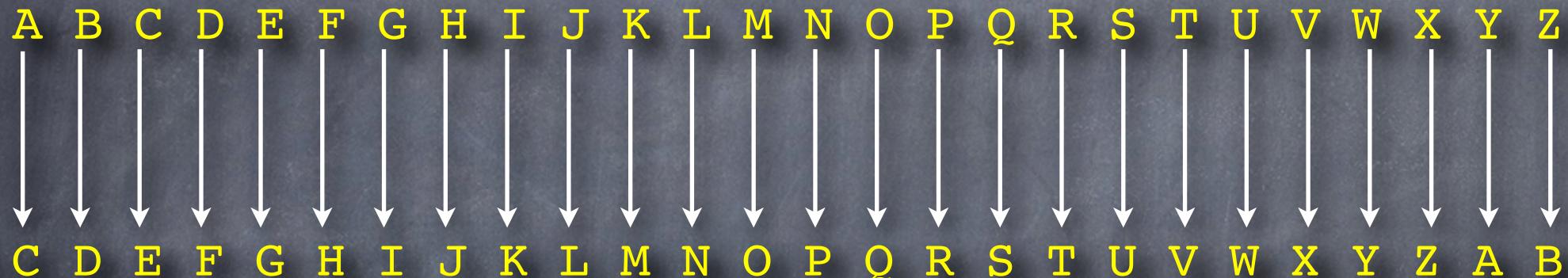


bcLéu'swrjucsklgLfgLàhvcuLd
cxmrxufakxl

La cryptographie* de César à aujourd'hui

* de κρυπτός qui veut dire caché

LE CODE DE CÉSAR



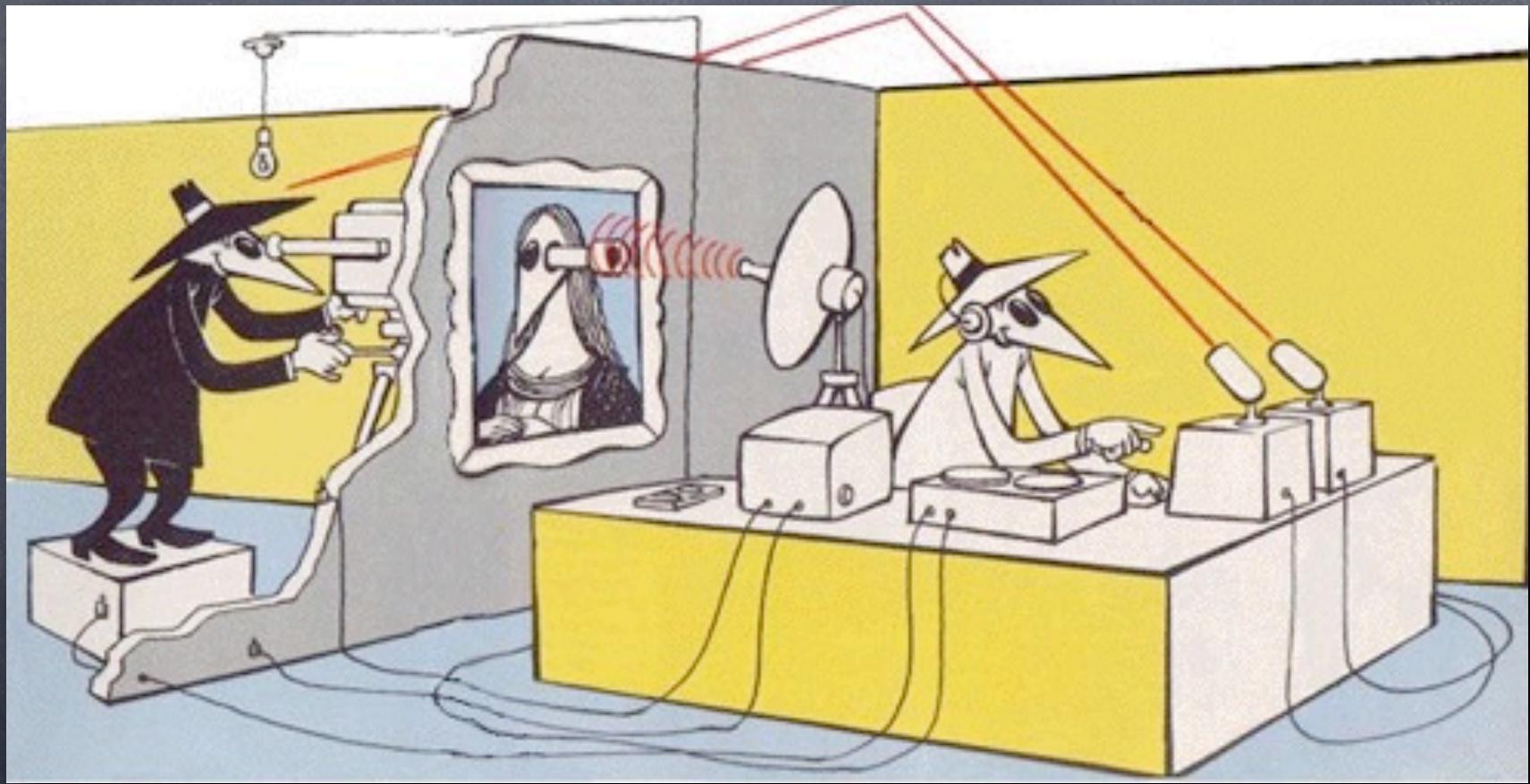
VQWVG



CNGC LCEVC GUV



COMMENT BRISER UN CODE À LA CÉSAR ? TROUVER LA CLÉ



R P R W T

B

QOQVS

C

PNPUR

D

OMOTQ

E

NLNSP

F

MKMRO

G

H

I

J

K

LJLQN

KIKPM

JHJOL

IGINK

HFHMJ

L

M

N

O

P

GEGLI

FDFKH

ECEJG

DBDIF

CACHE

Q

R

S

T

U

BZBGD

AYAFC

ZXZEB

YWYDA

XVXCZ

V

W

X

Y

Z

WUWBY

VTVAX

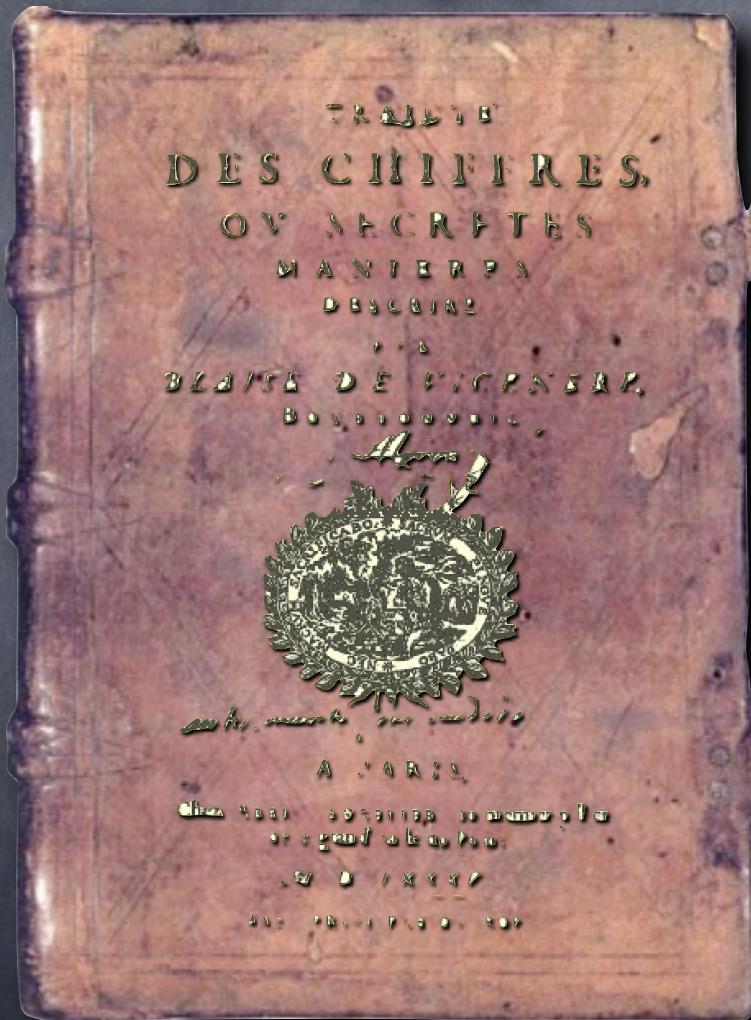
USUZW

TRTYV

SQSXU

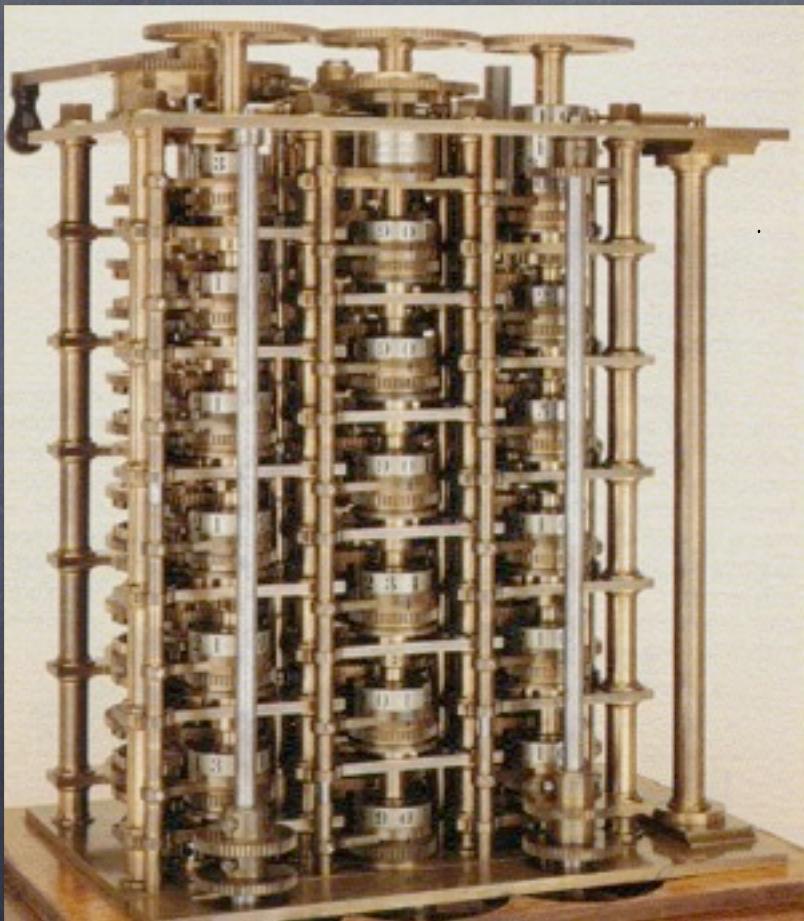
D'AUTRES SYSTÈMES CRYPTOGRAPHIQUES

LE CHIFFRE INDESCHIFFRABLE



BLAISE DE VIGENÈRE
(1523 - 1596)

DIFFERENCE ENGINE #1 (1827)



CHARLES BABBAGE
(1791 - 1871)

SHERLOCK HOLMES : "LES HOMMES DANSANTS"



A	H	P
B	I	R
C	L	S
D	M	T
E	N	V
G	O	Y

LA CLÉ



SIR ARTHUR CONAN DOYLE
(1859 - 1930)

L'ANALYSE DE FRÉQUENCE



