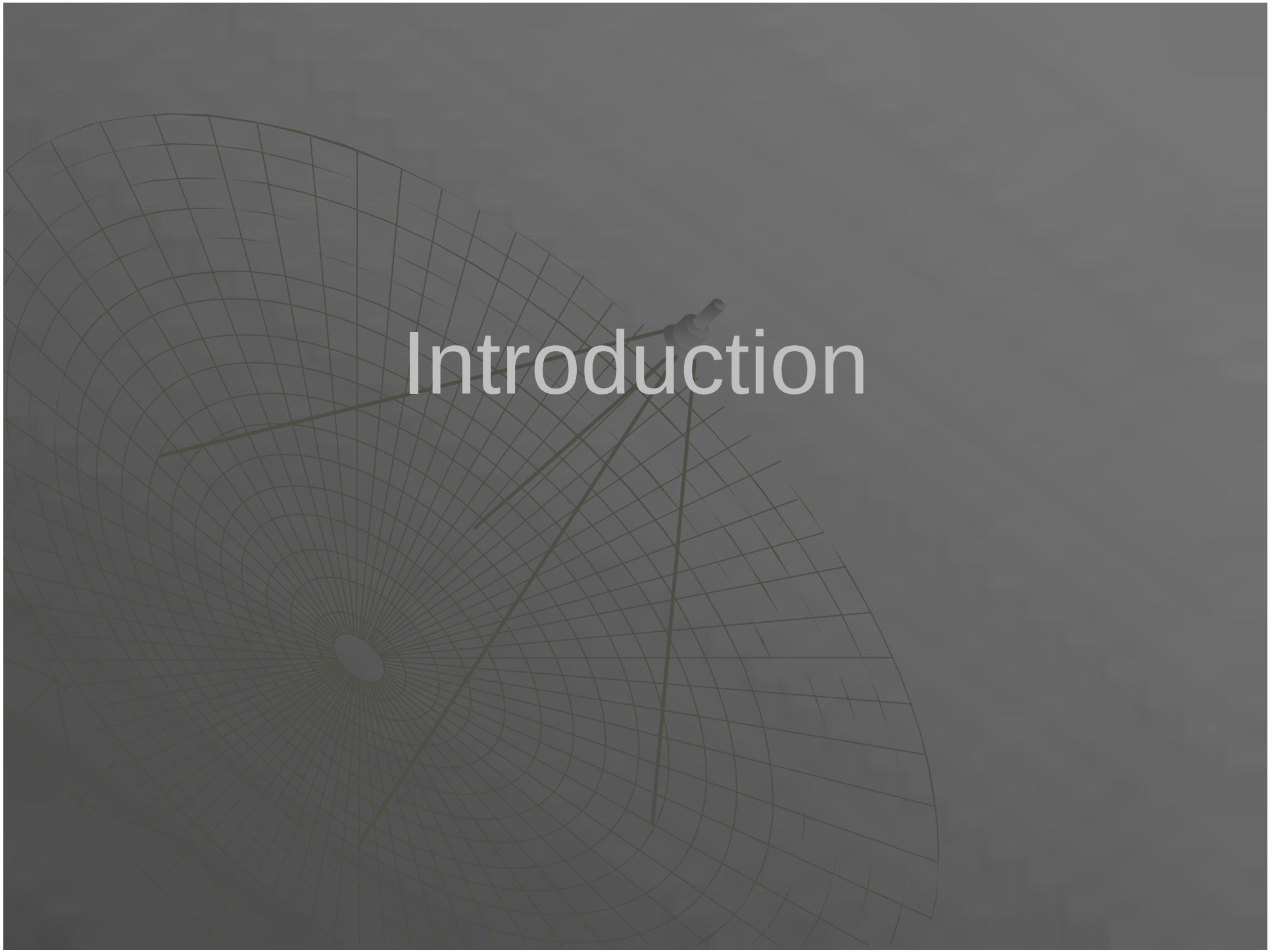
Cryptographie

Dr. Jean-Philippe Préaux
CReA/Univ. de Provence
30 mai 2007

PLAN :

- 0 - Introduction
- I - Histoire de la cryptographie
- II - Cryptographie moderne
- III - Cryptographie à venir


Introduction

- Cryptographie : *cryptos graphein,* « écriture cachée ». Désigne l'art de dissimuler le contenu d'un message.

- Cryptographie : *cryptos graphein,* « écriture cachée ». Désigne l'art de dissimuler le contenu d'un message.
- Ses origines sont ancestrales. Selon l'historien grec Plutarque elle serait née à Sparte au Vème siècle av. JC.

  Pour transmettre des messages confidentiels entre les magistrats de la cité et les généraux en campagne les spartiates utilisaient des *scytales* : deux bâtons de même diamètre, et un ruban pour colporter le message.

- La cryptographie s'est développée en domaine d'étude mathématique.
- *Cryptologie :* éthymologiquement 'science du secret', est le domaine des mathématiques constitué de :
  - *Cryptographie :* développement des algorithmes de cryptage/décryptage.
  - *Cryptanalyse :* Etude de la fiabilité des algorithmes de cryptographie.

- La cryptographie s'est développée en domaine d'étude mathématique.
- *Cryptologie :* éthymologiquement 'science du secret', est le domaine des mathématiques constitué de :
  - *Cryptographie :* développement des algorithmes de cryptage/décryptage.
  - *Cryptanalyse :* Etude de la fiabilité des algorithmes de cryptographie.
- Initialement de motivation d'origine militaire, les progrès technologiques en matière de réseau de communication ont propulsé la cryptologie au premier plan des domaines d'application des mathématiques que ce soit dans le domaine civil ou militaire.

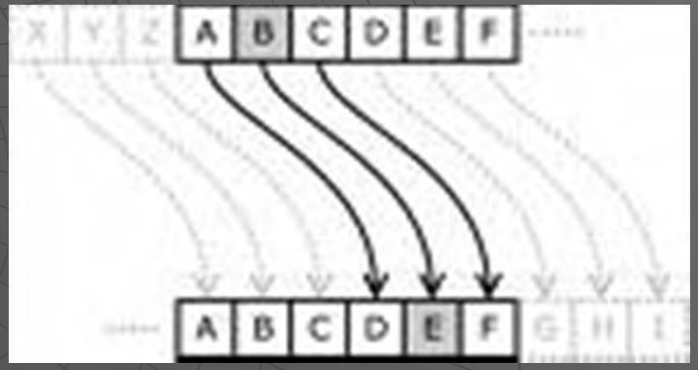
I - Histoire de la cryptographie

- Le chiffrement de César
- Substitution mono-alphabétique
- Les fréquences d'Al Kindi
- Le code de Vigenère
- Test de Kasiski
- La machine Enigma
- Cryptanalyse d'Enigma
- Le code de Vernam
- Application : le téléphone rouge
- Chronologie

Le chiffrement de César

- Durant la guerre des Gaules, César imagine une méthode de chiffrement pour communiquer avec ses généraux : le chiffrement de César. Cela consiste à décaler chaque lettre dans l'alphabet de N rangs à droite.

  N est la clef (privée) ; elle est nécessaire au cryptage et (à priori) au décryptage. Elle ne prend que 26 valeurs !



Amélioration : substitution (mono)alphabétique

- **La clef (privée) est une permutation de l'alphabet :**

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

Exemple :

TOUS_LES_CHEMINS_MENENT_A_ROME devient :
FQLJRPAJRHCAE_ZJREAZAZFRDRNQEA

Il y a 27!=10 888 869 450 418 352 160 768 000 000 possibilités…

Le premier cryptanaliste : Al Kindi (800-873)

- <u>Les Fréquences d'Al Kindi</u>

  Alors que la substitution mono-alphabétique (même le chiffrement de César) furent considérés pendant 9 siècles comme inviolables, le philosophe arabe Al Kindi donne une méthode pour les décrypter sans connaître la clef : comparer la fréquence d'apparition des lettres avec leur fréquence moyenne dans la langue utilisée.

Al Kindi

Exemple

BQPSNRSJXJNJXLDPCLDLPQBE_QRKJXHNKPKSJPJIK
SPUNBDKIQRBKPQPBQPZITEJQDQBTSKPELNIUNPHNK
PBKPCKSSQWKPSLXJPSNVVXSQCCKDJPBLDWPXBPS
NVVXJPGKPJKDXIPZLCEJKPGKSPSJQJXSJXHNKSPGP
LZZNIIKDZKPGKSPGXVVKIKDJKSPBKJJIKS

Comment déchiffrer ce message écrit en français ?

Chaque lettre est chiffrée de la même façon… On compare leur fréquence d'apparition à leur fréquence moyenne dans la langue standard.

Fréquence d’apparition des lettres

En français

_	19.3	L	4.7	H	0.8
E	13.9	O	4.1	G	0.8
A	6.7	D	2.9	B	0.6
S	6.3	P	2.5	X	0.4
I	6.1	C	2.4	Y	0.3
T	6.1	M	2.1	J	0.3
N	5.6	V	1.3	Z	0.1
R	5.3	Q	1.3	K	0.0
U	5.2	F	0.9	W	0.0

Dans le cryptogramme

P	14.3	D	4.6	W	1.0
K	12.8	L	4.1	U	1.0
S	9.2	V	3.1	T	1.0
J	9.2	Z	2.6	_	0.5
X	5.6	G	2.6	O	0.0
Q	5.6	C	2.6	M	0.0
N	5.6	E	2.0	F	0.0
B	5.1	R	1.5	A	0.0
I	4.6	H	1.5	Y	0.0

Remplaçons P par _ et K par E

BQ_SNRSJXJNJXLD_CLDL_QBE_QREJXHNE_ESJ_JIES
_UNBDEIQRBE_Q_BQ_ZITEJQDQBTSE_ELNIUN_HNE_B
E_CESSQWE_SLXJ_SNVVXSQCCEDJ_BLDW_XB_SNVV
XJ_GE_JEDXI_ZLCEJE_GES_SJQJXSJXHNES_G_LZZNII
EDZE_GES_GXVVEIEDJES_BEJJIES

Remplaçons Q par A et B par L

LA_SNRSJXJNJXLD_CLDL_ALE_AREJXHNE_ESJ_JIES_
UNLDEIARLE_A_LA_ZITEJADALTSE_ELNIUN_HNE_LE_C
ESSAWE_SLXJ_SNVVXSACCEDJ_LLDW_XL_SNVVXJ_G
E_JEDXI_ZLCEJE_GES_SJAJXSJXHNES_G_LZZNIIEDZE
_GES_GXVVEIEDJES_LEJJIES

Remplaçons S par S et G par D

LA_SNRSJXJNJXLD_CLDL_ALE_AREJXHNE_ESJ_JIES_UNLDEIARLE_A_LA_ZITEJADALTSE_ELNIUN_HNE_LE_CESSAWE_SLXJ_SNVVXSACCEDJ_LLDW_XL_SNVVXJ_DE_JEDXI_ZLCEJE_DES_SJAJXSJXHNES_D_LZZNIIEDZE_DES_DXVVEIEDJES_LEJJIES

Remplaçons J par T et I par R

LA_SNRSTXTNTXLD_CLDL_ALE_ARETXHNE_EST_TRES_UNLDERARLE_A_LA_ZRTETADALTSE_ELNRUN_HNE_LE_CESSAWE_SLXT_SNVVXSACCEDT_LLDW_XL_SNVVXT_DE_TEDXR_ZLCETE_DES_STATXSTXHNES_D_LZZNRREDZE_DES_DXVVEREDTES_LETTRES

Remplaçons X par I, H par Q et N par U

LA_SURSTITUTILD_CLDL_ALE_ARETIQUE_EST_TRES_U
ULDERARLE_A_LA_ZRTETADALTSE_ELURUU_QUE_LE_
CESSAWE_SLIT_SUVVISACCEDT_LLDW_IL_SUVVIT_DE_
TEDIR_ZLCETE_DES_STATISTIQUES_D_LZZURREDZE_D
ES_DIVVEREDTES_LETTRES

Remplaçons V par F et D par N

LA_SURSTITUTILN_CLNL_ALE_ARETIQUE_EST_TRES_U
ULNERARLE_A_LA_ZRTETANALTSE_ELURUU_QUE_LE_
CESSAWE_SLIT_SUFFISACCENT_LLNW_IL_SUFFIT_DE_
TENIR_ZLCETE_DES_STATISTIQUES_D_LZZURRENZE_D
ES_DIFFERENTES_LETTRES

Remplaçons R par B et L par O

LA_SUBSTITUTION_CONO_ALE_ARETIQUE_EST_TRES_UULNERABLE_A_LA_ZRTETANALTSE_EOURUU_QUE_LE_CESSAWE_SOIT_SUFFISACCENT_LONW_IL_SUFFIT_DE_TENIR_ZOCETE_DES_STATISTIQUES_D_OZZURRENZE_DES_DIFFERENTES_LETTRES

Finalement

LA_SUBSTITUTION_MONO_ALPHABETIQUE_EST_TRES_VULNERABLE_A_LA_CRYPTANALYSE_POURVU_QUE_LE_MESSAGE_SOIT_SUFFISAMMENT_LONG_IL_SUFFIT_DE_TENIR_COMPTE_DES_STATISTIQUES_D_OCCURRENCE_DES_DIFFERENTES_LETTRES

Le code de Vigenère

- La méthode des fréquences d'Al Kindi permet de casser tout code à substitution mono-alphabétique.
- Un diplomate français de la renaissance, Blaise de Vigenère imagina un code résistant à la méthode d'Al Kindi.
- Cette méthode consiste à faire varier la clef du codage de César à l'aide d'un mot *clef*.

