

La cryptographie ou les mathématiques au service de la protection de l'information

Anne Canteaut

INRIA-projet CODES

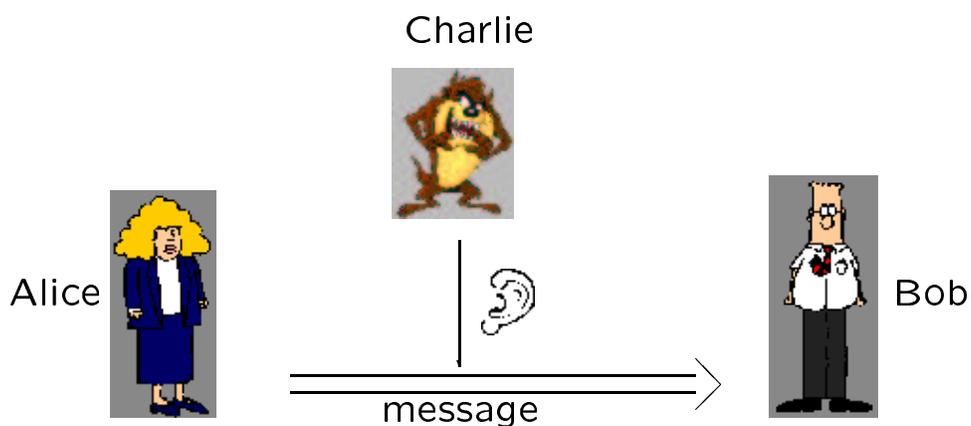
Domaine de Voluceau

78153 Le Chesnay

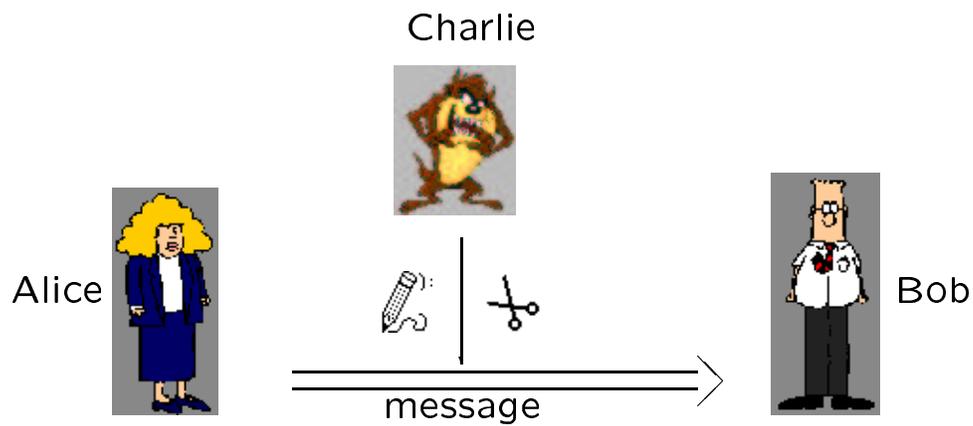
Anne.Canteaut@inria.fr

<http://www-rocq.inria.fr/codes/Anne.Canteaut/>

Attaques passives



menace contre la **confidentialité de l'information** :
une information sensible parvient à une personne autre
que son destinataire légitime.



menace contre l'**intégrité de l'information** :

l'information reçue est interprétée comme provenant d'une personne autre que son véritable auteur.

2

Différents types d'attaques actives

- usurpation d'identité (de l'émetteur ou du récepteur)
- altération des données = modification du contenu du message
- destruction du message
- retardement de la transmission
- répétition du message
- répudiation du message = l'émetteur nie avoir envoyé le message

3

- ... -19^e s. transpositions et substitutions alphabétiques
- 1883 *La cryptographie militaire* [Kerckhoffs]
→ formalisation des systèmes de chiffrement
- 1926 *Cipher printing telegraph systems for secret wire and radio telegraphic communications* [Vernam]
→ chiffrement de Vernam
- 1939-44 Enigma et les "bombes" de Bletchley Park
- 1949 *Communication theory for secrecy systems* [Shannon]
→ notion de sécurité inconditionnelle
- 1973-77 standardisation du DES
- 1976 *New directions in cryptography* [Diffie - Hellman]
→ invention de la cryptographie à clef publique
- 1978 *A method for obtaining digital signatures and public-key cryptosystems* [Rivest-Shamir-Adleman]
→ invention du RSA

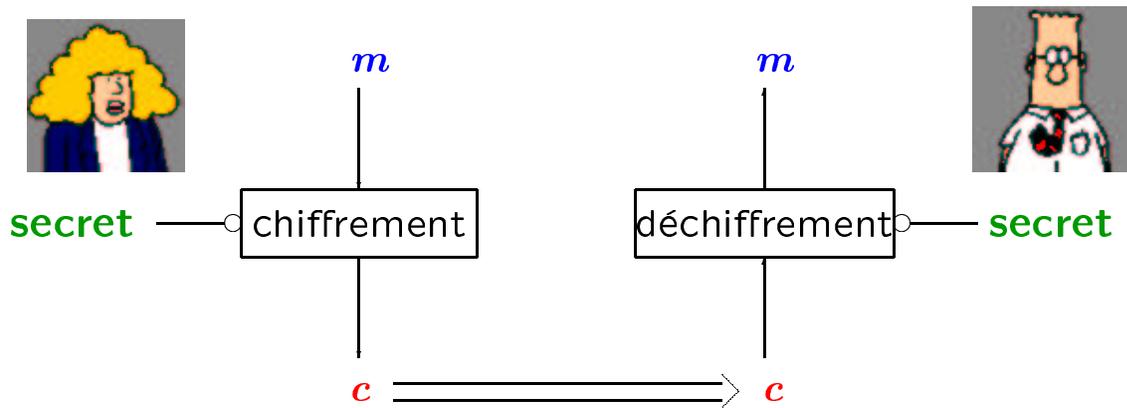
4

La cryptographie à clef secrète

5

Principe :

Emetteur et destinataire partagent un **même secret** qui leur permet de chiffrer et de déchiffrer.



6

Lettre de G. Sand à A. de Musset

Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir aussi vous dévoiler sans artifice mon âme toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde comme la plus étroite en amitié, en un mot la meilleure preuve que vous puissiez rêver, puisque votre âme est libre. Pensez que la solitude où j'habite est bien longue, bien dure et souvent difficile. Ainsi, en y songeant j'ai l'âme grosse. Accourez donc vite et venez me la faire oublier par l'amour où je veux me mettre.

7

Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir aussi vous dévoiler sans artifice mon âme toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde comme la plus étroite en amitié, en un mot la meilleure preuve que vous puissiez rêver, puisque votre âme est libre. Pensez que la solitude où j'habite est bien longue, bien dure et souvent difficile. Ainsi, en y songeant j'ai l'âme grosse. Accourez donc vite et venez me la faire oublier par l'amour où je veux me mettre.

8

Principes de Kerckhoffs (1883)

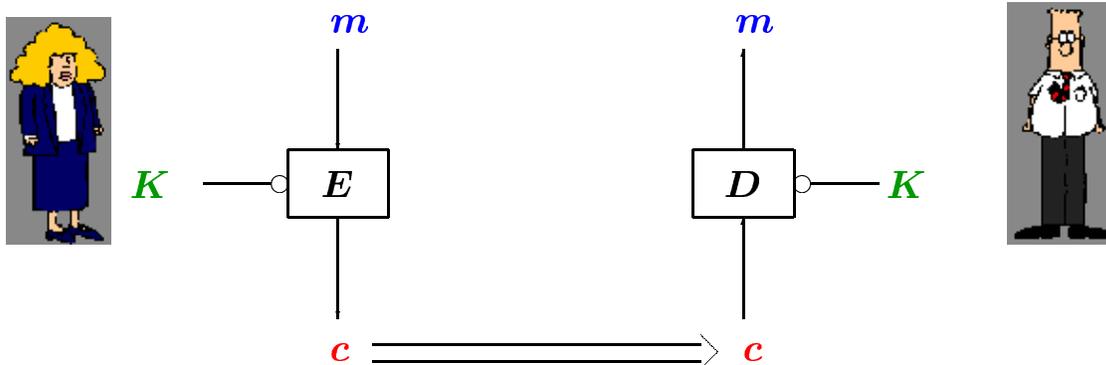
“Il faut bien distinguer entre un système d'écriture chiffré, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. [...]

Dans le second cas, [...] il faut que le système n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi. [...]

Si l'Administration veut mettre à profit tous les services que peut rendre un système de correspondance cryptographique bien combiné, elle doit absolument renoncer aux méthodes secrètes, et établir en principe qu'elle n'acceptera qu'un procédé qui puisse être enseigné au grand jour dans nos écoles militaires, que nos élèves seront libres de communiquer à qui leur plaira.”

9

Tous les détails du système, notamment les procédés de chiffrement et de déchiffrement, sont connus **sauf la valeur de la clef**.
La sécurité repose uniquement sur le secret de la clef.



10

Attaque d'un système de chiffrement

- L'attaquant connaît le texte chiffré c .
 \implies il veut retrouver le texte clair m ou mieux, la clef K .
- L'attaquant connaît des couples (texte clair, texte chiffré).
 \implies il veut retrouver la clef K ou au moins, pouvoir décrypter d'autres messages.

11

Substitution.

