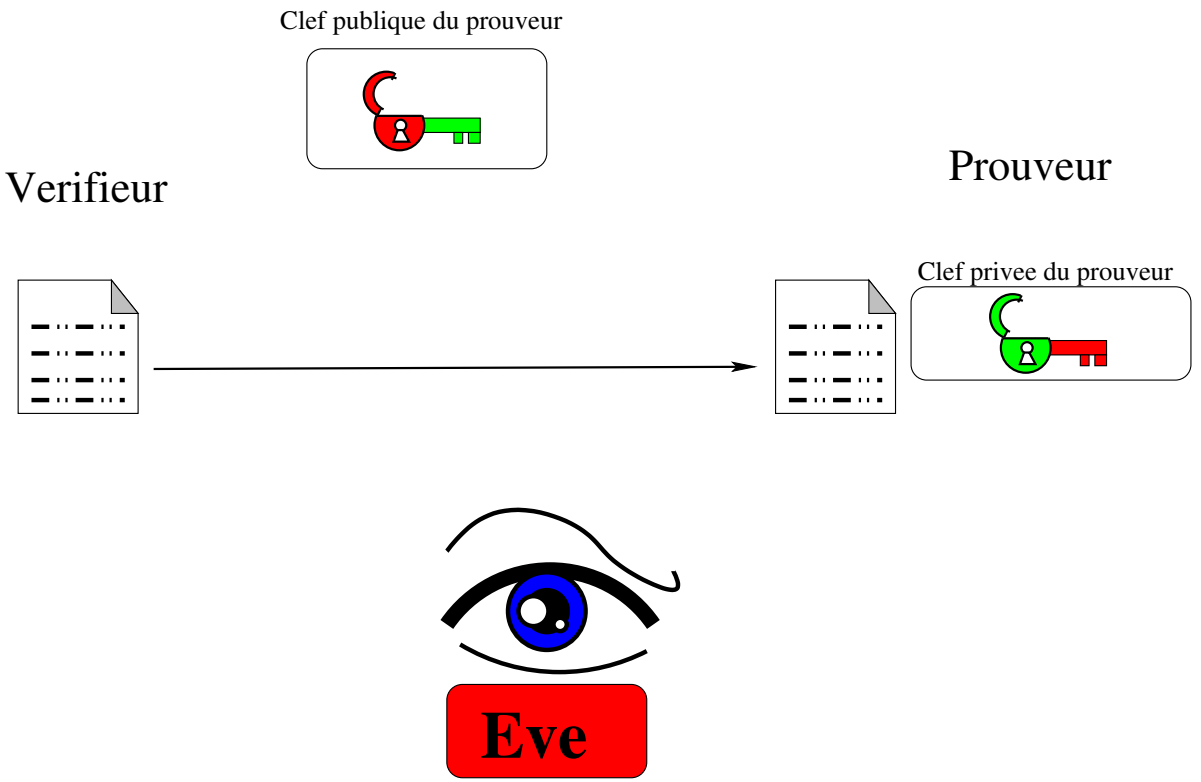


- Le texte est totalement confidentiel car le destinataire est le seul a avoir la clé privée