Blaise de Vigenère

Le code de Vigenère : exemple

- Considérons la clef (privée) AIR
- A donne le chiffrement de César :
  ABCDEFGHIJKLMNOPQRSTUVWXYZ_
  ABCDEFGHIJKLMNOPQRSTUVWXYZ_
- I donne le chiffrement de César :
  ABCDEFGHIJKLMNOPQRSTUVWXYZ_
  IJKLMNOPQRSTUVWXYZ_ABCDEFGH
- R donne le chiffrement de César :
  ABCDEFGHIJKLMNOPQRSTUVWXYZ_
  RSTUVWXYZ_ABCDEFGHIJKLMNOPQ

Le code de Vigenère : Exemple

- Pour crypter : *salon de provence* avec la clef privée *air*

S	A	L	O	N	_	D	E	_	P	R	O	V	E	N	C	E
A	I	R	A	I	R	A	I	R	A	I	R	A	I	R	A	I

Le code de Vigenère : Exemple

- Pour crypter : *salon de provence* avec la clef privée *air*

S	A	L	O	N	_	D	E	_	P	R	O	V	E	N	C	E
A	I	R	A	I	R	A	I	R	A	I	R	A	I	R	A	I
S			O			D			P			V			C	

Le code de Vigenère : Exemple

- Pour crypter : *salon de provence* avec la clef privée *air*

S	A	L	O	N	_	D	E	_	P	R	O	V	E	N	C	E
A	I	R	A	I	R	A	I	R	A	I	R	A	I	R	A	I
S	I		O	V		D	M		P	Z		V	M		C	M

Le code de Vigenère : Exemple

- Pour crypter : *salon de provence* avec la clef privée *air*

S	A	L	O	N	_	D	E	_	P	R	O	V	E	N	C	E
A	I	R	A	I	R	A	I	R	A	I	R	A	I	R	A	I
S	I	B	O	V	Q	D	M	Q	P	Z	E	V	M	D	C	M

On obtient le message crypté :

SIBOV QDMQP ZEVMD CM

Le code de Vigenère : Exemple

- Pour crypter : *salon de provence* avec la clef privée *air*

S	A	L	O	N	_	D	E	_	P	R	O	V	E	N	C	E
A	I	R	A	I	R	A	I	R	A	I	R	A	I	R	A	I
S	I	B	O	V	Q	D	M	Q	P	Z	E	V	M	D	C	M

On obtient le message crypté :

SIBOV QDMQP ZEVMD CM

Pour le décrypter il faut lui appliquer le même procédé en inversant l'ordre de lecture des 3 tables de substitutions alphabétiques (t*ransformations inverses).*

Cryptanalyse du code de Vigenère

- Pendant 3 siècles le code de Vigenère fût considéré comme inviolable.
- Jusqu'au XIXe siècle, où le mathématicien britannique Charles Babbage donna une méthode pour le casser (*test de Kasiski*).

Charles Babbage
(1791-1871)

Cryptanalyse du code de Vigenère

- Pendant 3 siècles le code de Vigenère fût considéré comme inviolable.
- Jusqu'au XIXe siècle, où le mathématicien britannique Charles Babbage donna une méthode pour le casser (*test de Kasiski*).

Charles Babbage
(1791-1871)

- Babbage est surtout connu comme inventeur de la *machine à différence*, précurseur de l'informatique,
  (réalisée fin XXe siècle).

Cryptanalyse du code de Vigenère

- Babbage remarque que si :
  - On connaît la longueur de la clef de Vigenère,
  - Sa longueur est petite comparée à celle du message crypté.
- alors la méthode des fréquences d'Al Kindi permet de casser le code :

Cryptanalyse du code de Vigenère

- Babbage remarque que si :
  - On connaît la longueur de la clef de Vigenère,
  - Sa longueur est petite comparée à celle du message crypté.
- alors la méthode des fréquences d'Al Kindi permet de casser le code :
- Exemple : si la longueur de la clef est 5, considérer les fréquences d'apparition dans les 5 messages réduits aux lettres :
  - 1,6,11,16,21, etc…
  - 2,7,12,17,22, etc…,
  - 3,8,13,18,23, etc…,
  - 4,9,14,19,24, etc…,
  - 5,10,15,20,25, etc… .

Cryptanalyse du code de Vigenère

- Il suffit donc de connaître (un petit multiple de) la longueur de la clef de Vigenère. Si elle est suffisamment courte, comparativement au message, on peut casser le code.

Cryptanalyse du code de Vigenère

- Il suffit donc de connaître (un petit multiple de) la longueur de la clef de Vigenère. Si elle est suffisamment courte, comparativement au message, on peut casser le code.
- Babbage propose une méthode pour déterminer (un petit multiple de) la longueur de la clef :

Cryptanalyse du code de Vigenère

- Il suffit donc de connaître (un petit multiple de) la longueur de la clef de Vigenère. Si elle est suffisamment courte, comparativement au message, on peut casser le code.
- Babbage propose une méthode pour déterminer (un petit multiple de) la longueur de la clef :
- Supposons que dans le message crypté une même série de lettres (au moins 3) apparaisse fréquement. (Ex : xxABCxxABCxxxxxxxABCx)
  Soit :
  - C'est dû au hasard
  - Une même série de 3 (ou +) lettres apparaît fréquemment au dessus d'une même portion du mot clef.

Cryptanalyse du code de Vigenère

- Il suffit donc de connaître (un petit multiple de) la longueur de la clef de Vigenère. Si elle est suffisamment courte, comparativement au message, on peut casser le code.
- Babbage propose une méthode pour déterminer (un petit multiple de) la longueur de la clef :
- Supposons que dans le message crypté une même série de lettres (au moins 3) apparaisse fréquement. (Ex : xxABCxxABCxxxxxxxABCx)
  Soit :
  - C'est dû au hasard : très improbable !
  - Une même série de 3 (ou +) lettres apparaît fréquemment au dessus d'une même portion du mot clef.
  - Distance entre 2 séries = multiple de longueur(clef) = 5

La machine Enigma

- Durant la seconde guerre mondiale, l'Allemagne nazi utilise la machine Enigma pour crypter toutes ses communications.

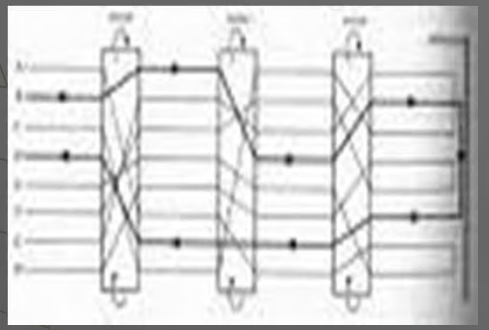
- Ils restaient convaincus de son inviolabilité... Son code fût pourtant systématiquement cassé par les services polonais puis britanniques ; marquant un tournant dans la guerre...

La machine enigma

- La machine Enigma ressemble à une machine à écrire. On saisit le texte à coder sur le clavier. Dès qu'on actionne une touche une diode éclaire la touche du caractère à retranscrire.
- Le même procédé permet le codage du message clair et le décodage du message crypté.

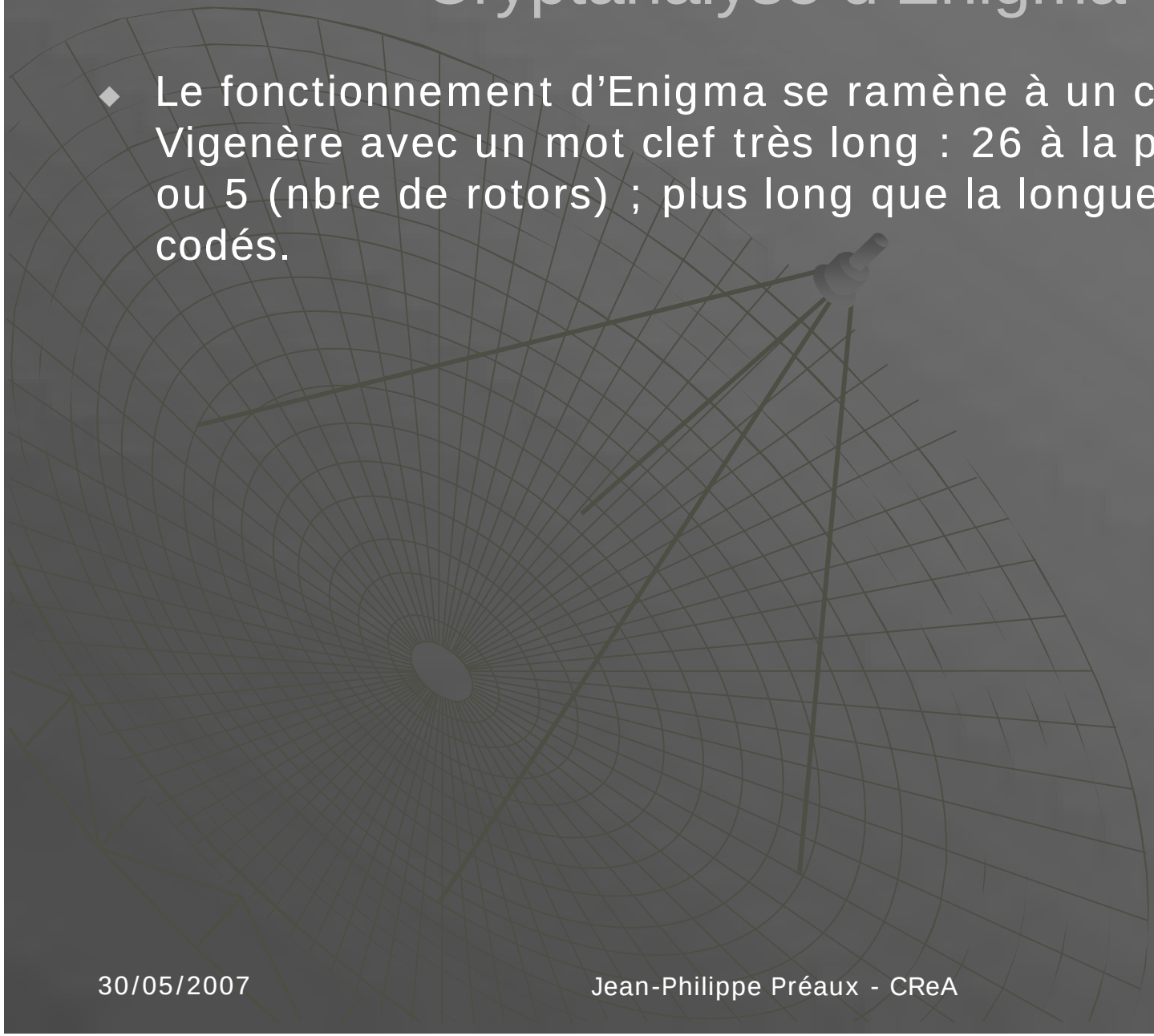
La machine enigma

- La machine Enigma ressemble à une machine à écrire. On saisit le texte à coder sur le clavier. Dès qu'on actionne une touche une diode éclaire la touche du caractère à retranscrire.
- Le même procédé permet le codage du message clair et le décodage du message crypté.
- De 3 à 5 rotors permettent de saisir la clef d'encryption. Elle était changée aléatoirement chaque jour et commune à toutes les communications nazis.
- Chaque rotor a 26 graduations et réalise une substitution monoalphabétique. La saisie d'une touche provoque la rotation d'un cran des rotors (comme pour les aiguilles d'une montre).