Abu Yusuf Ya'qub ibn Is-haq ibn
as-Sabbah Oòmrana ibn Ismaïl al-Kindi
(801-873)

نَاسِمَ الْحَدَّادِ، وَالْجُهْرِ، تَصَفُّ مَا كَلَمَ بِالْمُتَوَاهِرَةِ مِنْ هُوَ الْأَوَّلُ لِمُهَمَّةِ الْجَهَارِ
عَنْ مَا يَلْمِمُهُ الْأَيْمَانُ، وَهُوَ صَبِيٌّ يَجْعَلُ فِي سُطُونِ الْجَهَارِ عَسْلَمَةَ، حَالِمَ الْأَقْمَمَ، وَهُوَ طَلَابُ
مَا يَعْسُلُ الْجُهْرَ وَيَجْعَلُهُ دُورُ الْجَهَارِ لِمُغْصَفِ الْمُلْمَسَةِ، وَعَالِمَ الْجَهَارِ وَسَخْلَةَ
لِمُجْرِيَّصِيَّهِ، وَعَالِمَ الْجَهَارِ مُصْعِدَ الْجَهَارِ الْمُسَيَّبَةِ، وَالْجَهَارِ الْجَهَارِ الْمُسَيَّبَةِ
مِنْ الْجَهَارِ الْجَهَارِ دَكَّوكَ الْجَهَارِ، وَالْجَهَارِ الْجَهَارِ دَكَّوكَ الْجَهَارِ مِنْ الْجَهَارِ الْجَهَارِ
دَسَسَ الْجَهَارِ، وَبَلَقَ الْجَهَارِ وَلَقَهُ، الْجَهَارِ وَجَهَ، وَالْجَهَارِ الْجَهَارِ بِكَالْجَهَارِ،
أَسْمَرَ الْجَهَارِ بِكَالْجَهَارِ، أَسْمَرَ الْجَهَارِ بِكَالْجَهَارِ، الْجَهَارِ الْجَهَارِ

لِرَالَّهِ - وَلِلَّهِ اللَّهِ - وَالْعَالَمِيَّصِلِّيَّ اَسْمَاعِيَّهِ مُحَمَّدَ وَلِلَّهِ