Remplacement des lettres du clair par d'autres lettres ou d'autres symboles en respectant l'ordre.

Système de Jules César

$$E_K : \{0, 1, \dots, 25\} \longrightarrow \{0, 1, \dots, 25\}$$
$$i \longmapsto (i + K) \bmod 26$$

$K = 3$, BRUTUS \mapsto EUXWXV

12

Substitutions alphabétiques

La clef est un mot quelconque. $K = \text{CRYPTANALYSE}$

On supprime les lettres en double : CRYPTANLSE

On rajoute à la suite, dans l'ordre alphabétique, toutes les lettres qui ne sont pas dans le mot.

On les écrit dans un tableau $3 * 9$

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

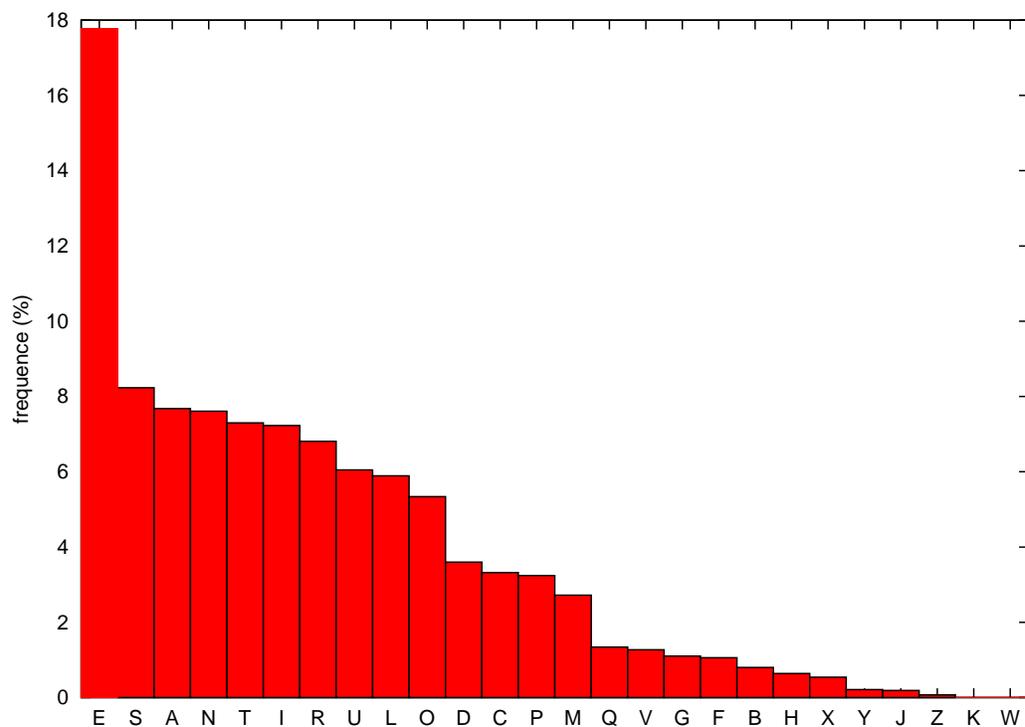
Le tableau lu colonne par colonne donne le nouvel alphabet.

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

13

nvxlbgi avxw n ctxnbw ubn dvttn r bhxqacyb
awbggbi rbn cueciwn lcnbn vqncxz rbn tbwn
hxq nxqlbgi qgrvubgin mvtacygvgn rb lvscy
ub gclqwb yuqncgi nxw ubn yvxooowbn ctbwn
c abqgb ubn vgi qun rbavnbn nxw ubn aucgmdbn
hxb mbn wvqn rb u ckxw tcucrwwqin bi dvgibxz
ucqnnbgi aqibxnbtdgi ubxwn ywcgrbn cqubn eucgmdbn
mvttb rbn clqwvgn iwcqgbw c mvib r bxz
mb lvscybxw cqub mvttb qu bni ycxmdb bi lbsub
uxq gcyxbwb nq ebcx hx qu bni mvtqhx b bi ucqr
u xg cycmb nvg ebn clbm xg ewxubyxbxub
u cxiwb tqtb bg evqicgi u qgoqwtb hxq lvucqi
ub avbib bni nbteuceub cx awqgmb rbn gxbbn
hxq dcgib uc ibtabib bi nb wqi rb u cwmdbw
bzqub nxw ub nvu cx tqubx rbn dxbbn
nbn cqubn rb ybcgi u btabmdbgi rb tcwmdbw

Fréquence des lettres en Français



Dans le chiffré :

B	N	C	U	X	Q	G	I	W	V
18,7	9,91	7,78	6,90	6,72	6,37	5,84	5,84	5,30	4,60

En Français :

E	S	A	N	T	I	R	U	L	O
17,8	8,23	7,68	7,61	7,30	7,23	6,81	6,05	5,89	5,34

B → E

N → S

C → A

16

svxlegi avxw s atxsew ues dvttes r ehxqaaye
aweggegi res aueaiwvs lasies vqseaxz res teww
hxq sxqlégi qgrvuegis mvtaaygvgs re lvsaye
ue galqwe yuqssagi sxw ues yvxoowes atews
a aeqge ues vgi qus reavses sxw ues auagmdes
hxe mes wvqs re u akxw tauarwvqis ei dvgiexz
uaqssegi aqixsetegi uexws ywagres aques euagmdes
mvtte res alqwvgs iwaqgew a mvie r exz
me lvsayexw aque mvtte qu esi yaxmde ei lexue
uxq gayxewe sq eeax hx qu esi mvtqhxe ei uaqr
u xg ayame svg eem alem xg ewxueyxexue
u axiwe tqte eg evqiagi u qgoqwte hxq lvuaqi
ue aveie esi seteuaeue ax awqgme res gxees
hxq dagie ua ietaeie ei se wqi re u awmdew
ezque sxw ue svu ax tqudex res dxees
ses aques re yeagi u etaemdegi re tawmdew

17

Bigrammes les plus fréquents dans le chiffré :

ES	UE	GI	RE	EG	EX	IE	SE	QU	TE	UA	EW	AG	AQ	HX	XW
25	17	13	12	9	8	8	8	8	8	8	7	7	7	7	7

Bigrammes les plus fréquents en Français :

ES	LE	EN	DE	RE	NT	ON	ER	TE	SE	ET	EL	QU	AN	NE	OU	AI
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

U → L

R → D

G → N

Q → I

18

Fréquence des bigrammes

Bigrammes les plus fréquents dans le chiffré :

ES	LE	NI	DE	EN	EX	IE	SE	IL	TE	LA	EW	AN	AI	HX	XW
25	17	13	12	9	8	8	8	8	8	8	7	7	7	7	7

Bigrammes les plus fréquents en Français :

ES	LE	EN	DE	RE	NT	ON	ER	TE	SE	ET	EL	QU	AN	NE	OU	AI
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

I → T

19

svxlent avxw s atxsew les dvttes d ehxiaaye
awennent des aleatwvs lastes viseaxz des teww
hxi sxilent indvlents mvtaaynvns de lvsaye
le naliwe ylissant sxw les yvxooowes atews
a aeine les vnt ils deavses sxw les alanmdes
hxe mes wwis de l akxw taladwvits et dvntexz
laissent aitexsetent lexws ywandes ailes elanmdes
mvtte des aliwvns twainew a mvte d exz
me lvsayexw aile mvtte il est yaxmde et lexle
lxi nayxewe si eeax hx il est mvtihxe et laid
l xn ayame svn eem alem xn ewxleyxexle
l axtwo tite en evitant l inoiwte hxi lvlait
le avete est setelaele ax awinme des nxees
hxi dante la tetaete et se wit de l awmdew
ezile sxw le svl ax tiliex des dxees
ses ailes de yeant l etaement de tawmdew

20

Quelques mots du chiffré :

indvlent vnt V → O

oiseaxz X → U

Z → X

a aeine A → P

leuws W → R

taladroits T → M

ygrandes Y → G

21

soulent pour s amuser les hommes d'equipage
prennent des aigles les oiseaux des mers
hui suilent indolents compagnons de voyage
le navire glissant sur les gouffres amers
a peine les ont ils deposes sur les planches
hue mes rois de l'air maladroits et doteux
laissent piteusement leurs grandes ailes etanchedes
comme des avions trainer a mort d'eux
me voyageur aile comme il est gauchet et leule
lui naguere si beau hui il est moche et laid
l'un agame son eem aile un eruleueule
l'autre mime en eotant l'oiseau hui l'olait
le poete est semelaele au prince des nees
hui dante la tempete et se rit de l'armee
exile sur le sol au milieu des nues
ses ailes de geant l'empechent de marcher

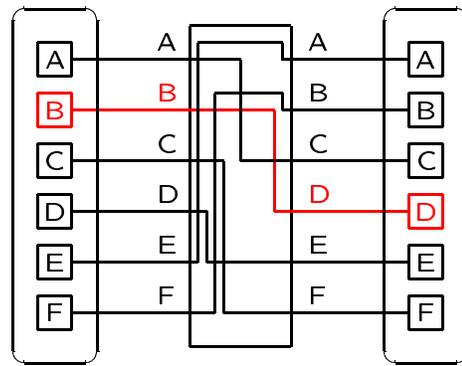
22

Enigma



source : <http://www.nsa.gov/museum/enigma.html>

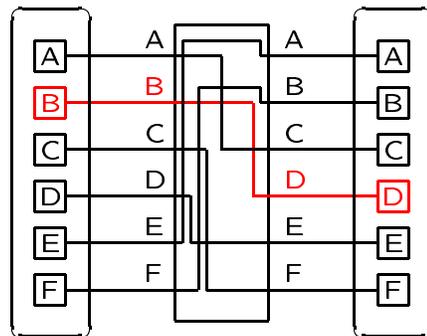
23



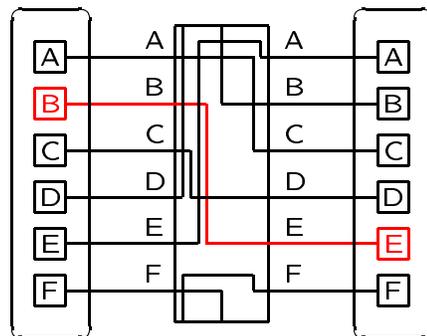
clavier rotor tableau lumineux

→ Substitution alphabétique.