Challenge

On vérifie que

$$D_{prive}(C_{public}(message)) = D_{public}(C_{prive}(message))$$



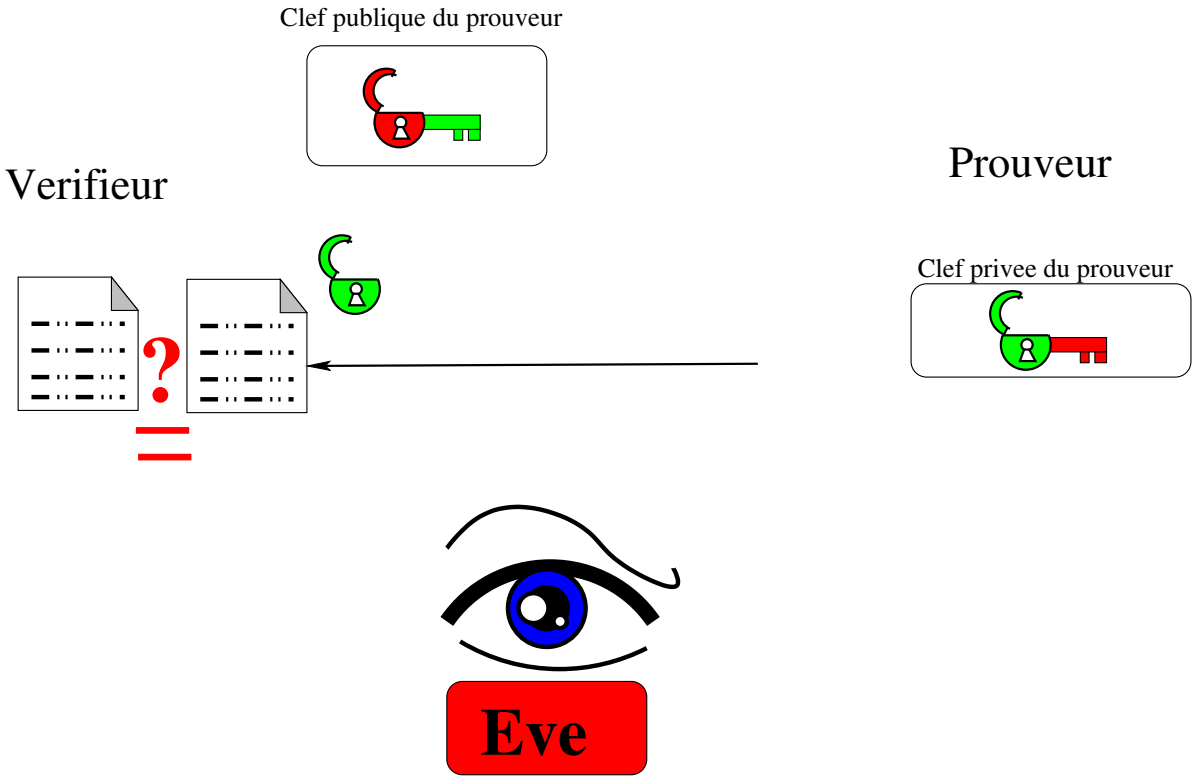
- Le texte est totalement confidentiel car le destinataire est le seul a avoir la clé privée