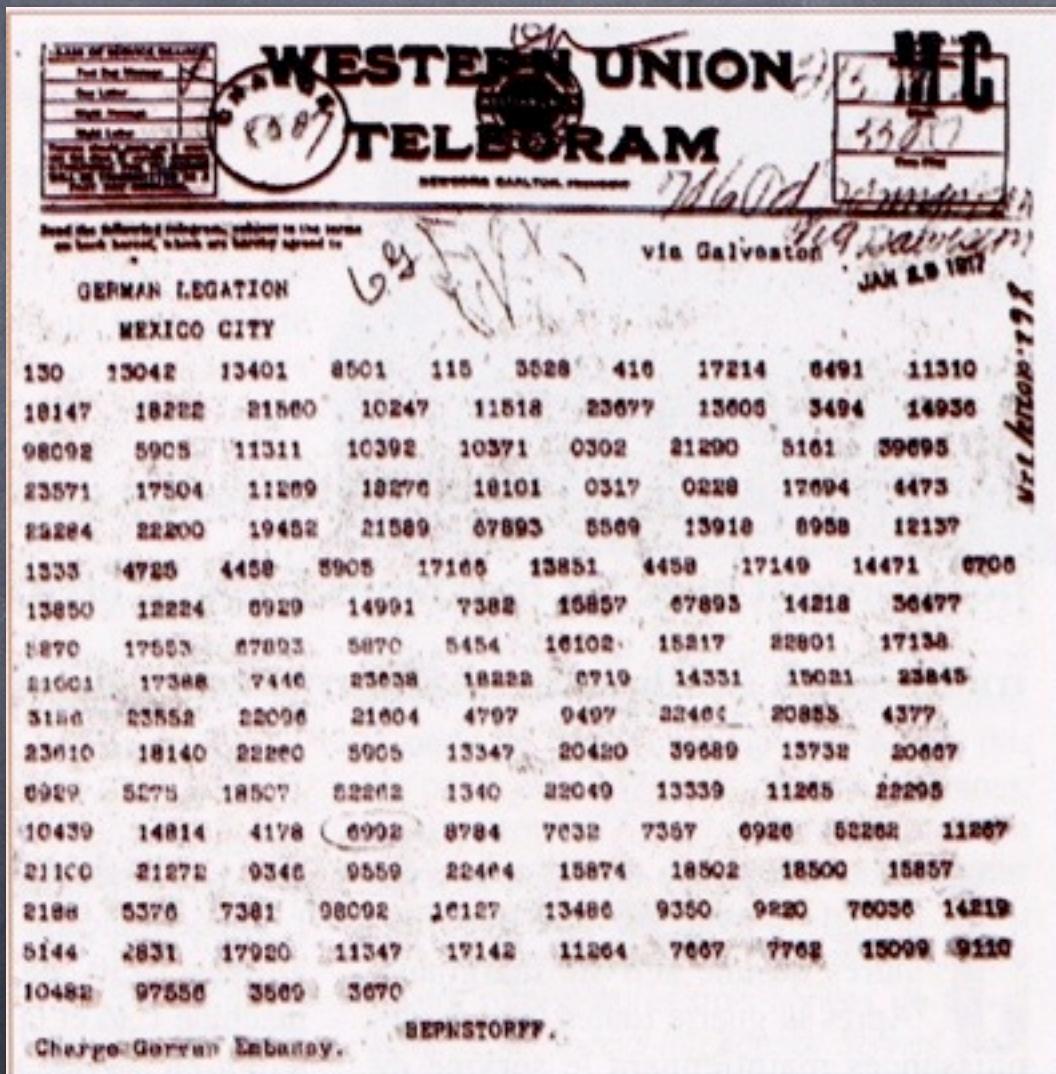
لِسَمَاءِ الْجَهَارِ - مُحَمَّدَ وَلِلَّهِ
وَسَادَ الْجَهَارِ مُصَبِّرَ الْجَهَارِ، اَسْفَلَ الْجَهَارِ الْجَهَارِ
لِهَمَدَ مُحَمَّدَ وَلِلَّهِ قَرْعَلَ الْجَهَارِ، وَكَاتَ مَكَارِدَهِ الْجَهَارِ اَسْجُونَهِ مَارِدَهِ
كَالْجَهَارِ الْجَهَارِ وَلِلَّهِ قَرْعَلَ الْجَهَارِ، مَكَارِدَهِ اَدَرِسَهِ اَكْمَنَهِ قَعْدَهِ
عَنْهُلَّهِ اَسْلَمَهِ، وَلِلَّهِ قَرْعَلَهُ وَسَكَّلَهُ اَشْخَرَهُ اَنْوَسَهِ وَسَدَّهُ اَصْنَعَهُ
الْجَهَارِ، وَسَعْلَهُ وَالْجَهَارِ وَقَهَّهُ، وَلِلَّهِ لَيْلَهُ اَنْتَهَرَهُ، وَاصْلَمَهُ لِرَالَّهِ الْجَهَارِ
لِرَطْبَرِ الْجَهَارِ اَدَبِهِزَهُ، اَفْلَسَهُ اَسْنَاقَهِ وَالْجَهَارِ، اَسْطَلَهُ وَصَمَّهُ الْجَهَارِ
مُجْهَلَهُ مَنَاهَهُ، وَلِلَّهِ قَرْعَلَهُ وَصَرَعَهُ اَسْهَمَهُ اَنْوَهُهُ، اَعْلَمَهُ وَالْجَهَارِ وَلِلَّهِ
سَهَّلَهُهُ وَلِلَّهِ اَسْفَلَهُهُ اَسْبَلَهُهُ، وَلِلَّهِ اَنْطَلَهُهُ وَلِلَّهِ اَسْرَعَهُهُ اَسْرَعَهُ
مُلَاحَمَهُهُ لِلَّهِ اَلَّا، وَلِلَّهِ اَصْمَمَهُهُ طَلَقَهُ اَسْسَرَهُهُ بِسَلَامَهُهُ اَسْلَمَهُهُ
اَسْمَسَهُهُ، وَلِلَّهِ اَسْهَمَهُهُ بِجَهَارِهِ طَرَمَهُ اَسْهَمَهُهُ لِرَالَّهِ اَسْهَمَهُهُ طَرَمَهُ
بِاسْمَهُهُ، وَلِلَّهِ اَسْهَمَهُهُ بِجَهَارِهِ طَرَمَهُ اَسْهَمَهُهُ لِرَالَّهِ اَسْهَمَهُهُ طَرَمَهُ
عَلَيْهِ، الْجَهَارِ اَسْهَمَهُهُ بِجَهَارِهِ طَرَمَهُ اَسْهَمَهُهُ بِجَهَارِهِ طَرَمَهُ وَرِسْمَهُهُ
دَهَّلَهُ اَسْهَمَهُهُ بِسَطَانِهِ الطَّهَرِ، لِاَسْلَالِهِ وَلِلَّهِ اَسْهَمَهُهُ، لِرَدَدِهِ وَلِلَّهِ اَسْهَمَهُهُ
مُهَمَّهُهُ اَلْجَهَارِ، وَلِلَّهِ اَسْهَمَهُهُ، لِرَدَدِهِ وَلِلَّهِ اَسْهَمَهُهُ، اَهْنَتَهُ اَسْهَمَهُهُ اَلْجَهَارِ
كَسَّا اَلْجَهَارِ، اَهْمَلَهُ اَلْجَهَارِ، وَلِلَّهِ اَسْهَمَهُهُ، اَهْنَتَهُ اَلْجَهَارِ، وَلِلَّهِ اَسْهَمَهُهُ
اَلْجَهَارِ، وَلِلَّهِ اَسْهَمَهُهُ، لِاَسْلَالِهِ وَلِلَّهِ اَسْهَمَهُهُ، اَهْنَتَهُ اَلْجَهَارِ،
وَلِلَّهِ اَسْهَمَهُهُ، لِاَسْلَالِهِ وَلِلَّهِ اَسْهَمَهُهُ، اَهْنَتَهُ اَلْجَهَارِ، وَلِلَّهِ اَسْهَمَهُهُ
صَصَصَهُهُ اَلْجَهَارِ، وَلِلَّهِ اَسْهَمَهُهُ، اَهْنَتَهُ اَلْجَهَارِ، وَلِلَّهِ اَسْهَمَهُهُ
بِالْسَّوَادِيَّاتِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ
بِلِلَّهِ اَلْجَهَارِ، وَلِلَّهِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ
بِالْجَهَارِ، وَلِلَّهِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ، وَلِلَّهِ اَلْجَهَارِ، اَلْجَهَارِ اَلْجَهَارِ

DES SYSTÈMES DE PLUS EN PLUS COMPLEXES

François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

1^{re} GUERRE MONDIALE, ALLEMAGNE → MEXIQUE, 1917.



François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

1^{re} GUERRE MONDIALE, ALLEMAGNE → MEXIQUE, 1917.

" Nous avons l'intention de déclencher à partir du 1er février une guerre sous-marine totale. Malgré cela, nous tenterons de maintenir les Etats-Unis dans la neutralité. Si nous n'y parvenons pas, nous proposerons au Mexique une alliance sur les bases suivantes : faire la guerre ensemble, faire la paix ensemble, large soutien financier et accord de notre part pour la reconquête par le Mexique des territoires perdus du Texas, du Nouveau Mexique, et de l'Arizona. Le règlement des détails est laissé à vos soins. Vous informerez secrètement le Président du Mexique dès que l'entrée en guerre des Etats-Unis sera certaine, et vous lui suggérerez que, sous sa propre initiative, il peut immédiatement solliciter la participation du Japon, et en même temps servir de médiateur entre le Japon et nous-même. Prière d'attirer l'attention du Président sur le fait que l'emploi sans limites de nos sous-marins offre désormais la possibilité d'obliger l'Angleterre à faire la paix dans peu de mois."