Cryptanalyse d’Enigma

- Le fonctionnement d’Enigma se ramène à un code de Vigenère avec un mot clef très long : 26 à la puissance 3, 4 ou 5 (nbre de rotors) ; plus long que la longueur des textes codés.



Cryptanalyse d'Enigma

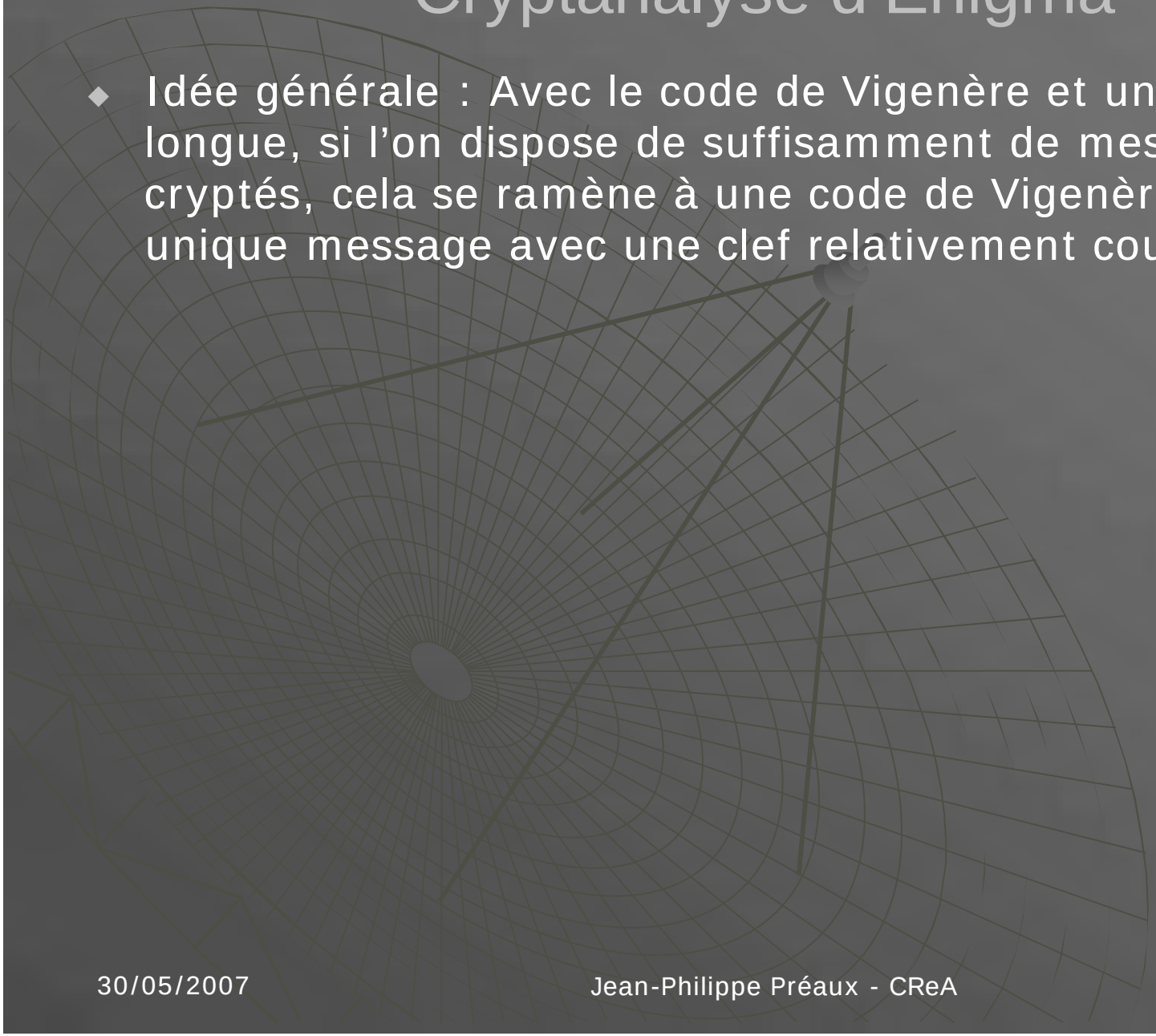
- Le fonctionnement d'Enigma se ramène à un code de Vigenère avec un mot clef très long : 26 à la puissance 3, 4 ou 5 (nbre de rotors) ; plus long que la longueur des textes codés.
- Quelques mois après le début de la guerre, les services secrets polonais obtiennent les plans d'Enigma (et donc l'algorithme de cryptage). Elle n'a alors que 3 rotors.
- Les travaux du mathématicien polonais Rejewski permettent régulièrement de casser le code. Ils permettent la destruction des sous-marins nazis U-110 (1941) et U-559 (1942).

Cryptanalyse d'Enigma

- Le fonctionnement d'Enigma se ramène à un code de Vigenère avec un mot clef très long : 26 à la puissance 3, 4 ou 5 (nbre de rotors) ; plus long que la longueur des textes codés.
- Quelques mois après le début de la guerre, les services secrets polonais obtiennent les plans d'Enigma (et donc l'algorithme de cryptage). Elle n'a alors que 3 rotors.
- Les travaux du mathématicien polonais Rejewski permettent régulièrement de casser le code. Ils permettent la destruction des sous-marins nazis U-110 (1941) et U-559 (1942).
- Les allemands passent à des machines à 4 ou 5 rotors.
- L'équipe britannique de mathématiciens dirigée par A.Turing développe une technique pour casser le code.
- L'impact sur les victoires alliés est retentissant ! Tandis que les allemands persistent à croire en l'inviolabilité d'Enigma.

Cryptanalyse d'Enigma

- Idée générale : Avec le code de Vigenère et une clef très longue, si l'on dispose de suffisamment de messages cryptés, cela se ramène à une code de Vigenère pour un unique message avec une clef relativement courte.



Cryptanalyse d'Enigma

- Idée générale : Avec le code de Vigenère et une clef très longue, si l'on dispose de suffisamment de messages cryptés, cela se ramène à une code de Vigenère pour un unique message avec une clef relativement courte.
- Le cryptage d'Enigma implique que les lettres doivent être changées : A ne peut devenir A.

Cryptanalyse d'Enigma

- Idée générale : Avec le code de Vigenère et une clef très longue, si l'on dispose de suffisamment de messages cryptés, cela se ramène à une code de Vigenère pour un unique message avec une clef relativement courte.
- Le cryptage d'Enigma implique que les lettres doivent être changées : A ne peut devenir A.
- Turing recherche des séquences standards comme : « *bulletin meteo atlantique nord* » dans un grand nombre de message grâce à cette propriété :

Cryptanalyse d'Enigma

- Idée générale : Avec le code de Vigenère et une clef très longue, si l'on dispose de suffisamment de messages cryptés, cela se ramène à une code de Vigenère pour un unique message avec une clef relativement courte.
- Le cryptage d'Enigma implique que les lettres doivent être changées : A ne peut devenir A.
- Turing recherche des séquences standards comme : « *bulletin meteo atlantique nord* » dans un grand nombre de message grâce à cette propriété :
  - …..BU_LETIN_METEO_ATLANTIQUE_NORD…..
  - …..JG**L**_IUQFQFLKHA_LFEIAPOAIEYA_UTTI…..
  - Impossible : on décale à droite jusqu'à ce qu'aucune lettre ne se corresponde plus.

Cryptanalyse d'Enigma

- Idée générale : Avec le code de Vigenère et une clef très longue, si l'on dispose de suffisamment de messages cryptés, cela se ramène à une code de Vigenère pour un unique message avec une clef relativement courte.
- Le cryptage d'Enigma implique que les lettres doivent être changées : A ne peut devenir A.
- Turing recherche des séquences standards comme : « *bulletin meteo atlantique nord* » dans un grand nombre de message grâce à cette propriété :
  - …..BULLETIN_METEO_ATLANTIQUE_NORD…..
  - …..JGL_IUQFQFLKHA_LFEIAPOAIEYA_UTTI…..
  - Impossible : on décale à droite jusqu'à ce qu'aucune lettre ne se corresponde plus.
- La faille d'Enigma réside dans la non jetabilité de la clef.

Cryptographie (à clé privée) sûre : le code de Vernam

- Pour contrer le décryptage du code de Vigenère, le cryptographe américain G.Vernam (1890-1960) eut l'idée d'utiliser une clé aussi longue que le message.

Cryptographie (à clé privée) sûre : le code de Vernam

- Pour contrer le décryptage du code de Vigenère, le cryptographe américain G.Vernam (1890-1960) eut l'idée d'utiliser une clé aussi longue que le message.
- Le mathématicien C.Shannon (1916-2000, père de la théorie de l'information) montre que si la clé est choisie aléatoirement et est utilisée une seule fois, ce système de cryptage (à clé privé) est inviolable. Il est parfaitement sûr !
- La raison en est que le texte crypté devient lui-même aléatoire, résistant par là même à toute cryptanalyse.

Application : le téléphone rouge

- Liaison fax transatlantique reliant directement le kremlin à la maison blanche.
- Le protocole de cryptage est le code de Vernam. A chaque communication la clé doit être transmise par voie diplomatique.

Application : le téléphone rouge

- Liaison fax transatlantique reliant directement le kremlin à la maison blanche.
- Le protocole de cryptage est le code de Vernam. A chaque communication la clé doit être transmise par voie diplomatique.
- Avantage : sécurité parfaite tant que la clé est secrète.
- Désavantages : transport de la clé lourd, lent et coûteux. risque d'interception. Clé à usage unique.

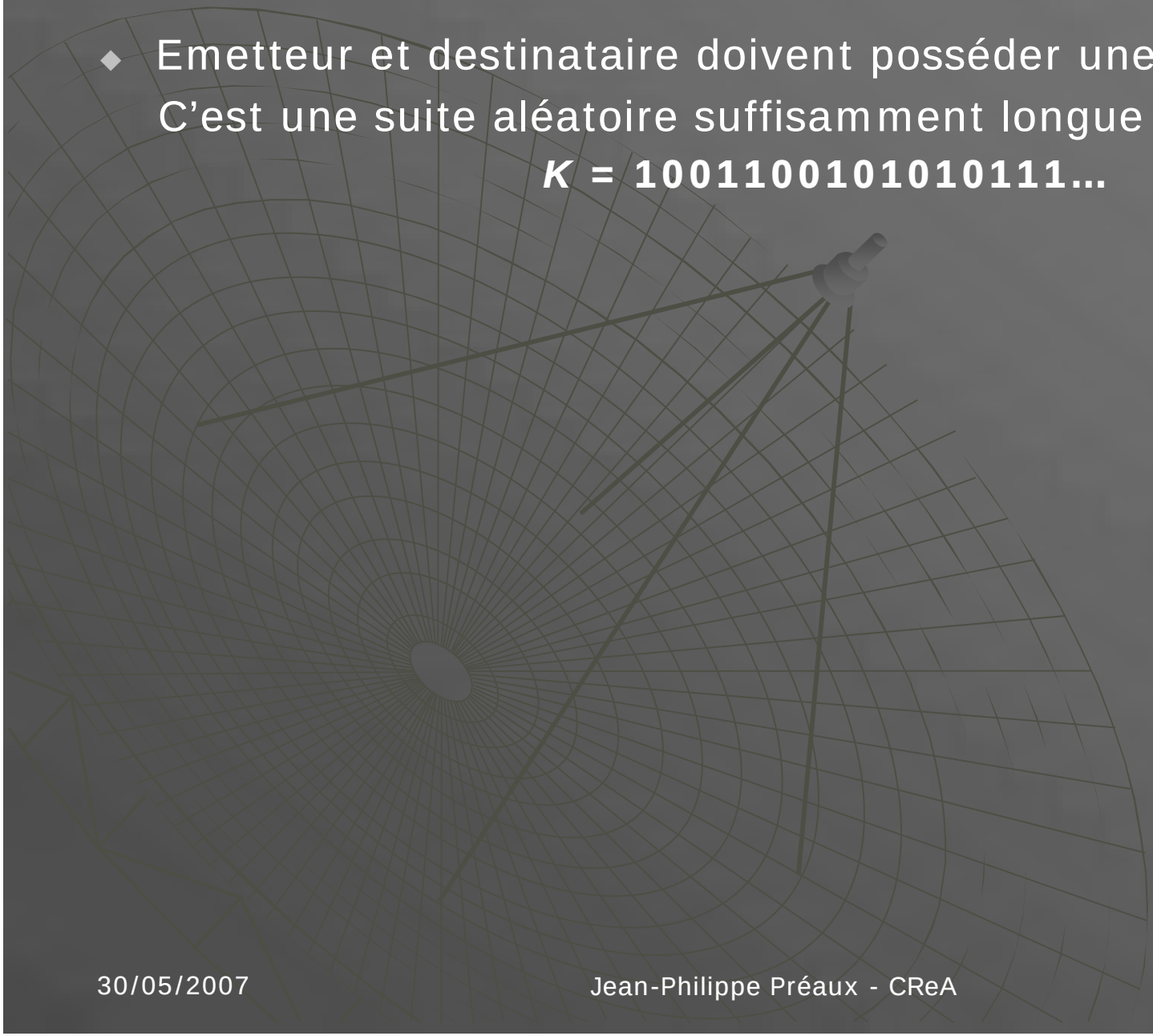
  Nécessite un acheminement hautement sécurisé.