DÉPARTEMENT Sciences Informatiques

Challenge

On vérifie que

$$D_{prive}(C_{public}(message)) = D_{public}(C_{prive}(message))$$

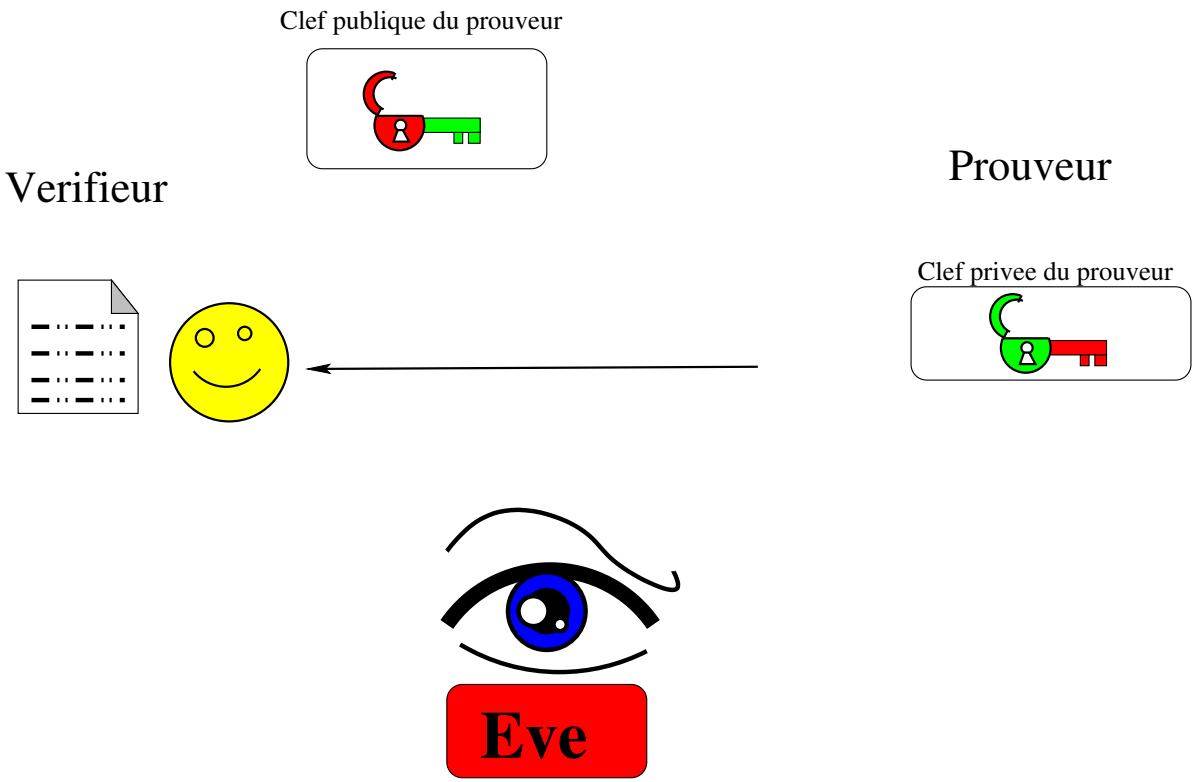


- Le texte est totalement confidentiel car le destinataire est le seul a avoir la clé privée