1^{re} GUERRE MONDIALE, ALLEMAGNE → MEXIQUE, 1917.

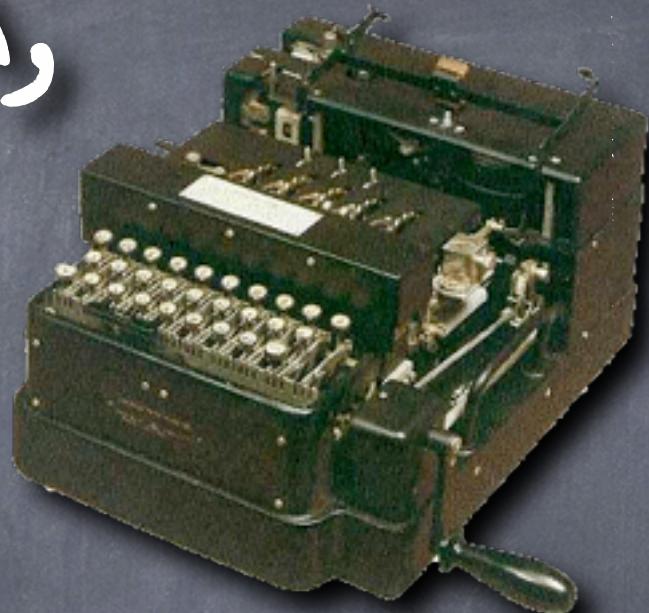
Décrypté par les britanniques le 22 février 1917, après un mois de travail.
Cela mènera les États-Unis à déclencher leur participation à la guerre contre l'Allemagne le 6 avril 1917.

LA MACHINE ENIGMA, 2^e GUERRE MONDIALE.

La machine de codage des allemands, leur agents secrets, l'armée, les SS, etc...

Nombre de position de codage:

3,283,883,513,796,974,198,700,882,
069,882,752,878,379,955,261,095,
623,685,444,055,315,226,006,433,
616,627,409,666,933,182,371,154,
802,769,920,000,000,000



LES POLONAIS, PUIS LES ANGLAIS,
ONT RÉUSSIS À DÉCODER LES
MESSAGES DES ALLEMANDS ...

CES SYSTÈMES DE CRYPTOGRAPHIE
SONT VULNÉRABLES si ON A
ACCÈS À UN ASSEZ GRAND
NOMBRE DE MESSAGES.

L'ORDINATEUR MODERNE



2.25×10^9
OPÉRATIONS
PAR SECONDES

2041
TÉMOINÉZ

1 000 000 000 000 000
Fais Plus RAPIDE

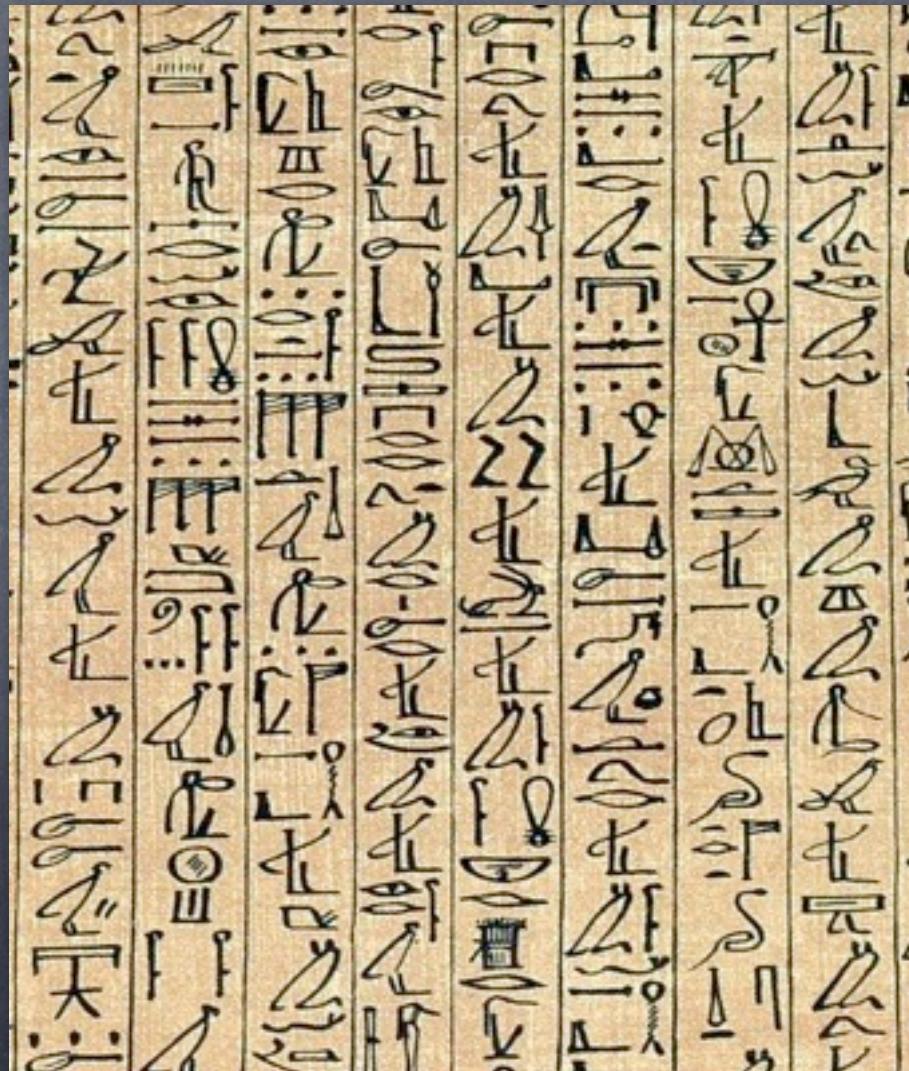
François BERGERON, DEPT. MATH, UQAM

AUTRES UTILISATIONS DES OUTILS MATHÉMATICO-INFORMATIQUES DÉVELOPPÉS.