  N'est réalisable que pour des voies de communications fixes et privilégiées.

Fonctionnement du téléphone rouge

- Emetteur et destinataire doivent posséder une même clé *K*.
  C'est une suite aléatoire suffisamment longue de 0 et de 1.

  ***K* = 1001100101010111…**



Fonctionnement du téléphone rouge

- Emetteur et destinataire doivent posséder une même clé *K*. C'est une suite aléatoire suffisamment longue de 0 et de 1.

  ***K* = 1001100101010111...**

- Le message clair *M* à transmettre est numérisé, grâce à un dictionnaire connu préétabli (morse ou Ascii..).

  ***M* = 1111111111111111...**

Fonctionnement du téléphone rouge

- Emetteur et destinataire doivent posséder une même clé *K.* C'est une suite aléatoire suffisamment longue de 0 et de 1.

  $K = 1001100101010111\ldots$

- Le message clair *M* à transmettre est numérisé, grâce à un dictionnaire connu préétabli (morse ou Ascii..).

  $M = 1111111111111111\ldots$

- L'émetteur forme le message crypté $M \oplus K$, (addition bit à bit), et le transmet :

  $M \oplus K = 01100110101000\ldots$

$$0+0=0$$
$$0+1=1$$
$$1+0=1$$
$$1+1=0$$

Fonctionnement du téléphone rouge

- Emetteur et destinataire doivent posséder une même clé *K.* C'est une suite aléatoire suffisamment longue de 0 et de 1.

  $K = 1001100101010111\ldots$

- Le message clair *M* à transmettre est numérisé, grâce à un dictionnaire connu préétabli (morse ou Ascii..).

  $M = 1111111111111111\ldots$

- L'émetteur forme le message crypté $M \oplus K$, (addition bit à bit(, et le transmet :

  $M \oplus K = 01100110101000\ldots$

$$0+0=0$$
$$0+1=1$$
$$1+0=1$$
$$1+1=0$$

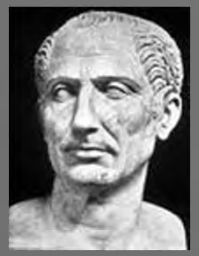
- Le destinataire reçoit le message crypté $M' = M \oplus K$. Il le décode en formant $M' \oplus K = M$, et le tour est joué.

  $M' \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0 = M$

Chronologie de la cryptographie à clé privée

CRYPTAGE

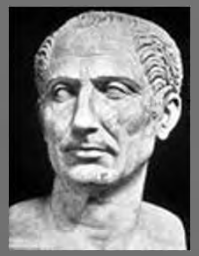
Ier siècle av. JC : Code de César, substitutions alphabétiques



Chronologie de la cryptographie à clé privée

CRYPTAGE

Ier siècle av. JC : Code de César, substitutions alphabétiques



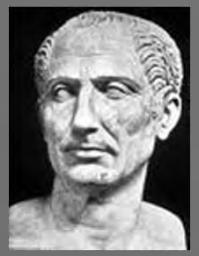
DECRYPTAGE

IXème siècle

d'Al kindi

Chronologie de la cryptographie à clé privée

CRYPTAGE — Ier siècle av. JC : Code de César, substitutions alphabétiques

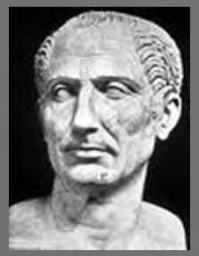


DECRYPTAGE — IXème siècle : Les fréquences d'Al kindi

CRYPTAGE — XVIème siècle : Code de Vigenère

Chronologie de la cryptographie à clé privée

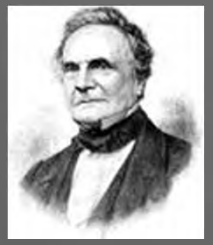
CRYPTAGE — Ier siècle av. JC : Code de César, substitutions alphabétiques



DECRYPTAGE — IXème siècle : Les fréquences d'Al kindi

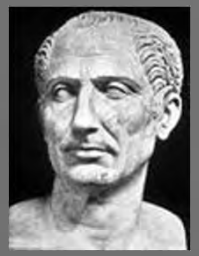
CRYPTAGE — XVIème siècle : Code de Vigenère

DECRYPTAGE — XIXème siècle : Test de Kasiski



Chronologie de la cryptographie à clé privée

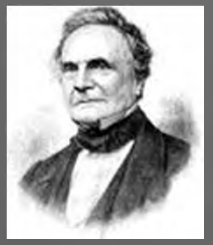
CRYPTAGE — Ier siècle av. JC : Code de César, substitutions alphabétiques



DECRYPTAGE — IXème siècle : Les fréquences d'Al kindi

CRYPTAGE — XVIème siècle : Code de Vigenère

DECRYPTAGE — XIXème siècle : Test de Kasiski



CRYPTAGE — XXème siècle : Code de Vernam – Théorème de Shannon

II - Cryptographie moderne

- Echange de clef à distance
- Cryptographie à clef publique
- Le système RSA
- Faiblesse de RSA
- Courbes elliptiques
- Cryptographie quantique

Cryptographie moderne

- La cryptographie à clé privée a un fonctionnement analogue à celui d'un cadenas. Seuls ceux pourvus de la clé peuvent ouvrir le cadenas (décoder le message).

- Malgré son infaillibilité, elle est inadéquate face aux techniques modernes de communication nomade : comment échanger numériquement une clef en toute sécurité dans un système de communication ouvert ?

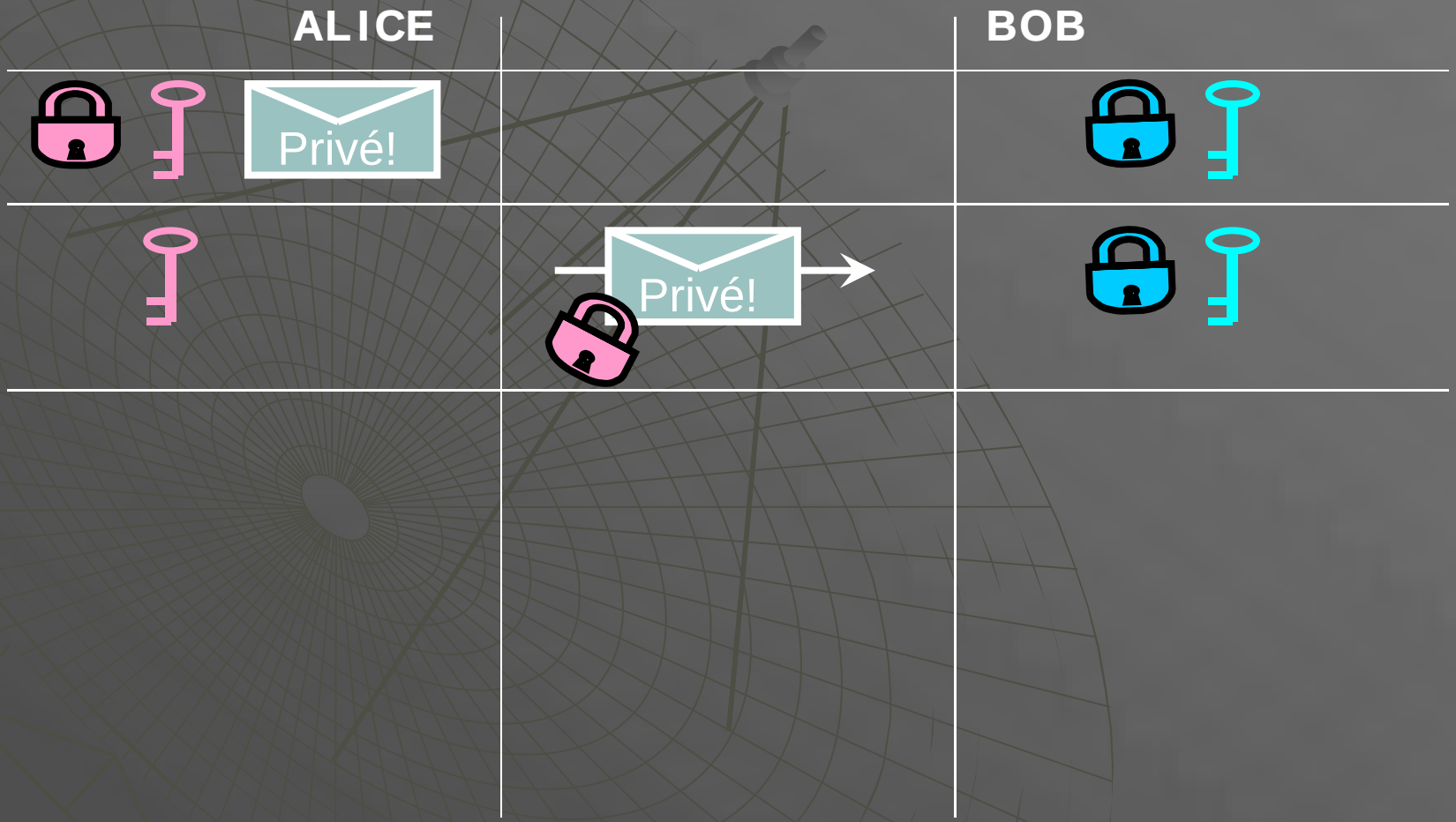
Echange de clef à distance

- Alice et Bob veulent s'échanger à distance une information. Il dispose tous deux d'une clé de cryptage privée *Ka* et *Kb*. On suppose que les 2 procédés de cryptage commutent : *Ka*(*Kb*(*M*)) = *Kb*(*Ka*(*M*))