Challenge

On vérifie que

$$D_{prive}(C_{public}(message)) = D_{public}(C_{prive}(message))$$

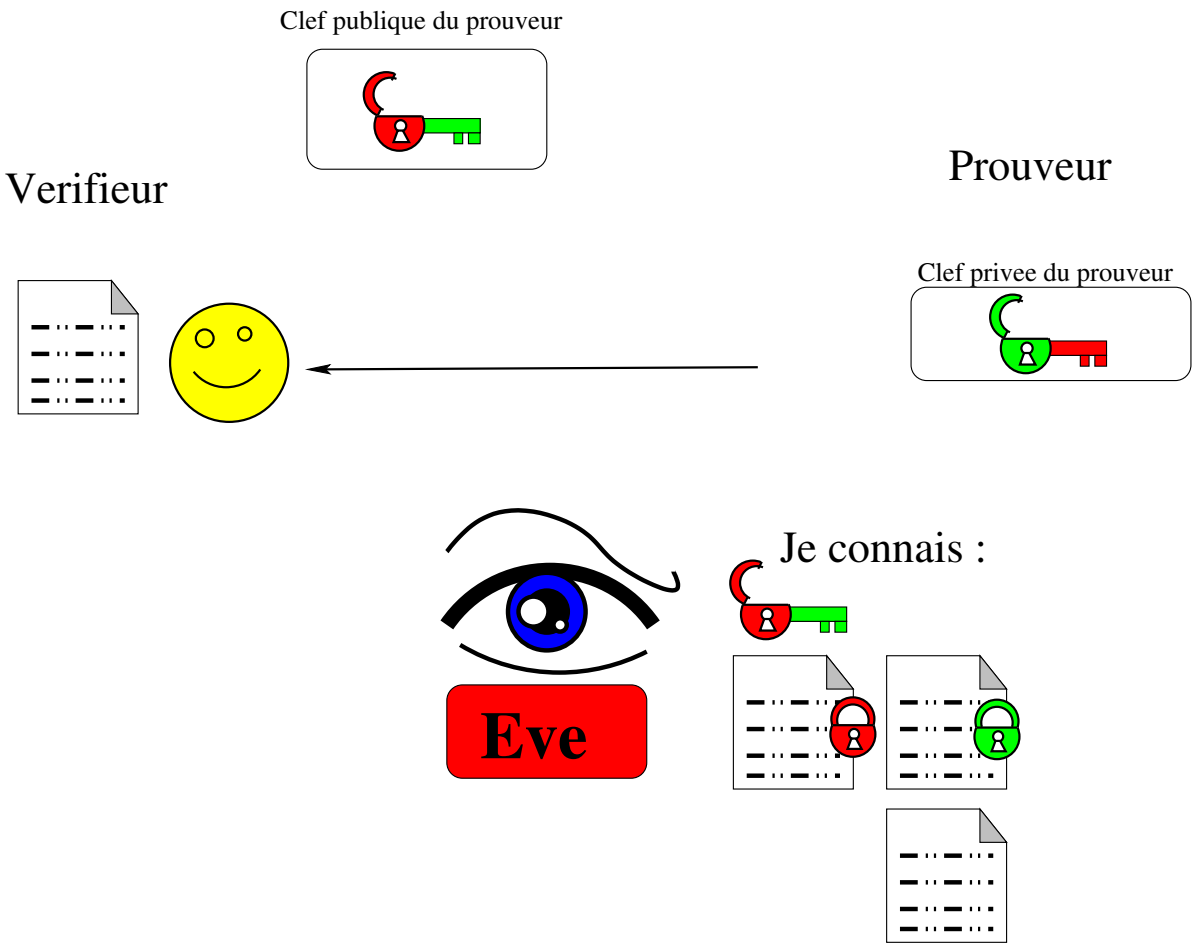


- Le texte est totalement confidentiel car le destinataire est le seul a avoir la clé privée

Challenge

On vérifie que

$$D_{prive}(C_{public}(message)) = D_{public}(C_{prive}(message))$$



DÉPARTEMENT
Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Intégrité et fonction de hachage

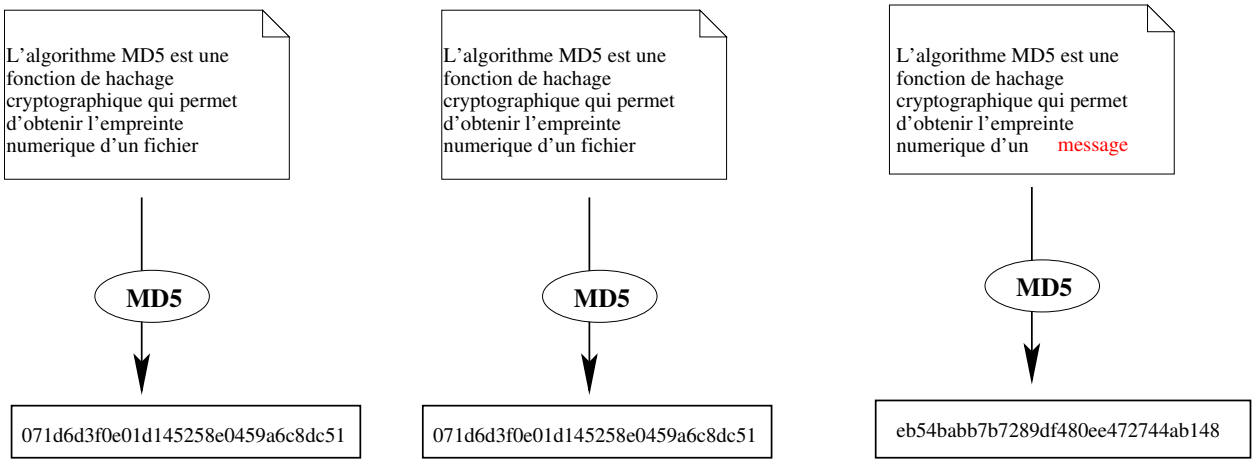
Comment savoir que le message n'a pas été altéré ? $\Rightarrow$ fonction de hachage