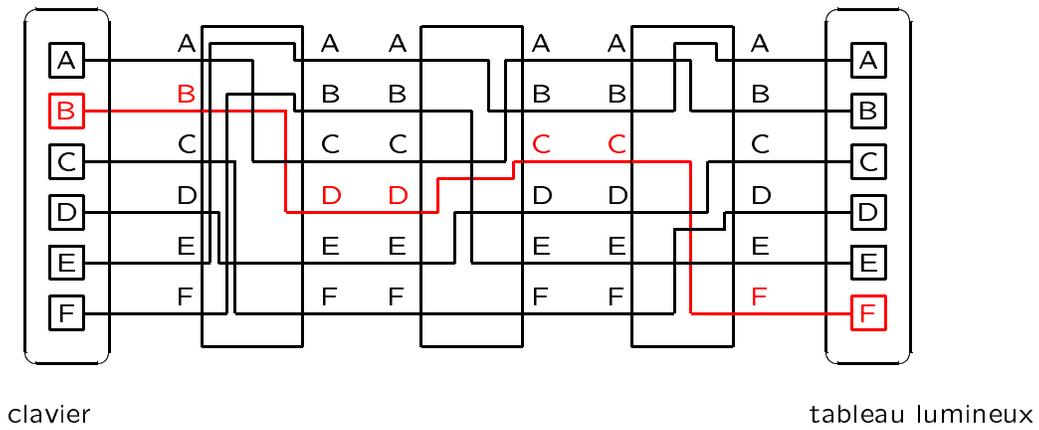
On tourne le rotor d'une position après chaque lettre



clavier rotor tableau lumineux



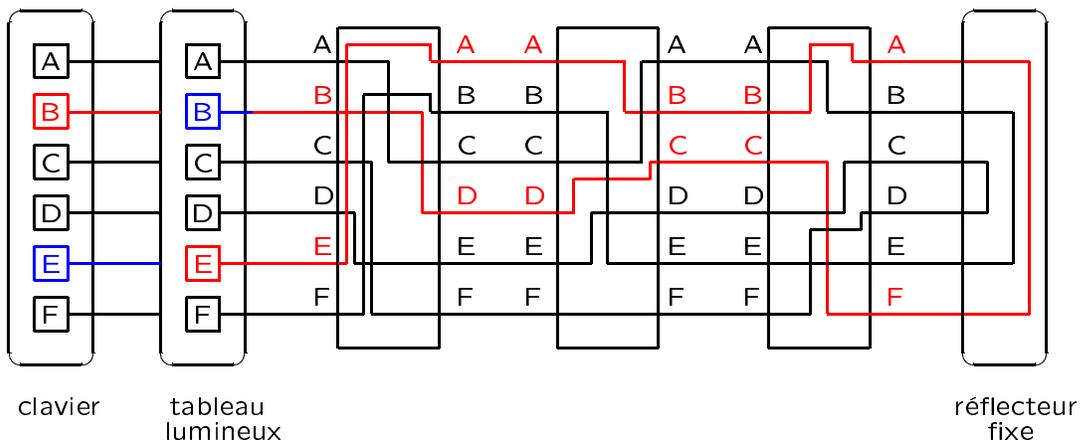
→ Substitution avec 26 alphabets différents.



→ Substitution avec 26^3 alphabets différents.

26

Machine à 3 rotors avec réflecteur

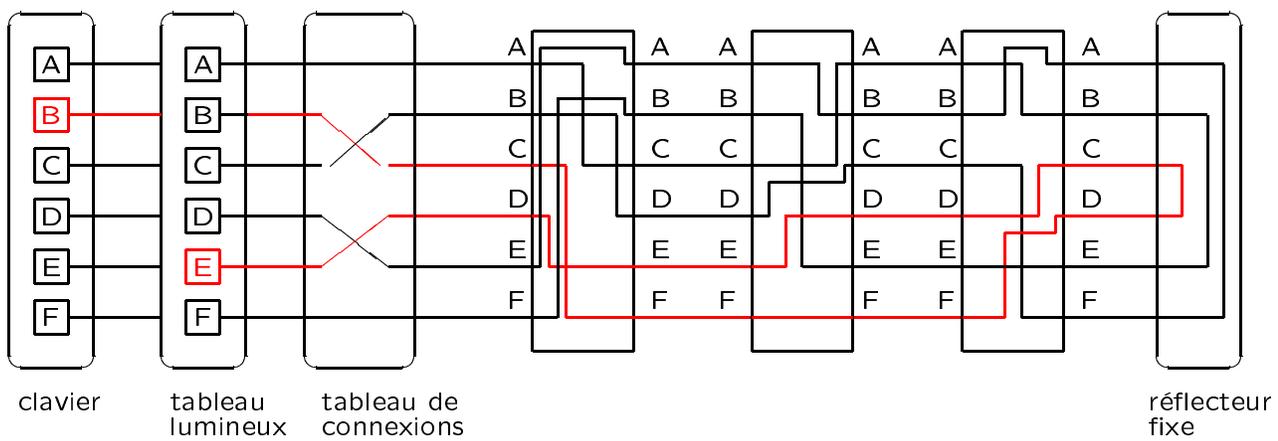


→ Le chiffrement et le déchiffrement sont les mêmes opérations.

Clef secrète : ordre des rotors + positions de départ des rotors.

$$6 \times (26)^3 = 105\,456 \text{ possibilités.}$$

27



Clef secrète :

ordre des rotors + positions des rotors + 6 couples de lettres transposées.

$$6 \times (26)^3 \times 100\,391\,791\,500 \simeq 10^{13} \text{ possibilités.}$$

28

Enigma au début de la guerre

Nombre de clefs secrètes

3 rotors choisis parmi 5	10 possibilités
Ordre des trois rotors	6 possibilités
Position initiale des rotors	$26^3 = 17\,576$ possibilités
Tableau de connexions (10 paires de lettres)	150 738 274 937 250 possibilités

$$\simeq 10^{20} \text{ possibilités}$$

Idée d'attaque [Rejewski 1939]

Dissocier la recherche des positions des rotors de celle des connexions en exploitant le fait que certains messages clairs sont connus.

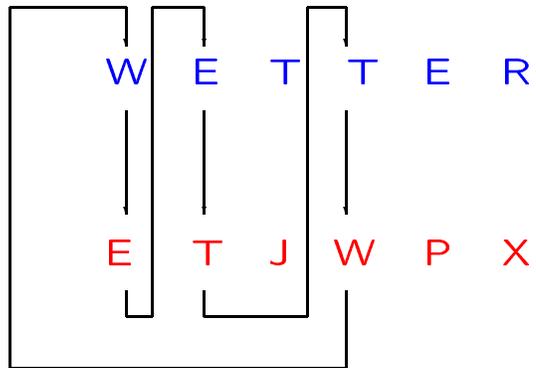
29

Principe.

On dispose d'un couple clair-chiffré.

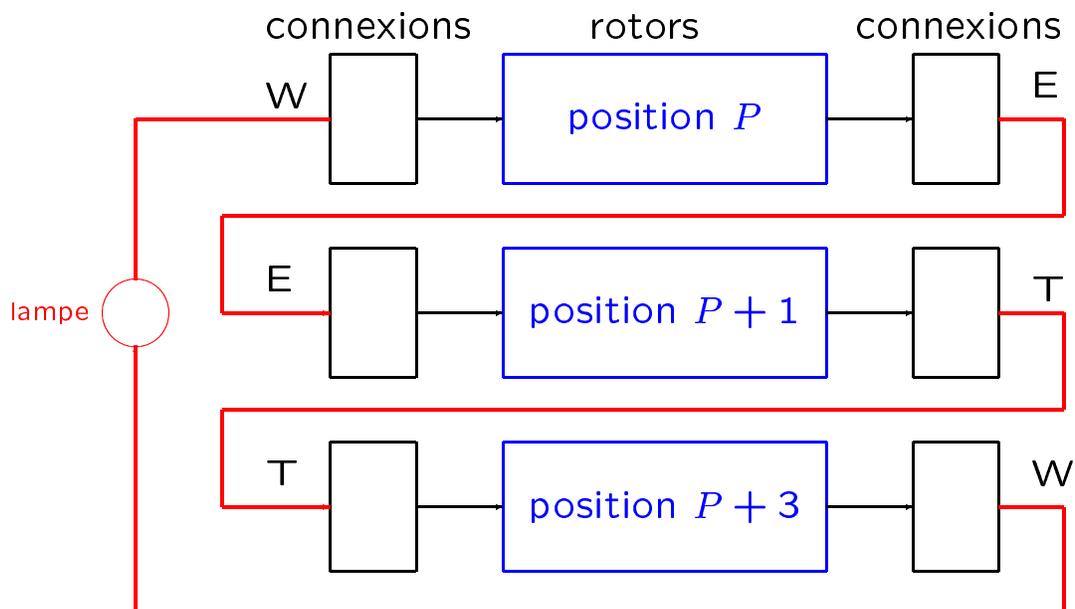
clair : WETTER chiffré : ETJWPX

On recherche des "boucles" au sein de ce message.