ALICE		**BOB**
		

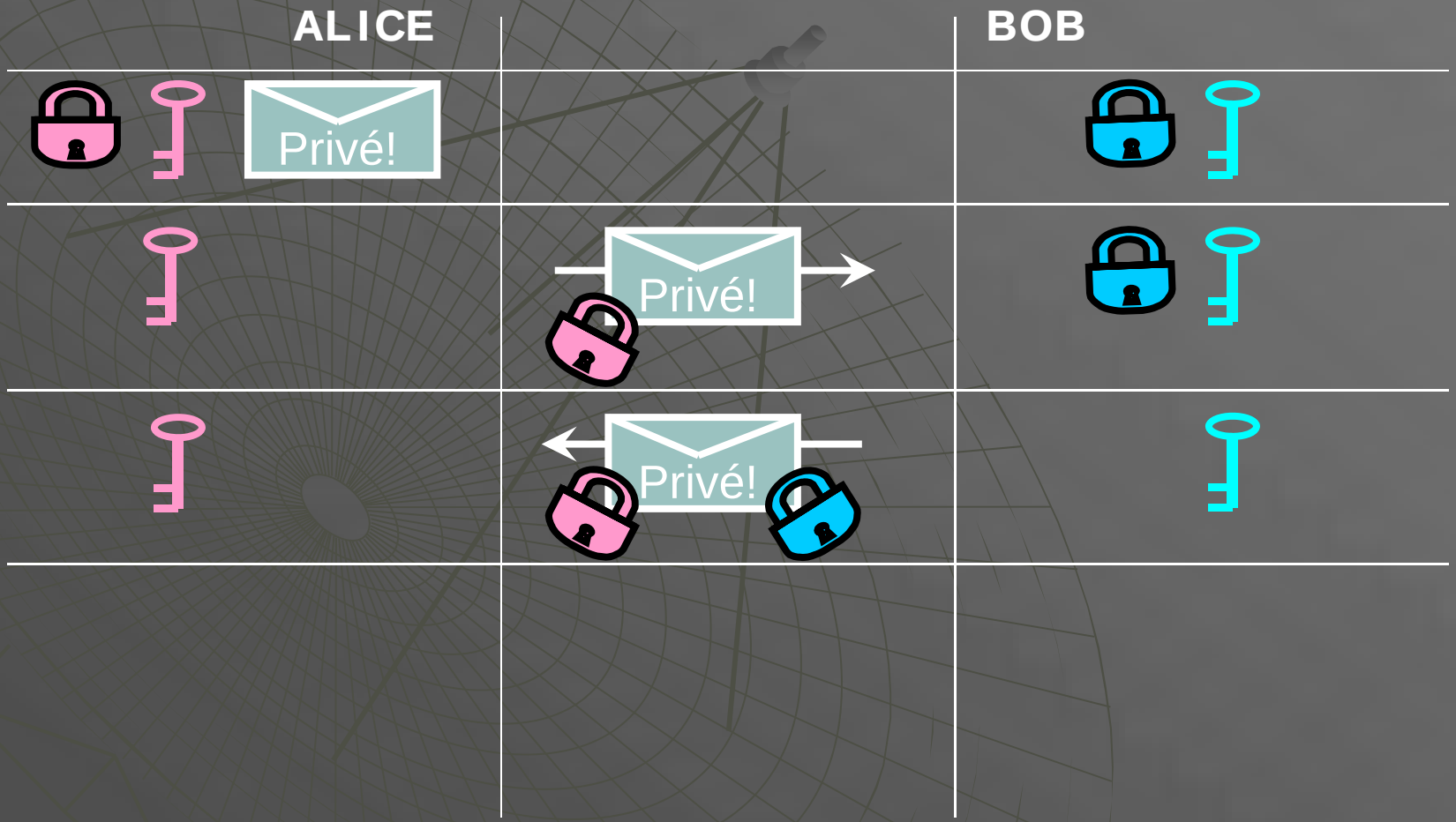
Echange de clef à distance

- Alice et Bob veulent s'échanger à distance une information. Il dispose tous deux d'une clé de cryptage privée *Ka* et *Kb*. On suppose que les 2 procédés de cryptage commutent : *Ka*(*Kb*(*M*)) = *Kb*(*Ka*(*M*))



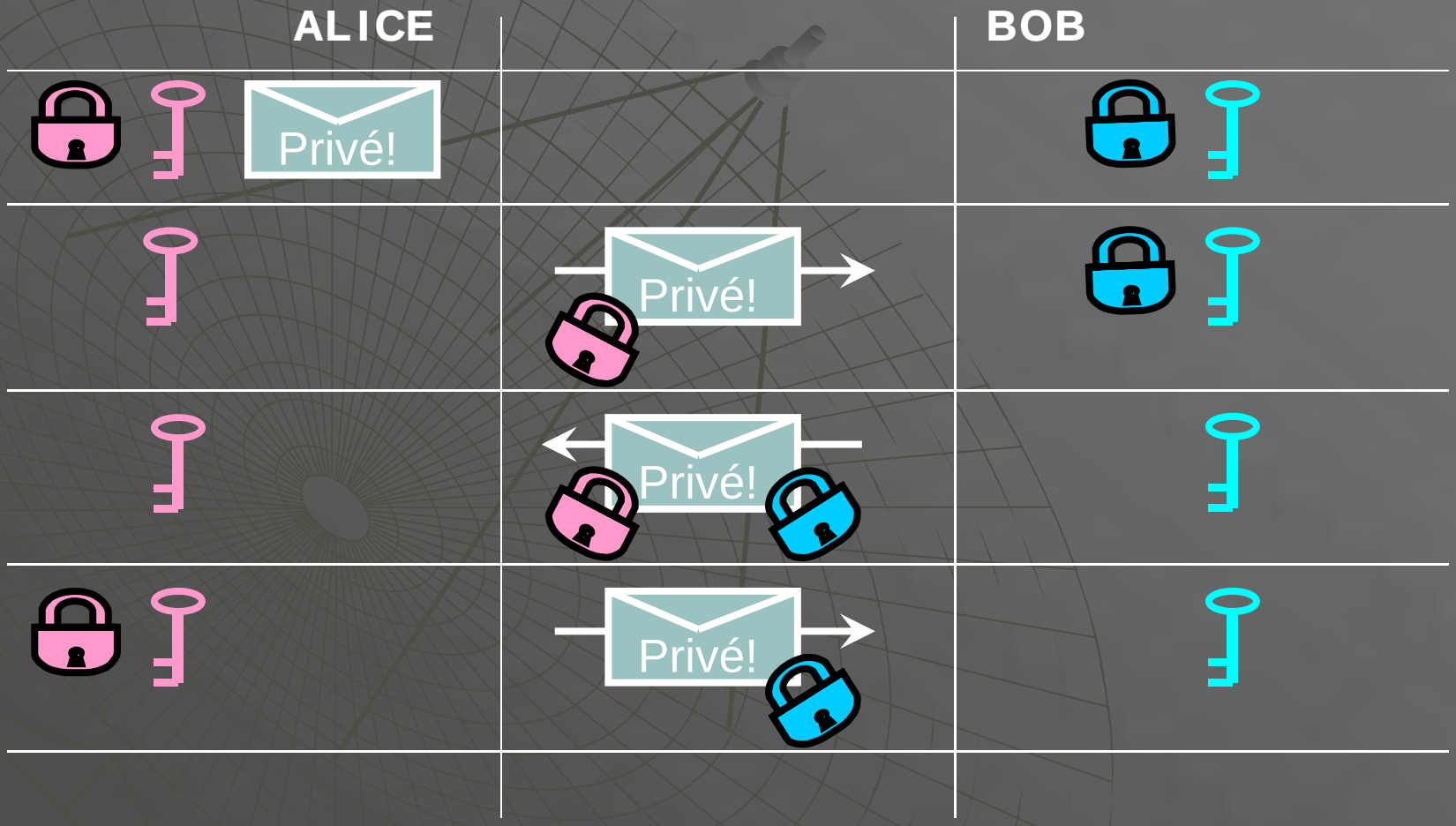
Echange de clef à distance

- Alice et Bob veulent s'échanger à distance une information. Il dispose tous deux d'une clé de cryptage privée *Ka* et *Kb*. On suppose que les 2 procédés de cryptage commutent : *Ka*(*Kb*(*M*)) = *Kb*(*Ka*(*M*))



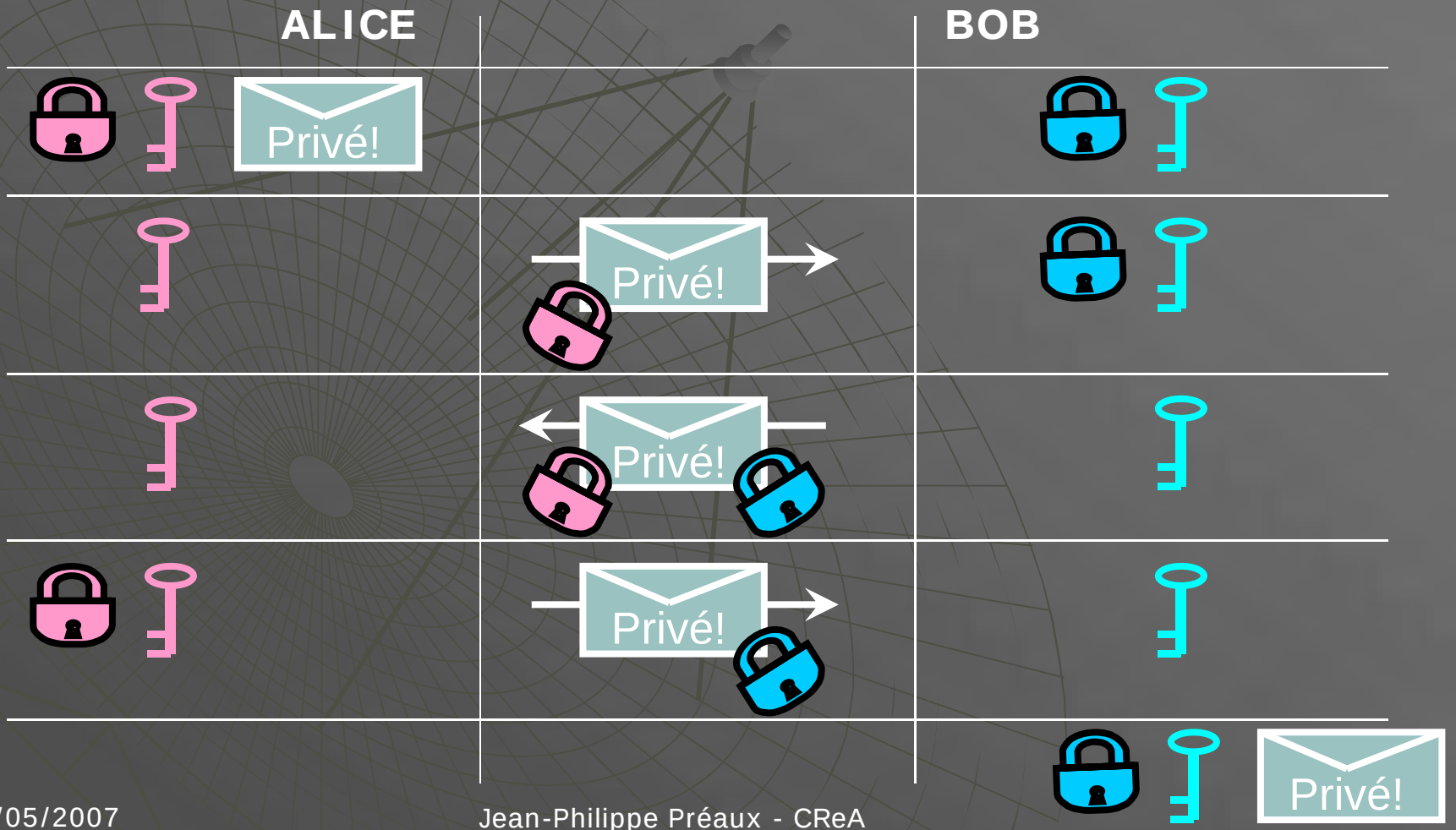
Echange de clef à distance

- Alice et Bob veulent s'échanger à distance une information. Il dispose tous deux d'une clé de cryptage privée *Ka* et *Kb*. On suppose que les 2 procédés de cryptage commutent : *Ka*(*Kb*(*M*)) = *Kb*(*Ka*(*M*))



Echange de clef à distance

- Alice et Bob veulent s'échanger à distance une information. Il dispose tous deux d'une clé de cryptage privée *Ka* et *Kb*. On suppose que les 2 procédés de cryptage commutent : *Ka*(*Kb*(*M*)) = *Kb*(*Ka*(*M*))



Exemple

- Deux clés publiques *P et m sont* connues de tous.
- Alice choisit une clef privée *A*, qu'elle garde secrète, et transmet à Bob Ka=*m^A [mod P].*

  Bob choisit une clé privée B et transmet *Kb=m^B [mod P]* à Alice.

Exemple

- Deux clés publiques *P et m sont* connues de tous.
- Alice choisit une clef privée *A*, qu'elle garde secrète, et transmet à Bob Ka=*m^A [mod P].*

  Bob choisit une clé privée B et transmet *Kb=m^B [mod P]* à Alice.
- Alice calcule *m^AB [P]* à partir de *Kb* et *A.*

  Bob calcule *m^AB [P]* à partir de *Ka* et B.