- MD5 (128 bits)
- SHA1 (160 bits)
- RIPEMD-160 (160 bits)
- Whirlpool (512 bits)

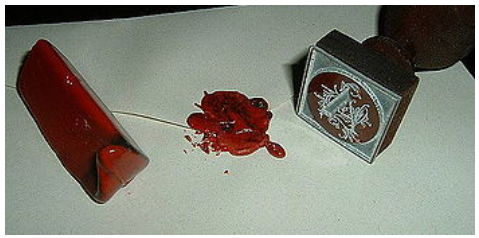
Une fonction de hachage

- prend une donnée quelconque
- renvoie une donnée de taille fixe
- est à sens unique sans trappe
- est facile à calculer

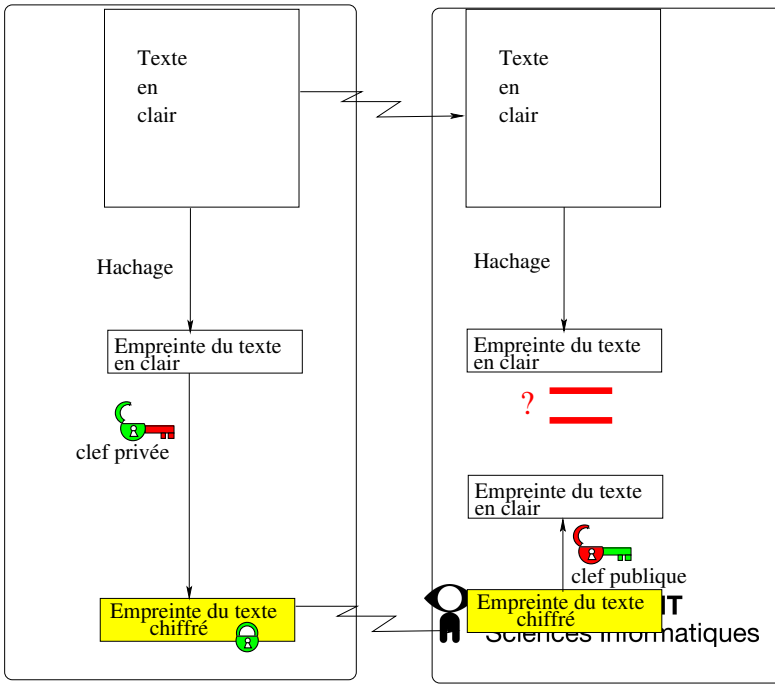
DÉPARTEMENT Sciences Informatiques


L'algorithme MD5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numerique d'un fichier
MD5
071d6d3f0e01d145258e0459a6c8dc51
L'algorithme MD5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numerique d'un fichier
MD5
071d6d3f0e01d145258e0459a6c8dc51
L'algorithme MD5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numerique d'un message
MD5
eb54babb7b7289df480ee472744ab148

Hachage et signature électronique



La fonction de hachage permet de garantir l'intégrité du message et est très rapide à calculer, mais ne garanti pas l'identité de l'expéditeur.
La signature électronique garanti l'identité de l'expéditeur, mais il faut signer tout le message pour garantir son intégrité ⇒ long
⇒ on utilise un sceau : on hache le message et on ne signe que le résultat haché.



DÉPARTEMENT
Sciences Informatiques

Crédits I

- http ://www.apprendre-en-ligne.net/crypto/ de Didier Müller.
- http ://fr.wikipedia.org/
- Histoire des codes secrets - Simon Singh Le livre de poche
- http ://www.sharevb.net/Les-bases-de-la-cryptographie.html

DÉPARTEMENT
Sciences Informatiques