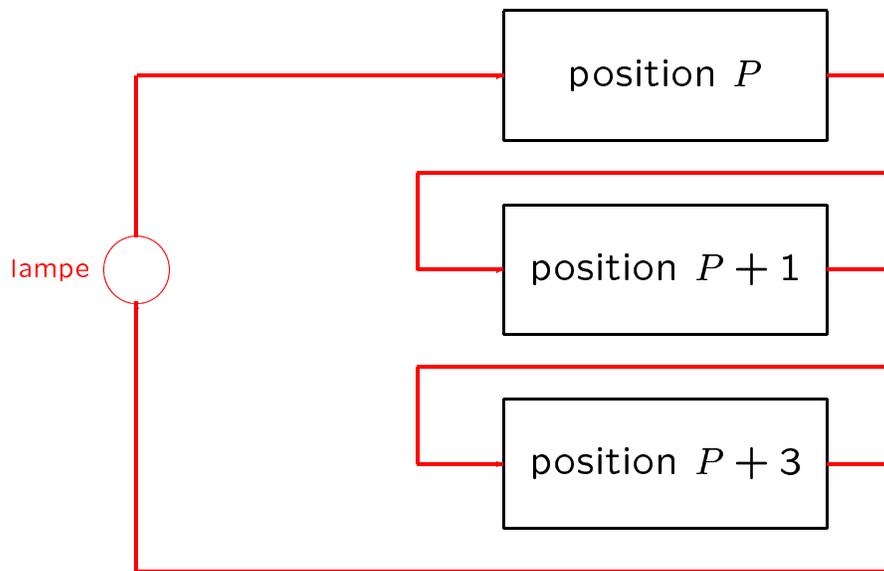


30

Recherche de la position des rotors



31



Il suffit d'essayer les $26^3 = 17\,576$ positions possibles pour chacun des 60 choix de rotors.

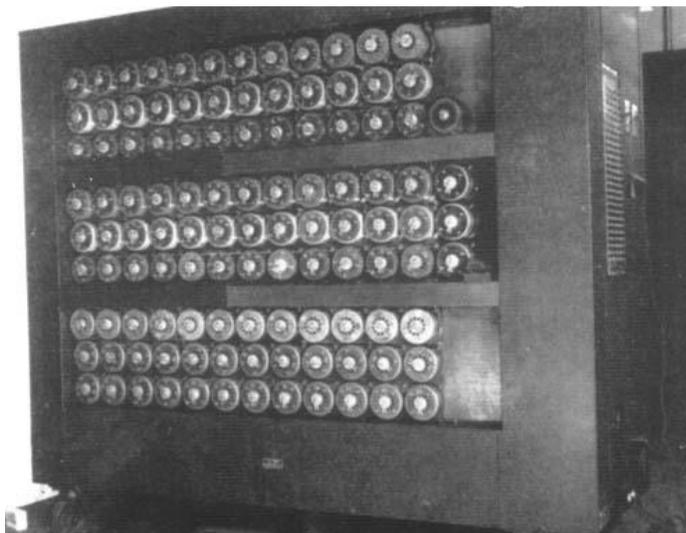
→ 1 054 560 possibilités.

32

Les bombes de Turing

Automatisation de la recherche de la clef secrète.

20 280 essais par seconde pour les plus rapides (50 secondes pour retrouver la clef).



source : <http://www.jharper.demon.co.uk/bombe1.htm>

33

Sécurité inconditionnelle

La connaissance du message chiffré n'apporte aucune information sur le message clair.

→ La seule attaque possible est la **recherche exhaustive de la clef secrète.**

34

Un système incassable : le chiffrement de Vernam (1926)

clair	s	y	s	t	e	m	e	i	n	c	a	s	s	a	b	l	e
	18	24	18	19	4	12	4	8	13	2	0	18	18	0	1	11	4
clef	g	v	w	q	t	y	s	k	r	g	s	e	d	l	w	p	m
	6	21	22	16	19	24	18	10	17	6	18	4	3	11	22	15	12
chiffré	24	19	14	9	23	10	22	18	4	8	18	22	21	11	23	0	16
	y	t	o	j	x	k	w	s	e	i	s	w	v	l	x	a	q

La clef est une suite aléatoire de lettres aussi longue que le clair.

35

clair s y s t e m e i n c a s s a b l e
clef g v w q t y s k r g s e d l w p m
chiffré y t o j x k w s e i s w v l x a q

clair a u c u n e i n f o r m a t i o n
clef y z m p k g j k r d e f j l e s c
chiffré y t o j x k w s e i s w v l x a q

Un même message chiffré peut correspondre à n'importe quel texte clair ayant le même nombre de lettres.

36

La sécurité en pratique

Sécurité inconditionnelle [Shannon 49]

Pour qu'un système soit inconditionnellement sûr, il faut que la clef secrète soit aussi longue que le texte clair.

→ Tous les autres systèmes sont théoriquement cassables.

Sécurité pratique

La connaissance du message chiffré (et de certains couples clairs-chiffrés) ne permet de retrouver ni la clef ni le message clair **en un temps humainement raisonnable**.

37

\mathcal{K} = nombre de clefs possibles.

Retrouver la clef nécessite en moyenne $\mathcal{K}/2$ essais.

Qu'est-ce qu'un temps humainement raisonnable ?

DES (standard U.S. de chiffrement 1977)

clef secrète : 56 bits $\longrightarrow 2^{56} \simeq 10^{17}$ possibilités.

39 jours sur 10 000 Pentium (réalisé en 1997)

2,5 jours sur une machine de moins de \$ 250 000 (1998)

Pour 1 million de \$, l'attaque prend 35 minutes.

Pour 10 millions de \$, l'attaque prend 3,5 minutes.

Actuellement, le nombre de clefs possibles doit être au moins de $2^{128} \simeq 10^{38}$ (clef de 128 bits)

Loi de Moore :

la puissance des ordinateurs double tous les 18 mois

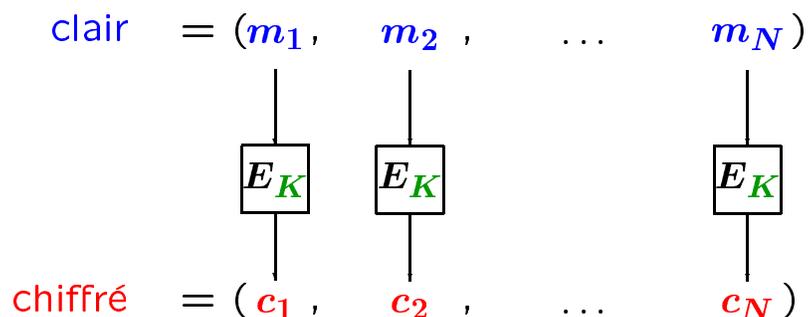
38

AES - Advanced Encryption Standard (2000)

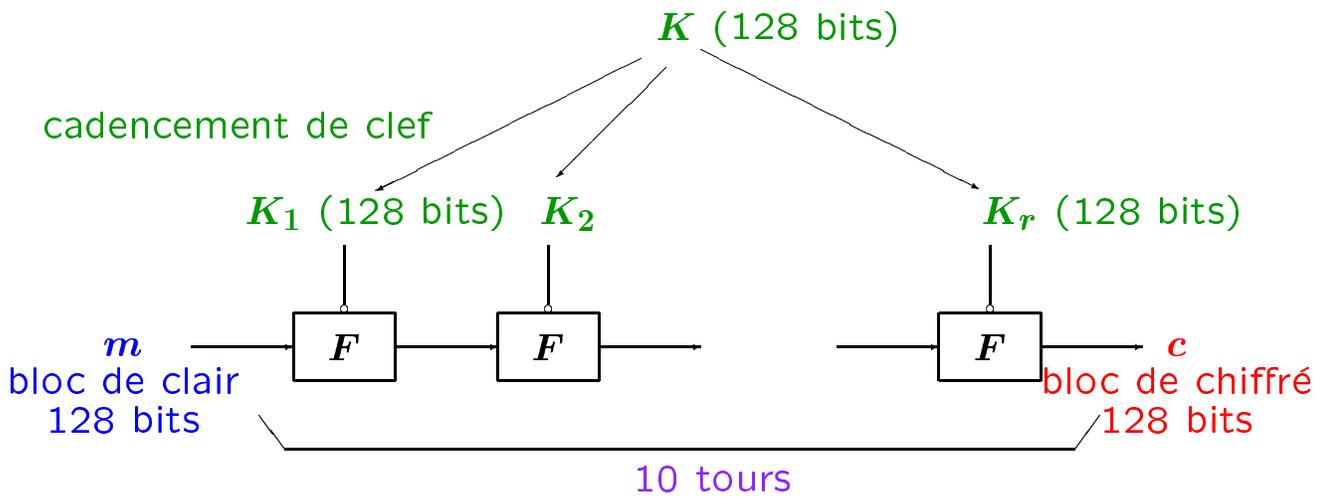
Taille de la clef : 128 /192 /256 bits

Le texte clair est découpé en blocs de 128 bits (16 caractères).