  Ils ont échangé la clé *K=m^AB [P]* secrète, et peuvent désormais s'en servir.

Exemple

- Deux clés publiques *P et m sont* connues de tous.
- Alice choisit une clef privée *A*, qu'elle garde secrète, et transmet à Bob Ka=*m^A [mod P].*

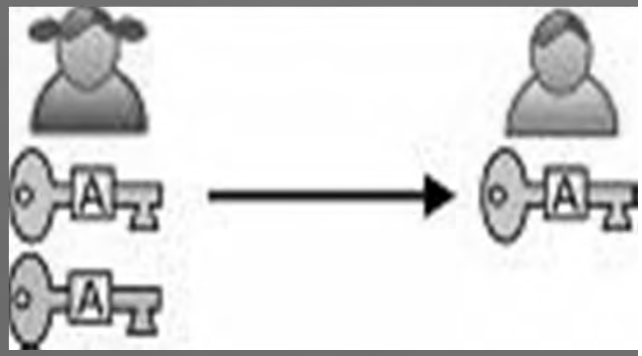
  Bob choisit une clé privée B et transmet *Kb=m^B [mod P]* à Alice.
- Alice calcule *m^AB [P]* à partir de *Kb* et *A.*

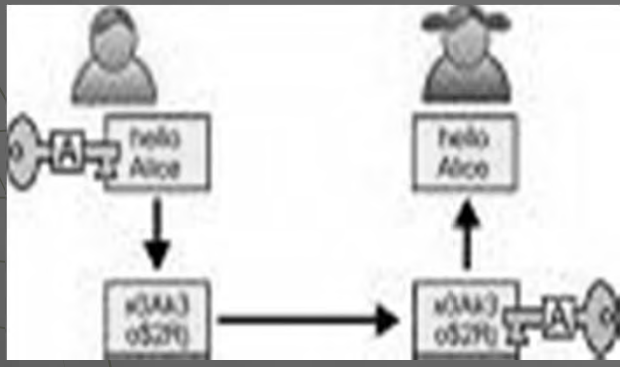
  Bob calcule *m^AB [P]* à partir de *Ka* et B.

  Ils ont échangé la clé *K=m^AB [P]* secrète, et peuvent désormais s'en servir.
- Si pour Alice et Bob le calcul de *K* est rapide, pour un pirate, déterminer *K* à partir de *Ka* et *Kb,* sans connaître *a* et *b* est très long (mais faisable : problème du logarithme discret) !

Cryptographie à clef publique

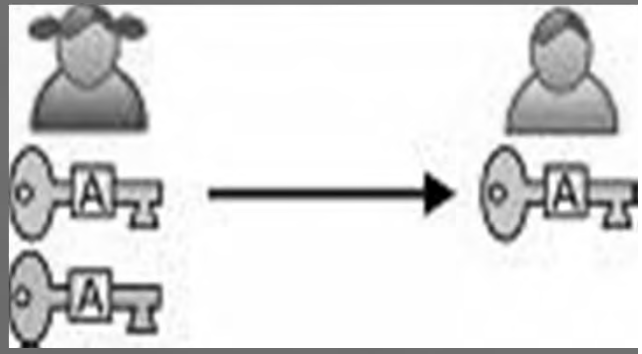
- A l'aide d'une clef publique K, Alice fabrique une clé publique Kp et une clé privée Ks. Elle publie Kp et garde Ks secrète.
- Le cryptage est asymétrique. Kp sert à coder et Ks à décoder.

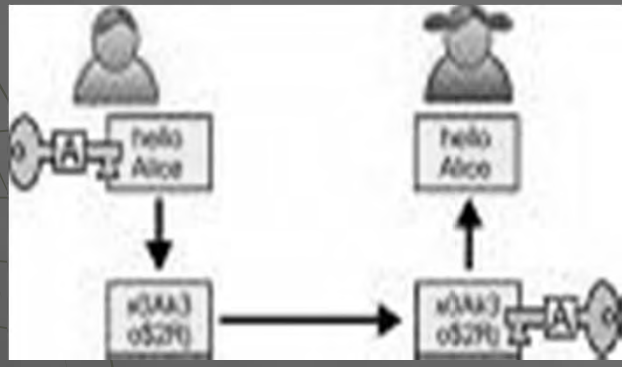




Cryptographie à clef publique

- A l'aide d'une clef publique K, Alice fabrique une clé publique Kp et une clé privée Ks. Elle publie Kp et garde Ks secrète.
- Le cryptage est asymétrique. Kp sert à coder et Ks à décoder.
- C'est par exemple le système RSA, le plus populaire, car le plus fiable, à ce jour.
- Dans tous les systèmes à clé publique actuels, on peut recalculer la clé privée à partir des clés publiques. Mais s'il est facile et rapide de créer les clés Kp et Ks à partir de K, il est difficile est long de retrouver Ks à partir de K et Kp.
- C'est cependant réalisable algorithmiquement ! Tout est basé sur la supposée gigantesque durée du calcul.





Le système

- Le système RSA (Rivest, Shamir, Adleman), supposé le plus fiable, est aujourd'hui amplement répandu.

P et Q : premiers gardés secrets,

N=PQ : clef publique

ed=1 mod (P-1)(Q-1)

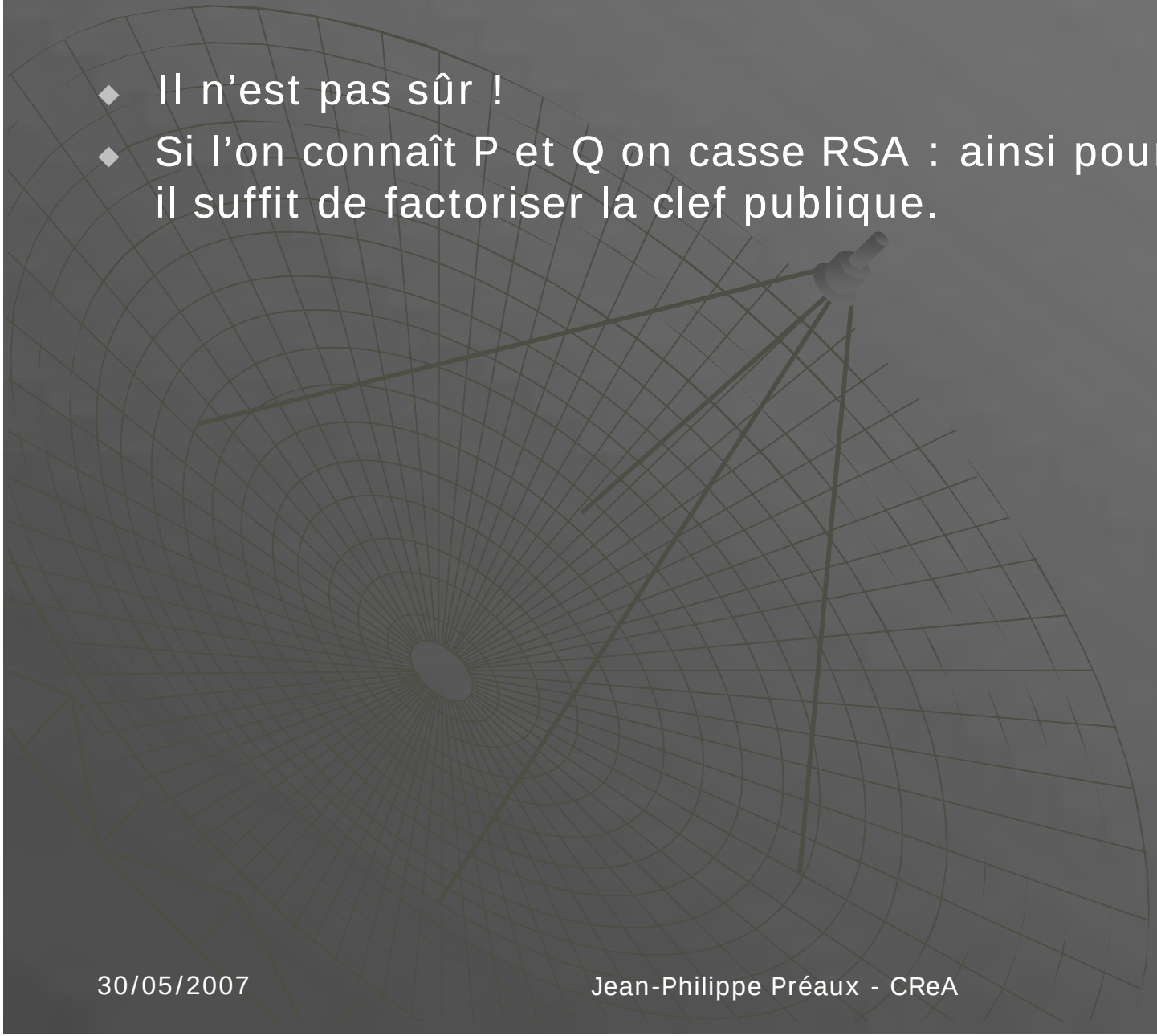
C=M^e mod N

M=C^d mod N

RSA Laboratories

Faiblesse de RSA

- Il n’est pas sûr !
- Si l’on connaît P et Q on casse RSA : ainsi pour casser RSA il suffit de factoriser la clef publique.



Faiblesse de RSA

- Il n’est pas sûr !
- Si l’on connaît P et Q on casse RSA : ainsi pour casser RSA il suffit de factoriser la clef publique.
- Les nombres P et Q doivent être très grands (200 chiffres).
- La taille actuelle de la clef est de plusieurs Kilo-octets. Le protocole est relativement lent.

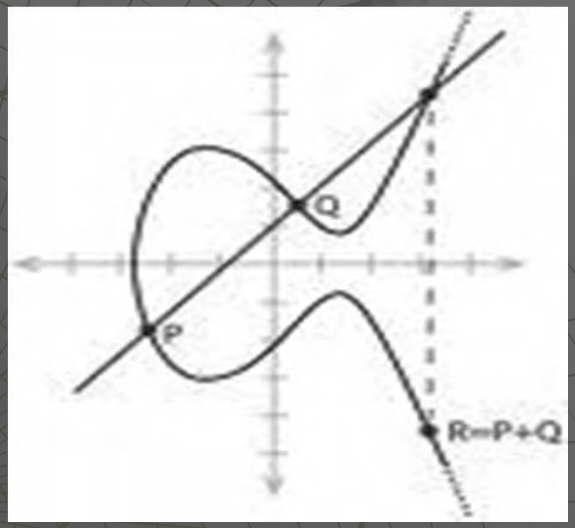
Faiblesse de RSA

- Il n'est pas sûr !
- Si l'on connaît P et Q on casse RSA : ainsi pour casser RSA il suffit de factoriser la clef publique.
- Les nombres P et Q doivent être très grands (200 chiffres).
- La taille actuelle de la clef est de plusieurs Kilo-octets. Le protocole est relativement lent.
- En 1997 S.Humpich factorise le nombre de 96 chiffres utilisé dans les cartes bancaires. Ils crée des 'Yes card' à volonté. Ce nombre est aujourd'hui de 232 chiffres. Combien de temps résistera-t-il.
- Il est interdit de factoriser le nombre N=PQ :

  N=155088080278376929842392150075130787847110202
  152067111027931119901138753945534599975760530 4
  671735856091597555389797408938173344043674704 78
  098639006990667909672893308140504493596951450 86
  762399424934407505892700157399623745293632518 27.