François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

DÉCODER LES HiÉROGLYPHES

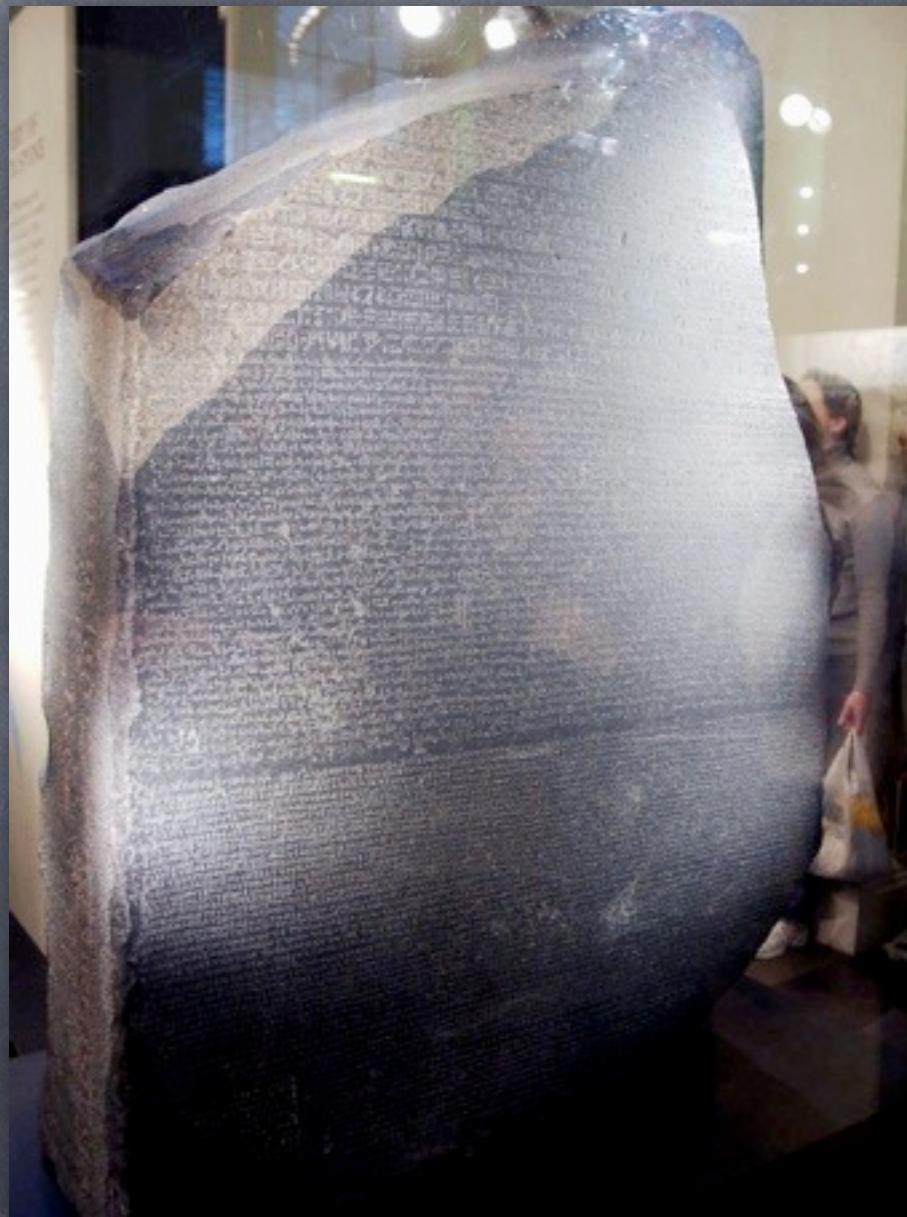


DÉCODER LES HiÉROGlyPHES

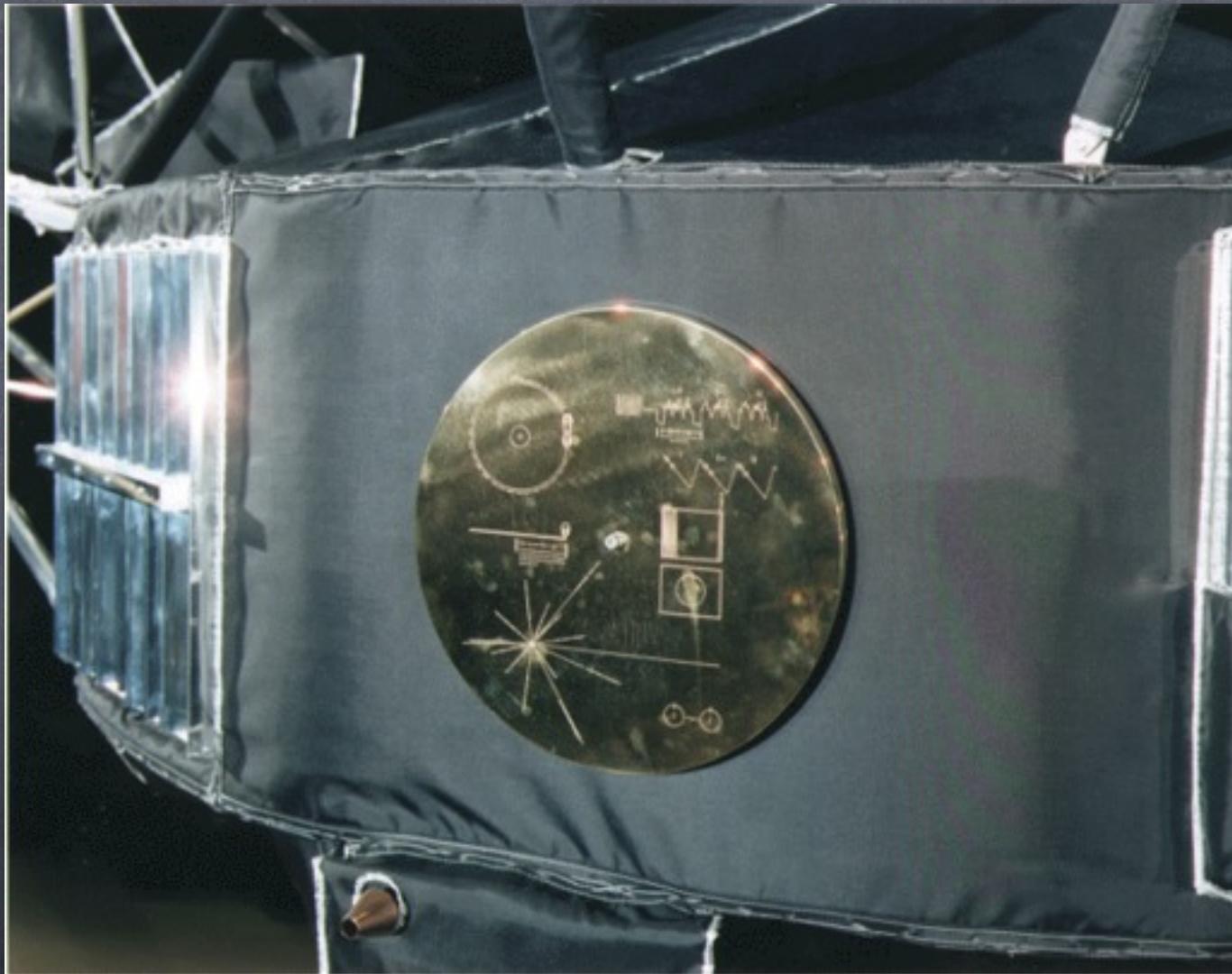
LA PIERRE DE
ROSETTE



Jean-François
Champollion
(1790-1832)