Le système chiffre les blocs successivement avec la même clef.

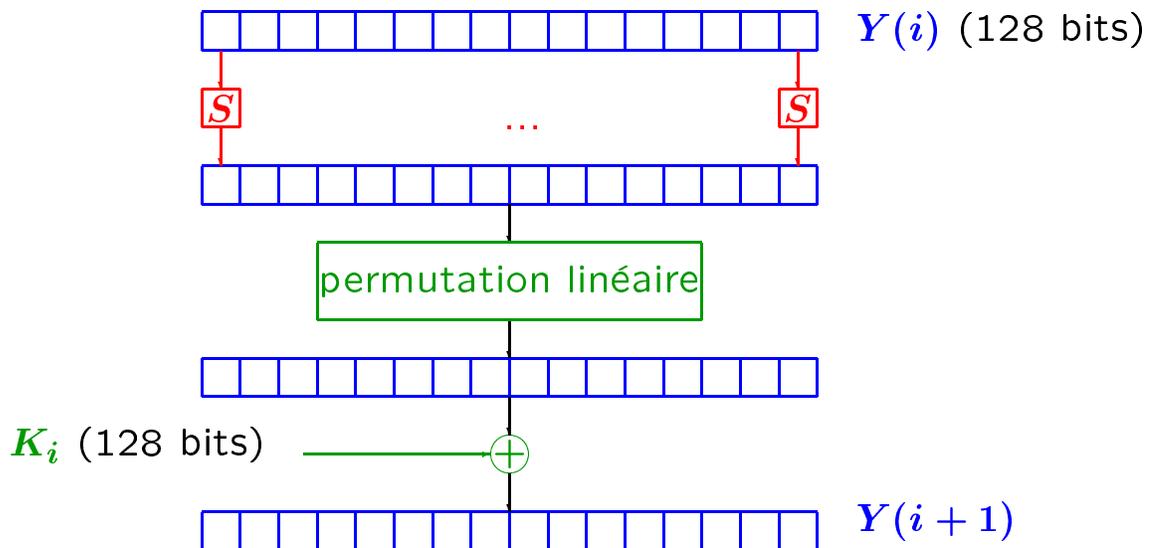


39



40

Fonction itérée de l'AES



S : inversion dans le corps fini à 2^8 éléments.

41

La cryptographie à clef publique

42

Fonctions à sens unique

$$f : x \mapsto f(x) = y$$

f est à sens unique si :

- étant donné x , il est facile de calculer $f(x)$.
- étant donné y , il est très difficile de calculer x .

très difficile = infaisable en un laps de temps réaliste avec une puissance de calcul raisonnable.

\implies De bonnes fonctions à sens unique sont des fonctions telles que la recherche de x à partir de $f(x)$ est un problème mathématique réputé difficile.

43

Notons $\mathbb{Z}/p\mathbb{Z}$ l'anneau des entiers modulo p , $\mathbb{Z}/p\mathbb{Z} = \{0, \dots, p-1\}$.
 Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$

$$f_{a,p}: (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ x \longmapsto a^x \bmod p$$

Exemple.

$$f: \{1, \dots, 540\} \longrightarrow \{1, \dots, 540\} \\ x \longmapsto 2^x \bmod 541$$

$$f(10) = 2^{10} \bmod 541 = 1024 \bmod 541 = 483$$

44

Les entiers modulo p

Proposition

$\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Proposition

Soit p un entier premier. Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique :

il existe $g \in (\mathbb{Z}/p\mathbb{Z})^*$, appelé **élément générateur**, tel que

$$(\mathbb{Z}/p\mathbb{Z})^* = \{g^0, g^1, g^2, \dots, g^{p-2}\}$$

Exemple.

$g = 3$ est un générateur de $(\mathbb{Z}/7\mathbb{Z})^*$:

$$\{3^i \bmod 7, 0 \leq i < 7\} = \{1, 3, 2, 6, 4, 5\}$$

45

Théorème

Soit p un entier premier et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.
La fonction

$$\begin{aligned} f : (\mathbb{Z}/p\mathbb{Z})^* &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ x &\longmapsto g^x \bmod p \end{aligned}$$

est bijective.

Exemple.

$$\begin{aligned} f : \{1, \dots, 540\} &\longrightarrow \{1, \dots, 540\} \\ x &\longmapsto 2^x \bmod 541 \end{aligned}$$

46

Calcul de $f(x) = g^x \bmod p$

On décompose x en base 2 :

$$x = 19 = 2^4 + \quad + \quad + 2^1 + 2^0 = (10011)_2 = (x_4, \dots, x_0)_2$$

Au départ, $y = 1$.

- Si $x_i = 0$, $y \longleftarrow y^2 \bmod p$.
- Si $x_i = 1$, $y \longleftarrow y^2 \cdot g \bmod p$.

$$\begin{aligned} y &= (1^2) \cdot g \\ y &= ((1^2) \cdot g)^2 \\ y &= (((1^2) \cdot g)^2)^2 \\ y &= (((((1^2) \cdot g)^2)^2)^2) \cdot g \\ y &= ((((((1^2) \cdot g)^2)^2)^2) \cdot g)^2 \cdot g \end{aligned}$$

$$\left(((((((1) \cdot g)^2)^2)^2) \cdot g)^2 \cdot g \right)^2 \cdot g = \left(g^{2^3+1} \right)^2 \cdot g = g^{2^4+2+1}$$

→ Calcul linéaire en la taille de x .

47

Trouver $x \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $g^x \bmod p = y$.

Exemple. Trouver x tel que $2^x = 69 \bmod 541$?

48

Le logarithme discret

Trouver $x \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $g^x \bmod p = y$.

Exemple. Trouver x tel que $2^x = 69 \bmod 541$?

$$2^{280} \bmod 541 = 58$$

$$2^{290} \bmod 541 = 423$$

$$2^{300} \bmod 541 = 352$$

49

Trouver $x \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $g^x \bmod p = y$.

Exemple. Trouver x tel que $2^x = 69 \bmod 541$?

$$2^{280} \bmod 541 = 58$$

$$2^{290} \bmod 541 = 423$$

$$2^{300} \bmod 541 = 352$$

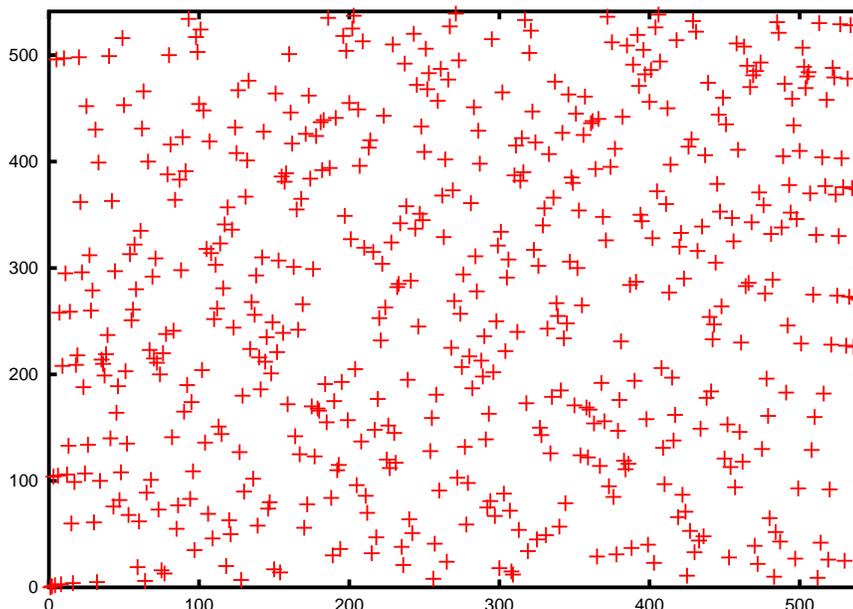
$$2^{292} \bmod 541 = 69$$

50

Le logarithme discret

Trouver x tel que $2^x = 69 \bmod 541$?

Logarithme en base 2 dans les entiers modulo 541

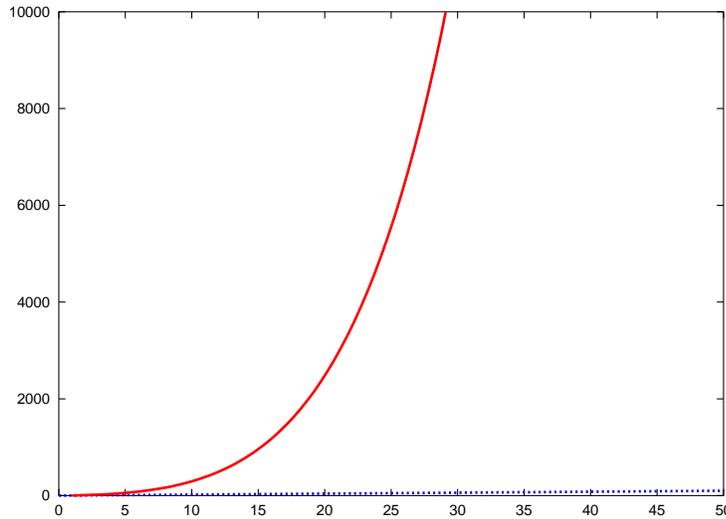


51

Algorithme du crible du corps de nombres [Gordon-Shirokauer 93]
Complexité.

$$\mathcal{O}\left(\exp(2(\log p)^{\frac{1}{3}}(\log \log p)^{\frac{2}{3}})\right)$$

Record. p : nombre de 120 chiffres décimaux [Joux-Lercier 01].