Utilisation des courbes elliptiques

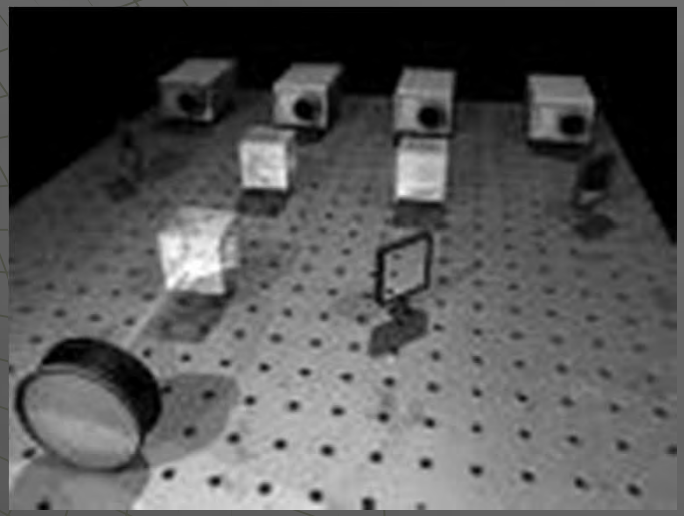
- Les courbes elliptiques ont la propriété qu'on peut 'additionner' des points de la courbe, et en fait développer une arithmétique.



- On les utilise pour créer un système à la RSA. Il a les même désavantages mais la clé peut-être choisie plus courte pour une fiabilité similaire.

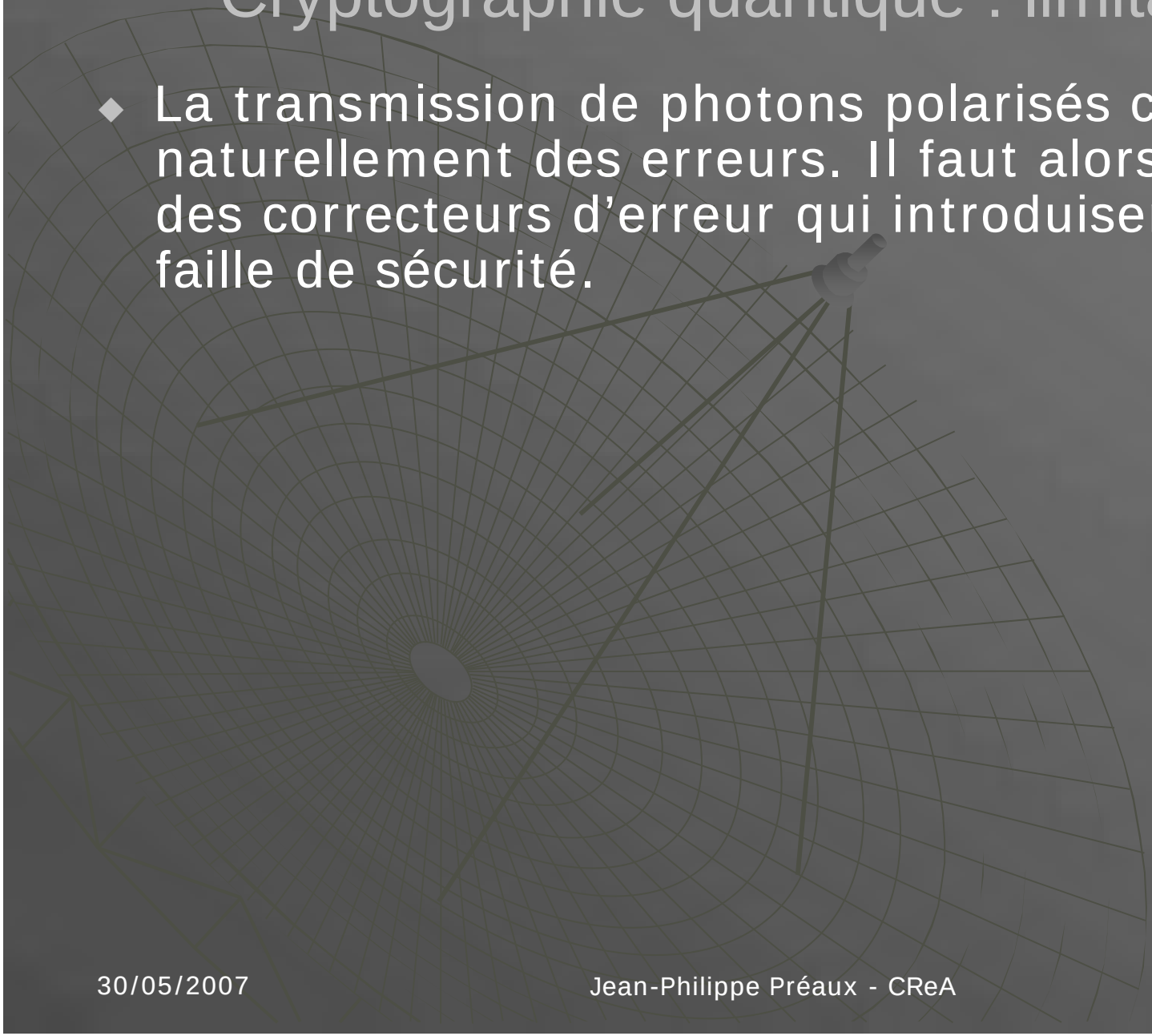
Cryptographie quantique

- La cryptographie quantique utilise le principe d'incertitude d'Heisenberg.
- L'information est colportée par des particules polarisées dans une fibre optique.
- Un observateur extérieur (espion) qui tenterait de lire le message le corromprait irrémédiablement.
- Un mécanisme de correction d'erreur permet de détecter l'espionnage.



Cryptographie quantique : limitations

- La transmission de photons polarisés colporte naturellement des erreurs. Il faut alors utiliser des correcteurs d'erreur qui introduisent une faille de sécurité.



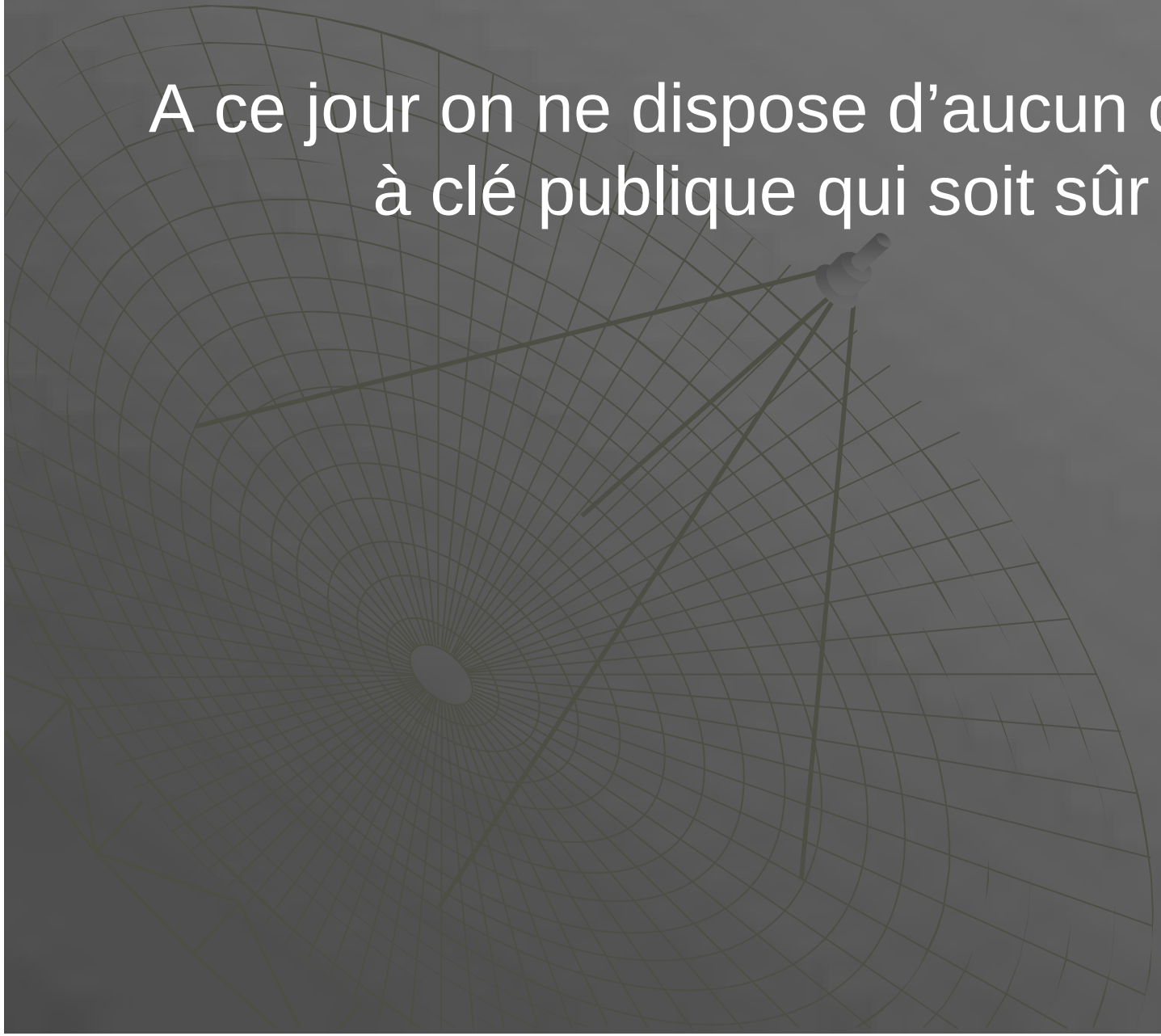
Cryptographie quantique : limitations

- La transmission de photons polarisés colporte naturellement des erreurs. Il faut alors utiliser des correcteurs d'erreur qui introduisent une faille de sécurité.
- On ne sait le réaliser que sur de très courtes distances (100km).
- Si le premier succès a eu lieu en 1991, il n'a amené à aucun développement applicable à ce jour.

Cryptographie quantique : limitations

- La transmission de photons polarisés colporte naturellement des erreurs. Il faut alors utiliser des correcteurs d'erreur qui introduisent une faille de sécurité.
- On ne sait le réaliser que sur de très courtes distances (100km).
- Si le premier succès a eu lieu en 1991, il n'a amené à aucun développement applicable à ce jour.
- Les technologies quantiques permettent aussi la réalisation de l'ordinateur quantique (chaque particule peut être dans plusieurs états simultanément), dont la première application serait de casser tous les codes à clé publique connus.

A ce jour on ne dispose d’aucun cryptage à clé publique qui soit sûr !



A ce jour on ne dispose d’aucun cryptage à clé publique qui soit sûr !

Tous les codages connus sont menacés à plus ou moins long terme !

A ce jour on ne dispose d’aucun cryptage à clé publique qui soit sûr !

Tous les codages connus sont menacés à plus ou moins long terme !

Personne ne peut prédire combien de temps ils tiendront !

A ce jour on ne dispose d’aucun cryptage à clé publique qui soit sûr !

Tous les codages connus sont menacés à plus ou moins long terme !

Personne ne peut prédire combien de temps ils tiendront !