DES CODES POUR LES EXTRATERRESTRES



François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

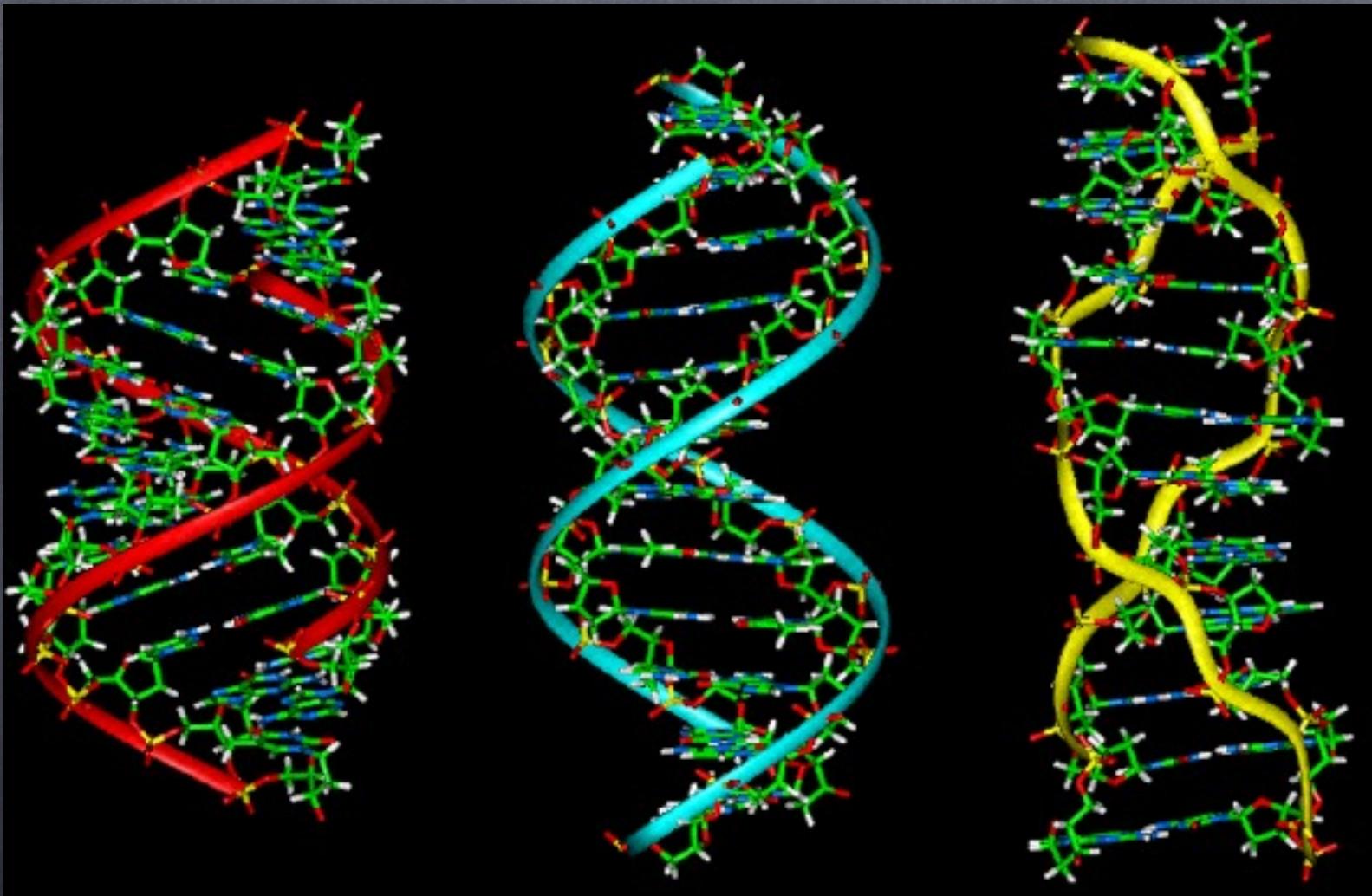
DÉCODER LES EXTRATERRESTRES



François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

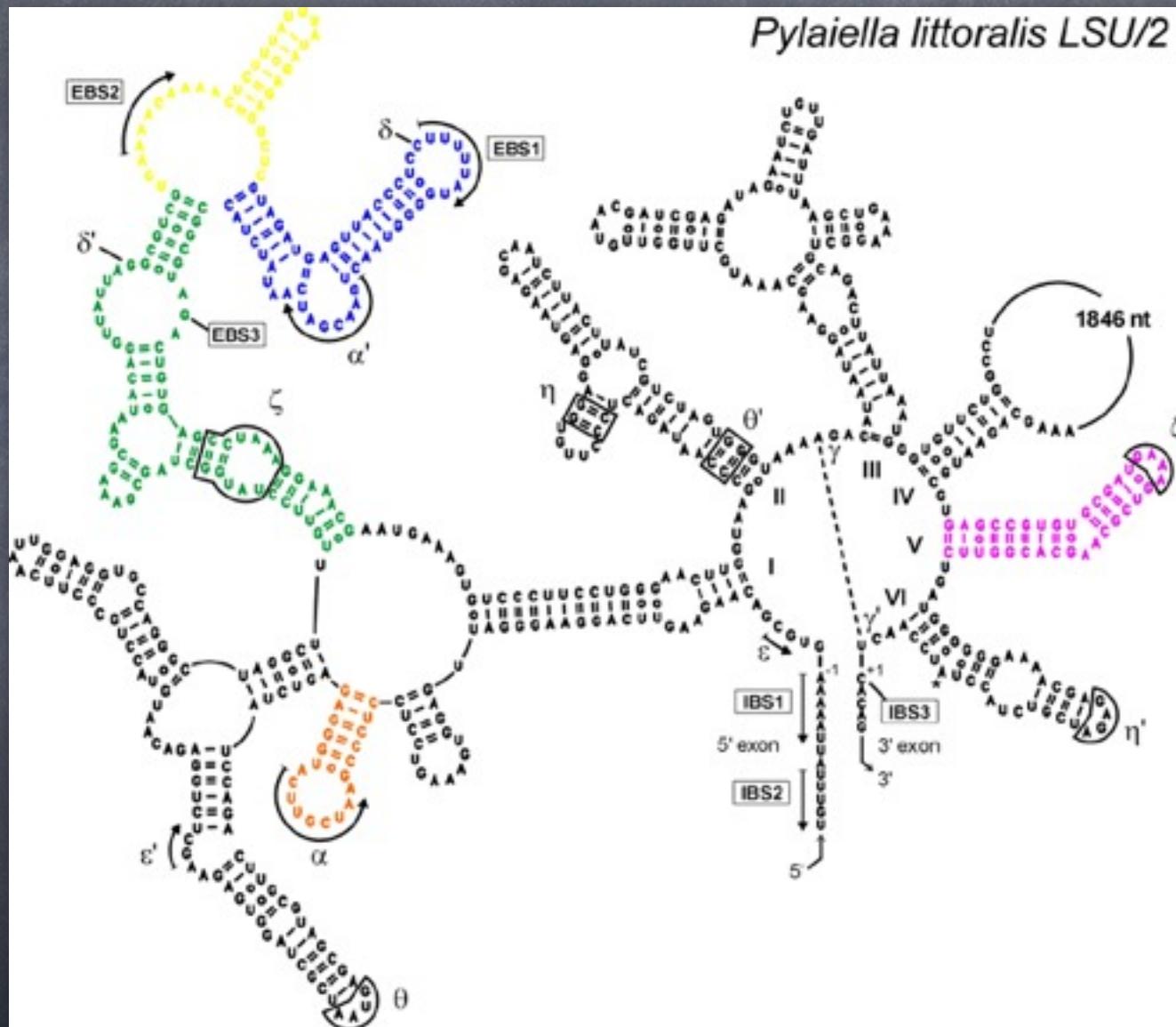
DÉCODER LE GÉNOME



François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

DÉCODER LE GÉNOME



François BERGERON, DEPT. MATH, UQAM

LA CRYPTOGRAPHIE MODERNE

François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

CYPTOGRAPHIE À CLÉS PUBLIQUES



François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

Cryptographie à clés publiques

- LA MÉTHODE DE CODAGE EST CONNUE DE TOUS.
- "SEUL" LE DESTINATAIRE PEUT DÉCODER LE MESSAGE CODE.
- LE CODAGE ET LE DÉCODAGE * SE FONT RAPIDEMENT.
- ON PEUT ENVOYER DES MESSAGES AUSSI LONGS QUE VOULU Si on connaît une information secrète METTRE LE SYSTÈME EN PERIL.