52

Protocole d'échange de clefs de Diffie-Hellman (1976)

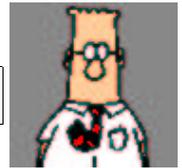
Soit p un entier premier d'au moins 230 chiffres (768 bits)
 et g un générateur de $\{1, \dots, p-1\}$.



choisit $x_A \in (\mathbb{Z}/p\mathbb{Z})^*$

$$y_A = g^{x_A} \bmod p$$

$$K = (y_B)^{x_A} \bmod p$$



choisit $x_B \in (\mathbb{Z}/p\mathbb{Z})^*$

$$y_B = g^{x_B} \bmod p$$

$$K = (y_A)^{x_B} \bmod p$$

$$K = (y_A)^{x_B} \bmod p = g^{x_A x_B} \bmod p = (y_B)^{x_A} \bmod p$$

53

$$p = 541 \text{ et } g = 2$$

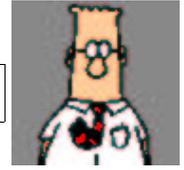


choisit 292

$$2^{292} \bmod 541 = 69$$

69

171



choisit 426

$$2^{426} \bmod 541 = 171$$

$$(171)^{292} \bmod 541 = 368$$

$$(69)^{426} \bmod 541 = 368$$

54

Sécurité du protocole de Diffie-Hellman

Retrouver le secret commun K revient à résoudre le problème suivant :

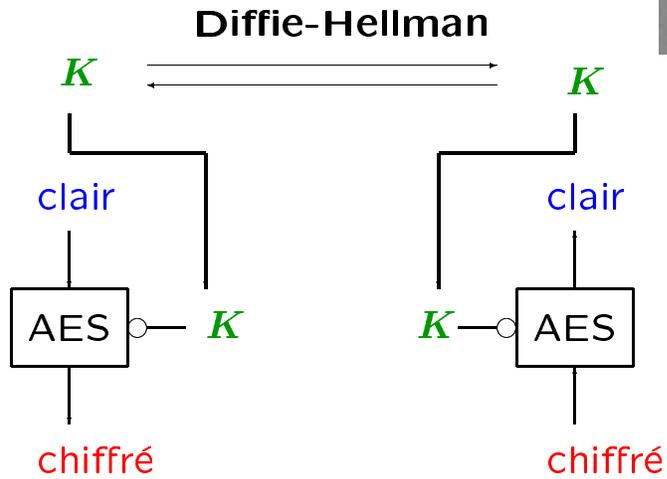
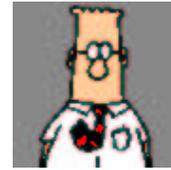
Problème de Diffie-Hellman :

Soit p un entier premier et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.
Étant données les valeurs de $(g^a \bmod p)$ et de $(g^b \bmod p)$,
calculer $g^{ab} \bmod p$.

Problème ouvert :

Peut-on résoudre le problème de Diffie-Hellman sans résoudre celui du logarithme discret modulo p ?

55



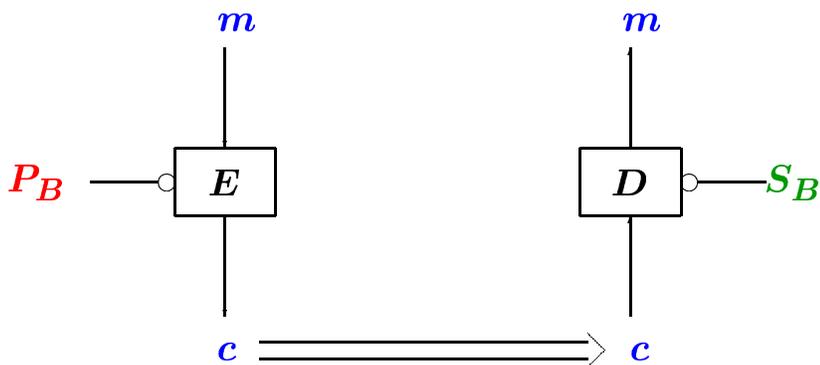
56

Le chiffrement à clef publique

Principe.

Chaque utilisateur dispose d'une **clef publique** P (disponible dans un annuaire) et d'une **clef privée** S .

⇒ pas de secret partagé.



57

Clef secrète : coffre-fort

Clef publique : boîte aux lettres

Alice et Bob ont la clef du coffre. Seul Bob a la clef de sa boîte.

Alice envoie un message à Bob : Alice envoie un message à Bob :

1. Alice utilise la clef pour déposer un courrier dans le coffre.
 2. Bob utilise la clef pour lire le courrier déposé par Alice.
1. Alice cherche l'adresse de Bob dans un annuaire et dépose un courrier dans la boîte de Bob.
 2. Bob utilise sa clef pour lire le courrier déposé dans sa boîte.

Propriétés du coffre-fort :

- seuls Alice et Bob peuvent déposer du courrier dans le coffre.
- seuls Alice et Bob peuvent lire le courrier déposé dans le coffre.

Propriétés :

- toute personne peut envoyer du courrier à Bob.
- seul Bob peut lire le courrier déposé dans sa boîte aux lettres.

58

Fonctions à sens unique avec trappe

$$f : x \mapsto f(x) = y$$

f est à sens unique avec trappe si :

- étant donné x , il est facile de calculer $f(x)$.
- étant donné y , il est très difficile de calculer x sauf si on connaît une trappe s .

59

Soit p et q deux entiers premiers, $n = pq$.

Soit e un entier inférieur à n , premier avec $(p - 1)(q - 1)$.

$$\begin{aligned} f_{e,n} : \{0, \dots, n - 1\} &\longrightarrow \{0, \dots, n - 1\} \\ x &\longmapsto x^e \bmod n \end{aligned}$$

Le calcul de $f_{e,n}(x)$ est linéaire en la taille de n .

60

Un peu d'arithmétique...

Théorème [Fermat]

Soit p un entier premier.

$$\forall x \in \{1, \dots, p - 1\}, \quad x^{p-1} \equiv 1 \pmod{p}$$

$\forall x \neq 0$, la multiplication par x est une bijection de $\{1, \dots, p - 1\}$.

$$\begin{aligned} \prod_{i=1}^{p-1} (xi \bmod p) &= \prod_{i=1}^{p-1} i \\ \implies x^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \end{aligned}$$

Comme $\text{pgcd}((p - 1)!, p) = 1$, on a

$$x^{p-1} \equiv 1 \pmod{p}$$

Corollaire

Soient p et q deux nombres premiers distincts.

$$\forall \lambda \equiv 1 \pmod{(p - 1)(q - 1)}, \quad \forall x, \quad x^\lambda \equiv x \pmod{pq}$$

61

Problème.

Soit $n = pq$ où p et q sont deux entiers premiers.

Soit $e \in \{1, \dots, n-1\}$ premier avec $(p-1)(q-1)$ et $y \in \{1, \dots, n-1\}$.

Trouver $x \in \{1, \dots, n-1\}$ tel que $x^e \bmod n = y$.

Quand on connaît p et q :

On cherche un couple de Bezout pour e et $(p-1)(q-1)$:

(a, b) tel que $ae + b(p-1)(q-1) = 1$ (algorithme d'Euclide).

Pour $d = a \bmod (p-1)(q-1)$, on a

$$ed \equiv 1 \pmod{(p-1)(q-1)} .$$

Alors, pour tout $x \in \{1, \dots, n-1\}$, on a

$$y^d \bmod n = (x^e)^d \bmod n = x^{ed} \bmod n = x^{1+k(p-1)(q-1)} = x .$$

\implies On peut retrouver x en un temps polynômial en la taille de n .

62

Exemple

$p = 127$, $q = 179$ ($n = pq = 22733$) et $e = 17$.

Trouver x tel que $x^{17} \bmod 22733 = 18763$?

On cherche d tel que $17d \equiv 1 \pmod{(p-1)(q-1)}$.

$$22428 - 1319 \times 17 = 5$$

$$17 - 3 \times 5 = 2$$

$$5 - 2 \times 2 = 1$$

$$5 - 2 \times 2 = 1$$

$$5 - 2 \times (17 - 3 \times 5) = 1$$

$$7 \times 5 - 2 \times 17 = 1$$

$$7 \times (22428 - 1319 \times 17) - 2 \times 17 = 1$$

$$7 \times 22428 - 9235 \times 17 = 1$$

$$-10 \times 22428 + (22428 - 9235) \times 17 = 1 \implies d = 13193$$

$$(x^{17})^{13193} = x \cdot x^{10 \cdot 22428} = x \bmod 22733$$

$$x = 18763^{13193} \bmod 22733 = 17564 .$$

63

Soit $n = pq$ où p et q sont deux entiers premiers.