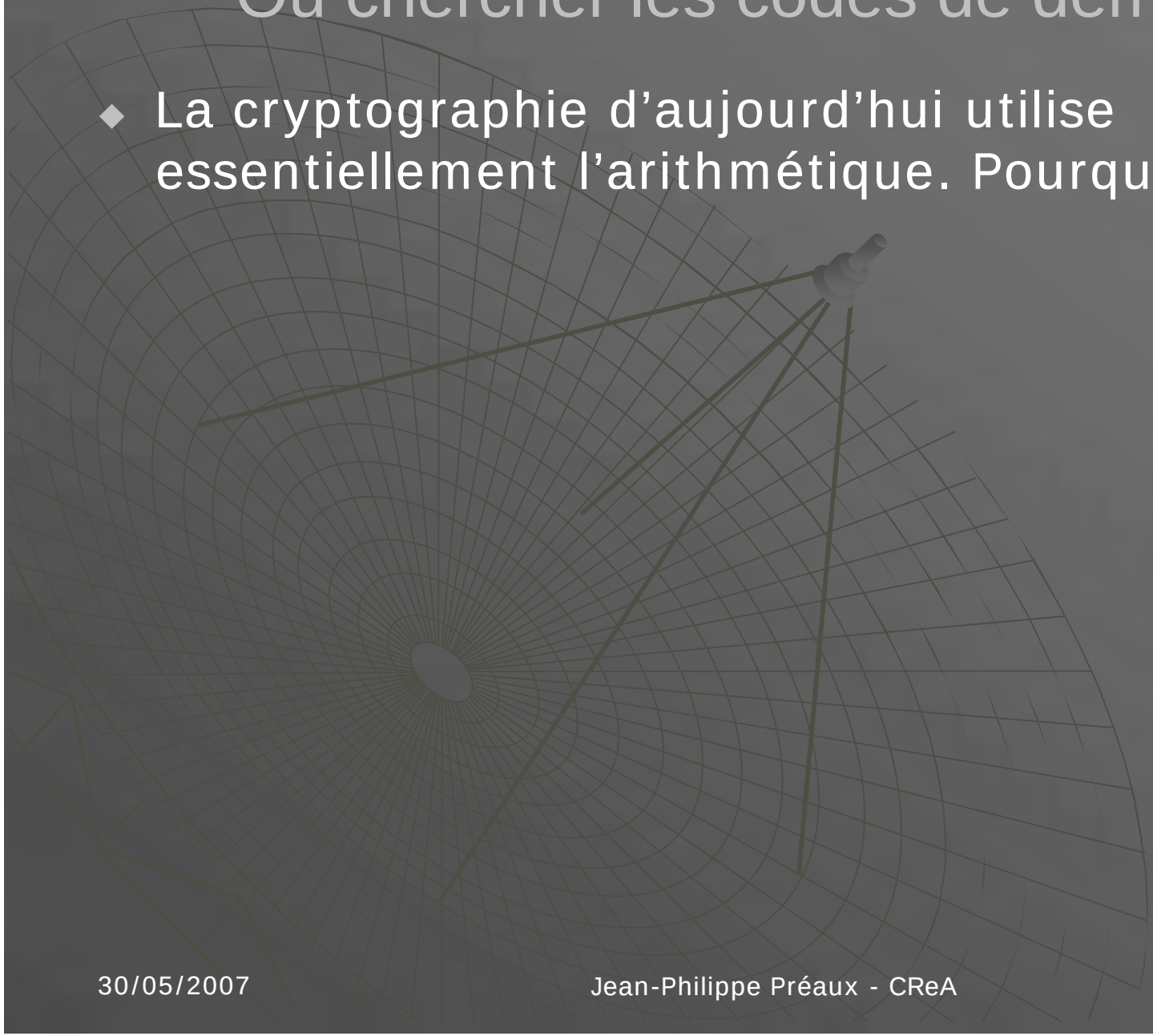
Combler leurs failles rend les protocoles plus lourds à implémenter !

Cryptographie de demain

- A ce jour tout est arithmétique. Pourquoi ?
- Où chercher les codes de demain ?
- Pourquoi la théorie des groupes ?

Où chercher les codes de demain ?

- La cryptographie d'aujourd'hui utilise essentiellement l'arithmétique. Pourquoi ?



Où chercher les codes de demain ?

- La cryptographie d'aujourd'hui utilise essentiellement l'arithmétique. Pourquoi ?
- En arithmétique, de nombreuses opérations sont faciles et rapides à implémenter : +,x,...
- D'autres, même si elles sont calculables, semblent très difficiles et longues à réaliser : comme factoriser un grand nombre en facteurs premier : multiplier P et Q pour obtenir N est rapide. Tester si N=PQ semble difficile et lent.

Où chercher les codes de demain ?

- La cryptographie d'aujourd'hui utilise essentiellement l'arithmétique. Pourquoi ?
- En arithmétique, de nombreuses opérations sont faciles et rapides à implémenter : +,x,...
- D'autres, même si elles sont calculables, semblent très difficiles et longues à réaliser : comme factoriser un grand nombre en facteurs premier : multiplier P et Q pour obtenir N est rapide. Tester si N=PQ semble difficile et lent.
- Cependant aucun théorème n'assure que des problèmes considérés comme difficiles aujourd'hui le seront encore demain... ? P=NP ?

Où chercher les codes de demain ?

- Depuis une poignée d'année, toute l'attention se porte sur la théorie des groupes. Le nombre de publications, conférences, financements, d'application de la théorie des groupes à la cryptographie a explosé.

Où chercher les codes de demain ?

- Depuis une poignée d'année, toute l'attention se porte sur la théorie des groupes. Le nombre de publications, conférences, financements, d'application de la théorie des groupes à la cryptographie a explosé.
- Dans ce domaine, le protocole de Ko-Lee a attiré toute l'attention… Jusqu'à ce qu'on trouve sa faille.
- Il a en tout cas depuis inspiré une pléthore de recherches en théorie des groupes sur la cryptographie.

Où chercher les codes de demain ?

- Depuis une poignée d'année, toute l'attention se porte sur la théorie des groupes. Le nombre de publications, conférences, financements, d'application de la théorie des groupes à la cryptographie a explosé.
- Dans ce domaine, le protocole de Ko-Lee a attiré toute l'attention… Jusqu'à ce qu'on trouve sa faille.
- Il a en tout cas depuis inspiré une pléthore de recherches en théorie des groupes sur la cryptographie.
- Celà pourrait mener à un codage parfaitement sûr…

Pourquoi les groupes

- Un groupe est un espace abstrait dans lequel on peut multiplier ses éléments.
- Etudiés depuis le début du siècle, de nombreux outils ont été développés et ils sont bien compris, bien qu'innombrables.

Pourquoi les groupes

- Un groupe est un espace abstrait dans lequel on peut multiplier ses éléments.
- Etudiés depuis le début du siècle, de nombreux outils ont été développés et ils sont bien compris, bien qu'innombrables.
- Les groupes se prêtent très bien au calcul informatique. Il y a en outre une longue tradition algorithmique dans les groupes.
- On connaît des algorithmes rapides pour effectuer certains calculs dans certains groupes.
- On connaît surtout des problèmes algorithmiques très difficiles, voire insolubles (donc incassables) !
- Ils sont centraux en mathématiques !

Pourquoi les groupes ?

- En général un groupe est donné par un alphabet et des relations. Un élément du groupe est donné par un mot sur l'alphabet. Deux mots représentent le même élément si l'on peut transformer l'un en l'autre à l'aide des relations.

Pourquoi les groupes ?

- En général un groupe est donné par un alphabet et des relations. Un élément du groupe est donné par un mot sur l'alphabet. Deux mots représentent le même élément si l'on peut transformer l'un en l'autre à l'aide des relations.
- Ex : Le groupe Z+Z des couples d'entiers, munis de l'addition usuelle est :

$$Z+Z = \langle a,b \mid ab=ba \rangle$$

  - Montrons que aab=baa :
  - aab = a ab = a ba = ab a= ba a= baa

Pourquoi les groupes ?

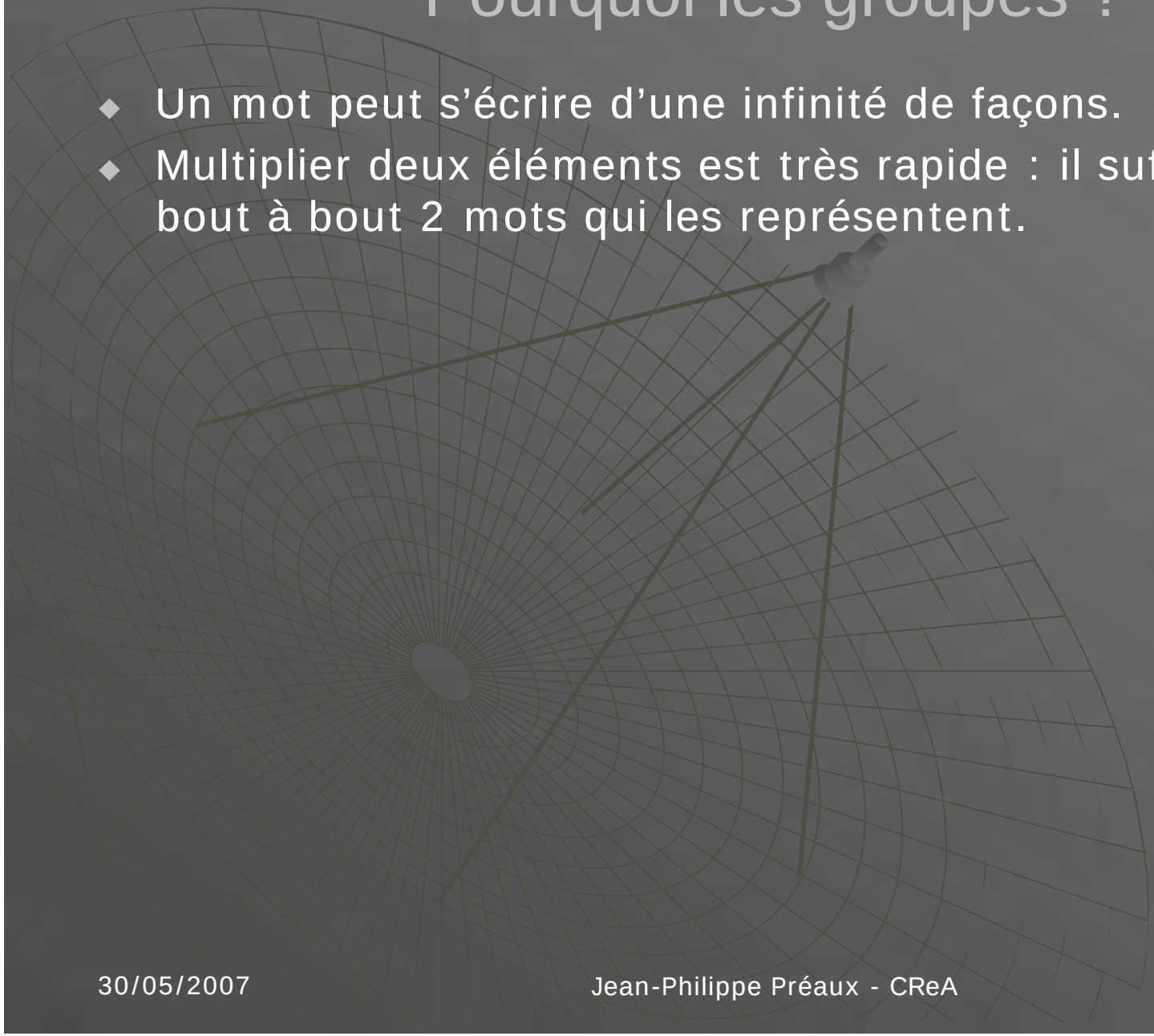
- En général un groupe est donné par un alphabet et des relations. Un élément du groupe est donné par un mot sur l'alphabet. Deux mots représentent le même élément si l'on peut transformer l'un en l'autre à l'aide des relations.
- Ex : Le groupe Z+Z des couples d'entiers, munis de l'addition usuelle est :

$$Z+Z = \langle a,b \mid ab=ba \rangle$$

  - Montrons que aab=baa :
  - aab = a ab = a ba = ab a= ba a= baa
- Un élément du groupe peut s'écrire d'une infinité de façons différentes. Pratique pour 'déguiser' l'élément.

Pourquoi les groupes ?

- Un mot peut s’écrire d’une infinité de façons.
- Multiplier deux éléments est très rapide : il suffit de mettre bout à bout 2 mots qui les représentent.



Pourquoi les groupes ?

- Un mot peut s'écrire d'une infinité de façons.
- Multiplier deux éléments est très rapide : il suffit de mettre bout à bout 2 mots qui les représentent.
- Dans certains groupes il est impossible de décider algorithmiquement si deux mots quelconques représentent le même élément.
- Dans certains groupes il est impossible de décider algorithmiquement si pour 3 éléments P,Q,N, on a N=PQ. Comparer à RSA !

Pourquoi les groupes ?

- Un mot peut s'écrire d'une infinité de façons.
- Multiplier deux éléments est très rapide : il suffit de mettre bout à bout 2 mots qui les représentent.
- Dans certains groupes il est impossible de décider algorithmiquement si deux mots quelconques représentent le même élément.
- Dans certains groupes il est impossible de décider algorithmiquement si pour 3 éléments P,Q,N, on a N=PQ. Comparer à RSA !
- Il suffirait d'appliquer des techniques analogues à RSA dans un groupe judicieusement choisi : tout est là. Le choix judicieux d'un groupe pourrait raisonnablement aboutir à un codage sûr. Ou du moins à un codage où un théorème affirme que pour le casser un pirate doit effectuer au moins X opérations (X très grand et connu)

FIN

Dr. Jean-Philippe Préaux
CReA / Univ. de Provence
jpreaux@cr-ea.net
http://www.cmi.univ-mrs.fr/~preaux