CALCUL DE MODULO

François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

CALCUL DE MODULO

$$(213 \bmod 10) = 3$$

$$(213 \bmod 12) = 9$$

$$(213 \bmod 24) = 21$$

$b = (a \bmod n)$ SIGNIFIE QUE

b EST LE RESTE DE
LA DIVISION DE
 a PAR n

CALCUL MODULO n

Si $(A \bmod n) = (a \bmod n)$
 $(B \bmod n) = (b \bmod n)$

Alors

$$(A+B \bmod n) = (a+b \bmod n)$$
$$(A \cdot B \bmod n) = (a \cdot b \bmod n)$$
$$(A^k \bmod n) = (a^k \bmod n)$$

À CALCULER MODULO 100

$3^{4005} =$

742378100761437674254482911596034763672844703194862983410686366203
833621965291749982896196686484518958259942842842644662587311190713
851146041936989307942425056392811748081991577526066640999363476680
86414233904489620132930698559993597751955945262768594838860134631
31672791849506237974396633509345085837881454217705438380057184425
898068851013046516711459508887220242614739983091267564396496088987
04616941205669064333001303451964948880544307655029172800534942880
38146162212069375094404539847012408699426299777813062286146192034
85249072903042165427365288359510198527982937844720108126519712523
85787781072741847029156104268099815733412492860937326916696868688
178197944726424981469262768096865030169335324831304811368293503686
663549196171890768324231171409999387054012750417077477132972019107
66301314977932292368038234265544132896348637366720846141301397509
560809819759475008211692551418241179684233636063104597371044077212
33625836078518207385051316503836082199897516206902797141526388967
959807912387482199333213832923264335184049021205139215053911127598
06000324120550978814064087304441808799262057313883823362015164444
70813504290096184071690296200359494792233790135569293745844496796
69034278577373728913158657704315491779000100105413772021644718878
81468820712768053515832367552617890856835174213506488221450906269
15175043784931704996071202000562553604055488831534301398365768720
47633071832019625694035082342164734513529264897297470514330758050
290419568851492897616111416492039293001103158148280091499080613795
455009470962093671721705827848500599668355806760480795151194614791
08375356974085615307524585293205739056891359629859284709241480618
47728782038416770660483221178546807893342728768614292672281688876
67337187158562183779208192405487484909908073046203354742056725918
487889321471098977605165343323921155693891956215276546995026395116
07098967307833833755756990222701067072546831802959323821366377872
89742473840243

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (3 (3^{15} \bmod 100)^2 \bmod 100)$$

$$(3^{15} \bmod 100) = (3 (3^7 \bmod 100)^2 \bmod 100)$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (3 (3^{15} \bmod 100)^2 \bmod 100)$$

$$(3^{15} \bmod 100) = (3 (2187 \bmod 100)^2 \bmod 100)$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (3 (3^{15} \bmod 100)^2 \bmod 100)$$

$$(3^{15} \bmod 100) = (3 (87)^2 \bmod 100)$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (3 (3^{15} \bmod 100)^2 \bmod 100)$$

$$(3^{15} \bmod 100) = (3 \cdot 7569 \bmod 100)$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (3 (3^{15} \bmod 100)^2 \bmod 100)$$

$$(3^{15} \bmod 100) = (22707 \bmod 100)$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (3 (3^{15} \bmod 100)^2 \bmod 100)$$

$$(3^{15} \bmod 100) = 7$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (3 (7)^2 \bmod 100)$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = (147 \bmod 100)$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = ((3^{31} \bmod 100)^2 \bmod 100)$$

$$(3^{31} \bmod 100) = 47$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = (3 (3^{62} \bmod 100)^2 \bmod 100)$$

$$(3^{62} \bmod 100) = 9$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = ((3^{125} \bmod 100)^2 \bmod 100)$$

$$(3^{125} \bmod 100) = 43$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = ((3^{250} \bmod 100)^2 \bmod 100)$$

$$(3^{250} \bmod 100) = 49$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = (3 (3^{500} \bmod 100)^2 \bmod 100)$$

$$(3^{500} \bmod 100) = 1$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = ((3^{1001} \bmod 100)^2 \bmod 100)$$

$$(3^{1001} \bmod 100) = 3$$

Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = (3 (3^{2002} \bmod 100)^2 \bmod 100)$$

$$(3^{2002} \bmod 100) = 9$$

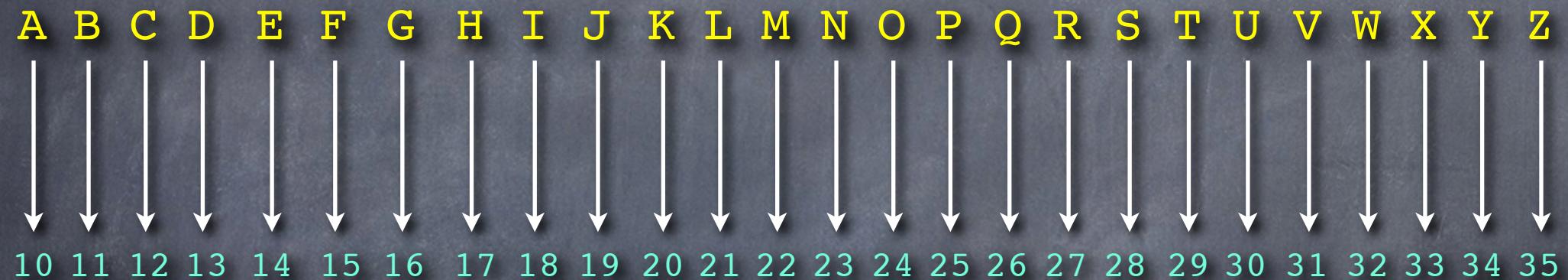
Exponentiation RAPIDE MODULO $n=100$

$$(3^{4005} \bmod 100) = 43$$

LE SYSTÈME RSA

François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13



ABRACADABRA

(10, 11, 27, 10, 12, 10, 13, 10, 11, 27, 10)

$$\mathcal{M} = 1011271012101310112710$$

LE SYSTÈME RSA



Rivest, Shamir, Adleman (1977)
(2003)

CODAGE $m \longrightarrow c = (m^e \bmod n)$

DÉCODAGE $c \longrightarrow m = (c^h \bmod n)$

POUR SE CONSTRUIRE UNE CLÉ
ON SE CHOISIT DEUX GRANDS
NOMBRES PREMIERS

 $p =$

913902128079995508420979283933
9950865492110849686519861047978

 $q =$

55827109843033411493792496
5487299024960457275829277553000
16964

"TOP SECRET!" "TOP SECRET!"