Soit $e \in \{1, \dots, n-1\}$ premier avec $(p-1)(q-1)$ et $y \in \{1, \dots, n-1\}$.

Trouver $x \in \{1, \dots, n-1\}$ tel que $x^e \bmod n = y$.

Quand on ne connaît pas p et q :

La méthode connue la plus efficace pour retrouver x consiste à chercher d tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Pour celà, il faut trouver les deux facteurs premiers p et q de n .

64

La factorisation

Défi de Pour la Science (1977)

Le nombre

114 381 625 757 888 867 669 235 779 976 146 612 010 218 296
721 242 362 562 561 842 935 706 935 245 733 897 830 597 123
563 958 705 058 989 075 147 599 290 026 879 543 541

est le produit de 2 nombres premiers. Lesquels ?

65

Défi de Pour la Science (1977)

Le nombre

114 381 625 757 888 867 669 235 779 976 146 612 010 218 296
721 242 362 562 561 842 935 706 935 245 733 897 830 597 123
563 958 705 058 989 075 147 599 290 026 879 543 541

est le produit de 2 nombres premiers. Lesquels ?

Réponse [Atkins, Graff, Lenstra, Leyland 95]

3 490 529 510 847 650 949 147 849 619 903 898 133 417 764
638 493 387 843 990 820 577

et

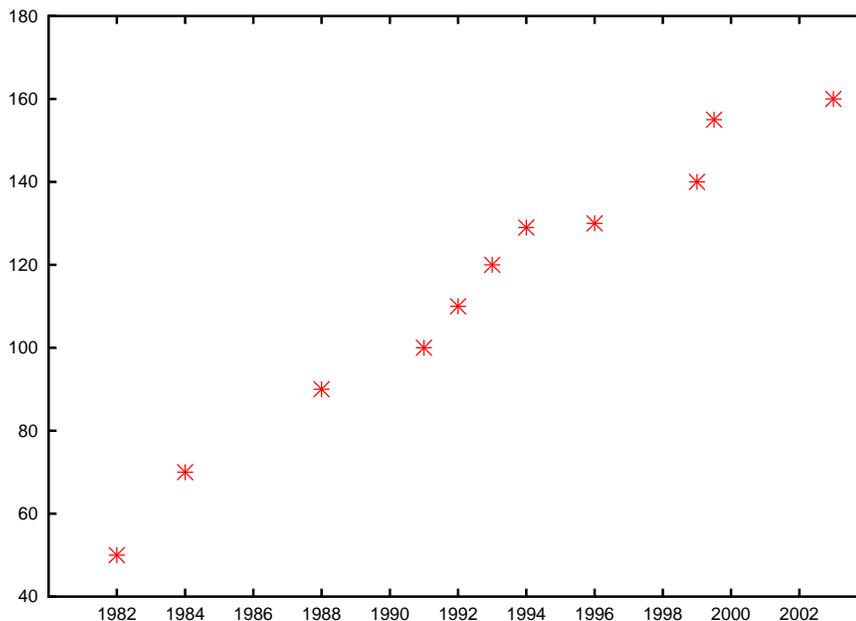
32 769 132 993 266 709 549 961 988 190 834 461 413 177 642
967 992 942 539 798 288 533

8 mois de calcul faits par 600 volontaires dans 20 pays
et 45 heures sur une machine massivement parallèle.

66

Records de factorisation [F. Morain]

Evolution du nombre de chiffres décimaux des nombres factorisés
au cours des années.



67

Factoriser le nombre suivant de 174 chiffres (576 bits)

188 198 812 920 607 963 838 697 239 461 650 439 807 163 563
379 417 382 700 763 356 422 988 859 715 234 665 485 319 060
606 504 743 045 317 388 011 303 396 716 199 692 321 205 734
031 879 550 656 996 221 305 168 759 307 650 257 059

Prix : 10 000 \$.

<http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html>

68

Le chiffrement RSA [Rivest - Shamir - Adleman 78]

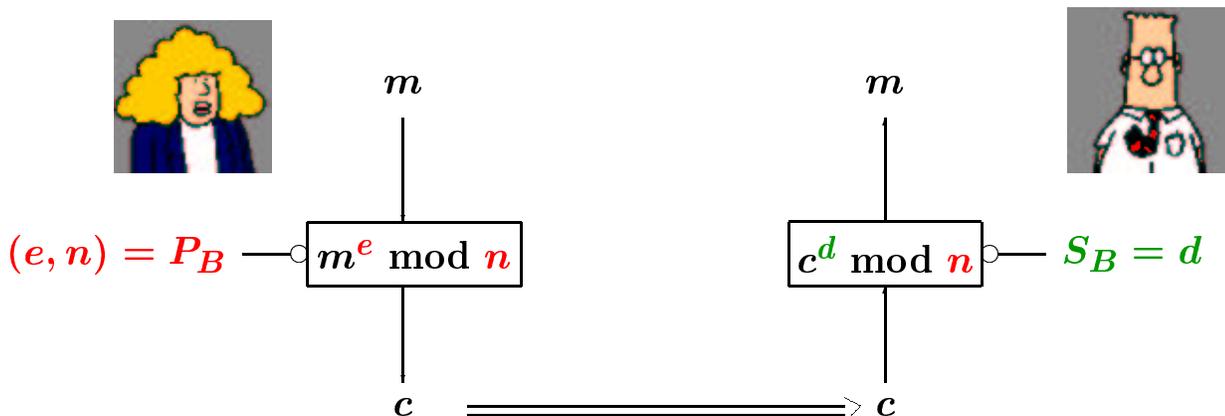
Principe :

Bob choisit deux grands nombres premiers p et q

et un entier e premier avec $(p - 1)(q - 1)$.

Il calcule $n = pq$ et d tel que $ed \bmod (p - 1)(q - 1) = 1$.

\Rightarrow clef publique = (e, n) , clef privée = d



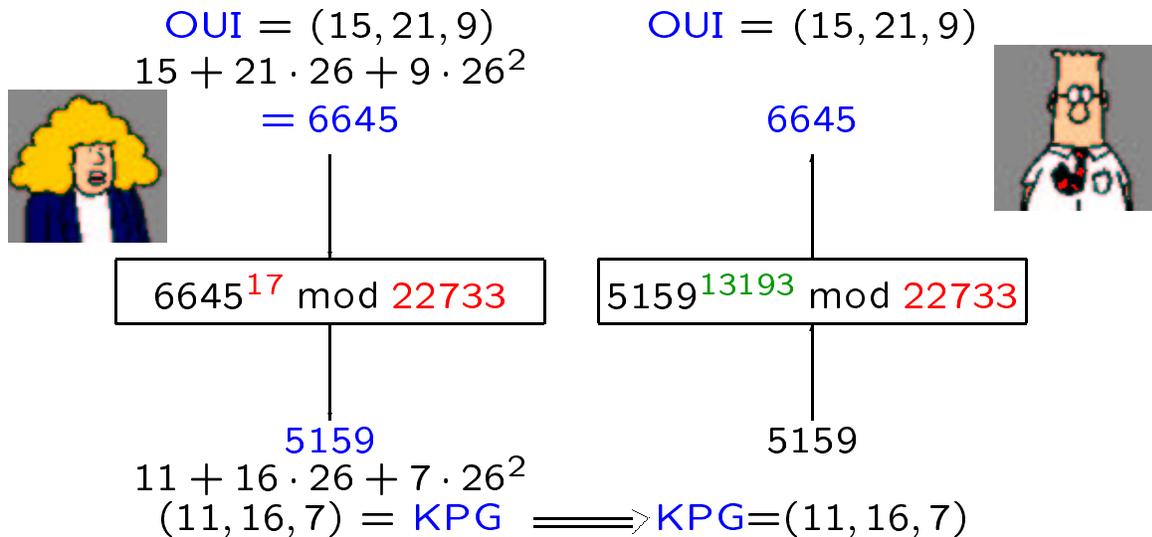
69

Bob choisit $p = 127$ et $q = 179$ et $e = 17$.

Il calcule $n = pq = 22733$

et d tel que $17d \bmod (p-1)(q-1) = 1 \implies d = 13193$

\implies clef publique = $(17, 22733)$, clef privée = $d = 13193$



70

Remarques sur la taille des clefs

- Chiffrement à clef secrète avec une clef de k bits

Recherche exhaustive parmi tous les mots de k bits
 $= 2^{k-1}$ essais en moyenne.

\implies Longueur de clef recommandée : 128 bits.

- RSA avec une clef privée de k bits

Factorisation d'un nombre de k bits $\ll 2^{k-1}$ essais

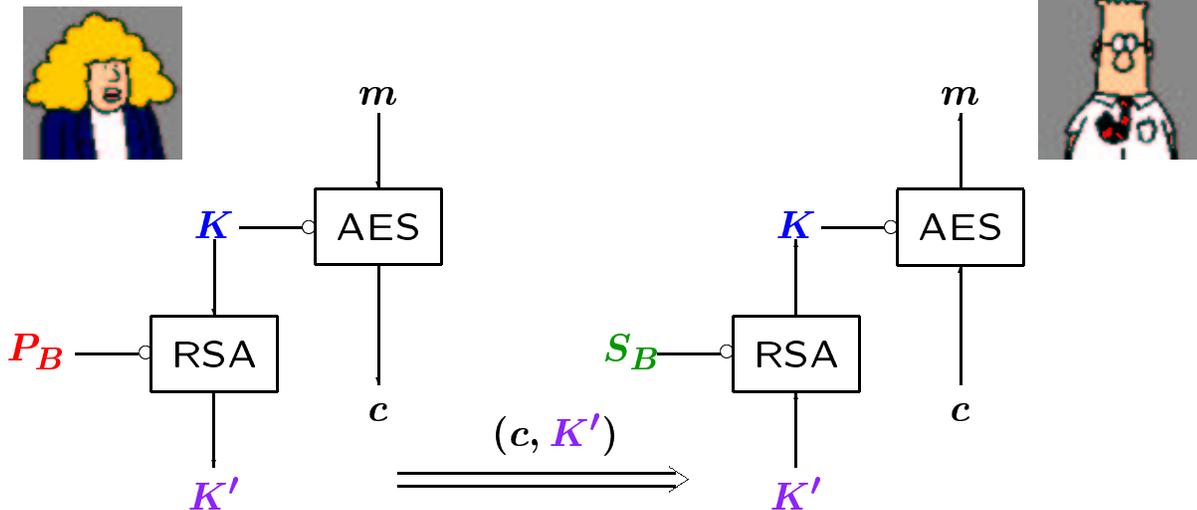
\implies Longueur de clef recommandée : 768 ou 1024 bits.

71

	clef secrète	clef publique
gestion	la clef est secrète aux 2 extrémités. grand nombre de clefs dans un réseau	seule la clef privée est secrète. garantie de l'authenticité des clefs publiques
sécurité	pas de preuve formelle de sécurité	repose sur la difficulté (supposée) de problèmes mathématiques
performances	très rapides 10-100 Mbits/s	très lents 10-100 Kbits/s

72

Systemes de chiffrement hybrides



73

Principe :

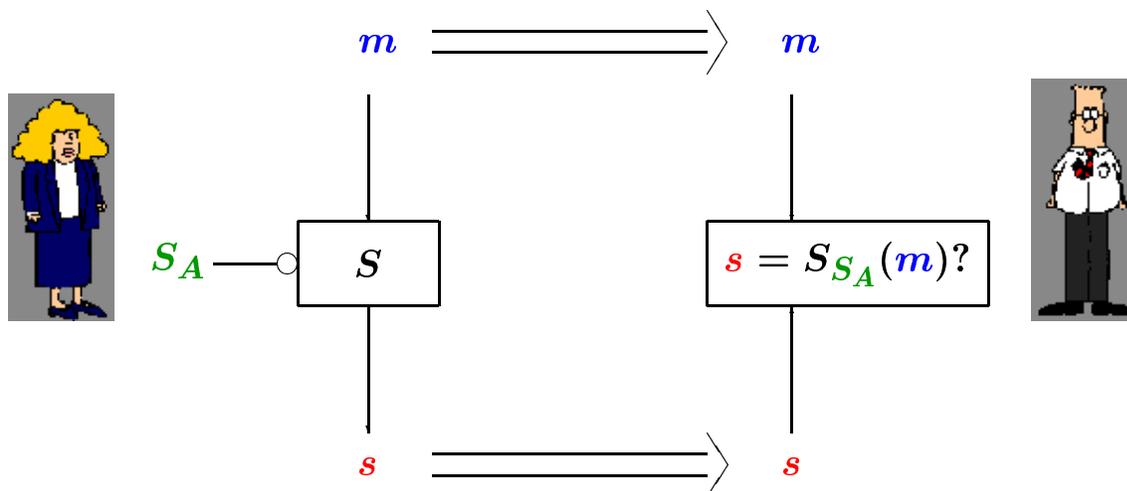
Alice envoie à Bob un message clair m et lui associe une signature s .

Propriétés requises :

- La signature s ne peut pas être contrefaite
→ **identification du signataire.**
- La signature s n'est pas réutilisable.
- Le message signé est inaltérable
→ **authentification du message.**
- Alice ne peut pas nier avoir signé le message
→ **non-répudiation.**

74

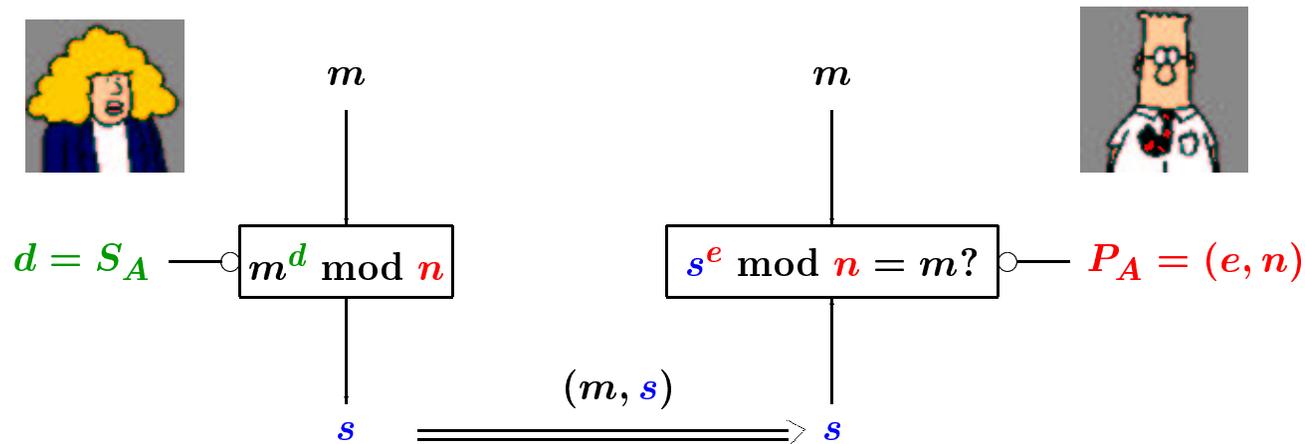
La signature numérique



Seule la personne qui connaît la clef S_A est capable de produire la signature.

75

Soit (e, n) la clef publique d'Alice et d sa clef secrète.



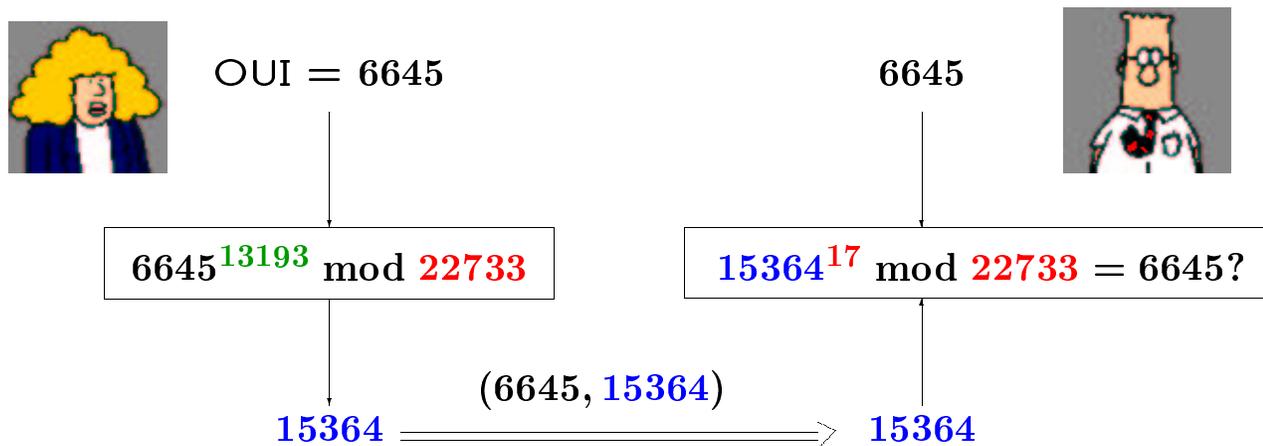
\Rightarrow Seul celui qui connaît d peut produire s .

76

La signature RSA : exemple

Clef publique d'Alice = $(17, 22733)$

Clef privée d'Alice = 13193 .



\Rightarrow Seule Alice est capable de trouver s tel que

$$s^{17} \bmod 22733 = 6645 .$$

77

Chiffrement à clef secrète

- conception de nouvelles attaques ;
- élaboration de preuves de sécurité et définition de critères de sécurité ;
- construction de nouveaux systèmes de chiffrement à clef secrète.

Cryptographie à clef publique

- étude de la complexité de la factorisation et du logarithme discret.
- recherche de nouveaux algorithmes à clef publique fondés sur d'autres problèmes et plus rapides que les algorithmes existants.

Autres fonctionnalités cryptographiques

protection des droits d'auteurs ; protocoles complexes.

78

Eléments bibliographiques

Aspects historiques

- S. Singh. *Histoire des codes secrets*. Jean-Claude Lattès, 1999.
- J. Stern. *La science du secret*. Odile Jacob, 1996.
- D. Kahn. *Codebreakers, revised edition*. Ed. Charles Scribner, 1996.

Ouvrages de référence

- A.J. Menezes, P.C. van Oorschot, et S.A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.
Disponible gratuitement sur <http://cacr.math.uwaterloo.ca/hac/>.
- B. Schneier. *Applied Cryptography*. Wiley Inc., 1996.

79