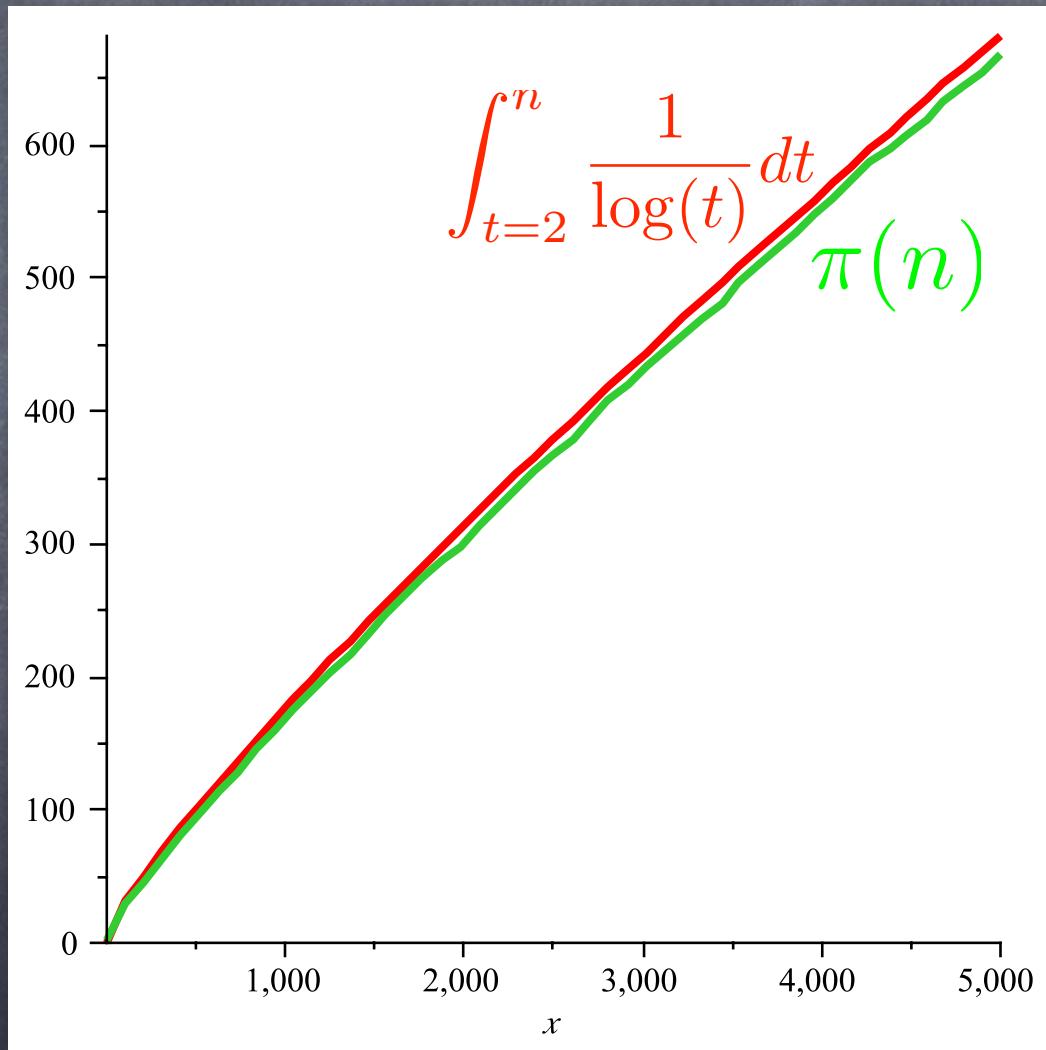
QU'ON GARDE SECRETS



CARL FRIEDRICH GAUSS (1777 - 1855)

François BERGERON, DEPT. MATH, UQAM

THÉORÈME DES NOMBRES PREMIERS



IL Y A AU MOINS

195749131700000000000000000000000000000000
00
00
00
00
00

NOMBRE Premiers DE
200 CHIFFRES

C'EST \sim 196 FOIS PLUS GRAND
QUE LE NOMBRE D'ATOMES DANS
L'UNIVERS OBSERVABLE.

Pour le codage

CALCULER m EN Multipliant
 p ET q

$m = 3530077361882448142729008764302657633090807756$
6841536554471443803162568247004783252409970439
2825688399971668487048756462309933330394616119
178578931081472702153607465462868484508727

Choisir e (l'algorithme d'Euclide)

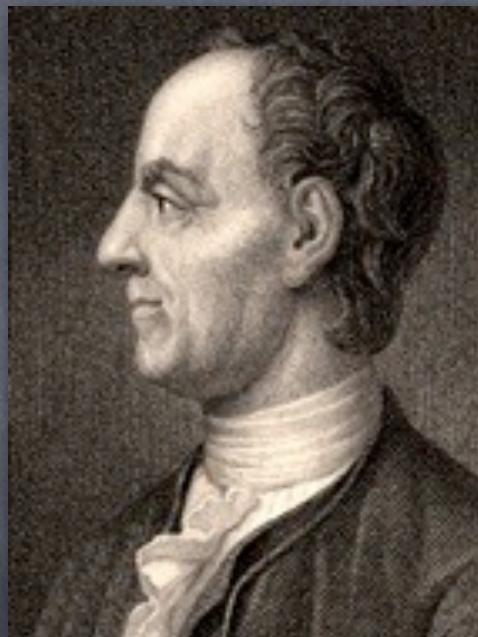
$$\text{PGCD}(e, (p-1)(q-1)) = 1$$

$e = 150650905007553408748182082815984929359632269$
852681585809504709739738485231104248045693804
710098188302655538010818866476054310788175542
136407374106205605523687223946800025812242019

LE THÉORÈME D'EULER - FERMAT



Pierre de Fermat
(1601-1665)



Leonhard Euler
(1707-1783)

LE THÉORÈME D'ÉULER-FERMAT

POUR DES NOMBRES PREMIERS p ET q

SI a NE SE DIVISE NI PAR p

NI PAR q , ALORS

$$(a^k \bmod pq) \equiv a$$

EXACTEMENT
QUAND

$$\left(\bmod (-1)(-1) \right) = 1$$

Pour le décodage

CALCULES
QUE **TOP SECRET!** SECÈMENT h TEL
 $h = 272908\ldots 6934878229217801120\ldots 1646454$
 $\ldots 3\ldots 894855412667939050\ldots 9\ldots 392216103$
 $\ldots 8894683760749895638\ldots 4384927721690$
 $\ldots 638511237029583823313697\ldots 0855228779$

TOP SECRET!

IL EST TRÈS DIFFICILE DE
CALCULER h SEULEMENT À PARTIR
DE m ET e

LE SYSTÈME RSA

CODAGE $m \rightarrow c = (m^e \bmod n)$

DÉCODAGE $c \rightarrow m = (c^h \bmod n)$

$$m = (m^{e^h} \bmod n)$$

31074182404900437213507500358885679300373460228427
27545720161948823206440518081504556346829671723286
78243791627283803341547107310850191954852900733772
4822783525742386454014691736602477652346609

=

1634733645809253848443133883865090859841783670033
092312181110852389333100104508151212118167511579

×

1900871281664822113126851573935413975471896789968
515493666638539088027103802104498957191261465571

30 ANNÉES DE CALCUL
(5 MOIS SUR UNE BANQUE
D'ORDINATEURS)

François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

ON NE SAIT PAS CALCULER*

p ET q TELS QUE

74037563479561712828046796097429573142593188889231

28908493623263897276503402826627689199641962511784

39958943305021275853701189680982867331732731089309

00552505116877063299072396380786710086096962537934

650563796359 = $p \times q$

* DANS UN TEMPS
RAISONABLE

LE SYSTÈME RSA EXPLORÉ
CETTE DIFFICULTÉ.

UTILISATIONS DE RSA



Alice



$(n(b), e(b))$

$$c = (m^{e(b)} \bmod n(b))$$



Bob

$$(c^{h(b)} \bmod n(b)) = m$$

UTILISATIONS DE RSA



bonjour bob

Alice

1124231924302736112411

(1124231924302736112411 ^

15065090500755340874818208281598492935963226985268158580950470973973848523110

42480456938047100981883026555380108188664760543107881755421364073741062056055

23687223946800025812242019 mod

35300773618824481427290087643026576330908077566841536554471443803162568247004

7832524099704392825688399971668487048756462309933303946161191785789310814727

02153607465462868484508727) =

87304996478027264907042836389229549516957080381965287808822

55996682353183622549387201629036734530192117735532736839848

78137203624150249408750079286817109383488270357845218125656

93

UTILISATIONS DE RSA



Bob

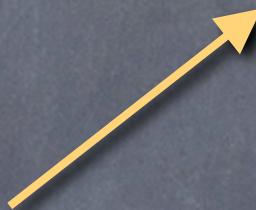
8730499647802726490704283638922954951695708038196528780
8822559966823531836225493872016290367345301921177355327
3683984878137203624150249408750079286817109383488270357
84521812565693 ^
2729084375762693487822921780112081021016746454325189395369485541266793
90501464985171592216103279809889468376074989563842009269643849277216903
63851123702958382331369780470855228779 mod
3530077361882448142729008764302657633090807756684153655447144380316256824700
4783252409970439282568839997166848704875646230993333039461611917857893108147
2702153607465462868484508727 =
1124231924302736112411

bonjour bob



Alice

$$(c^{h(a)} \bmod n(a)) = m$$



$$c = (m^{e(a)} \bmod n(a))$$



Bob

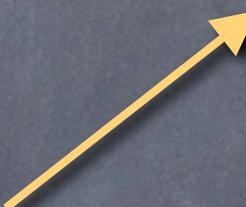


$$(n(a), e(a))$$



Alice

$$(c^{h(a)} \bmod n(a)) = m$$



$$c = (m^{e(a)} \bmod n(a))$$



NATASHA



$$(n(a), e(a))$$

MESSAGE AVEC SIGNATURE

SIGNATURE

$$p := (m^{h(b)} \bmod n(b))$$

$$c := (p^{e(a)} \bmod n(a))$$

$$d := (c^{h(a)} \bmod n(a))$$

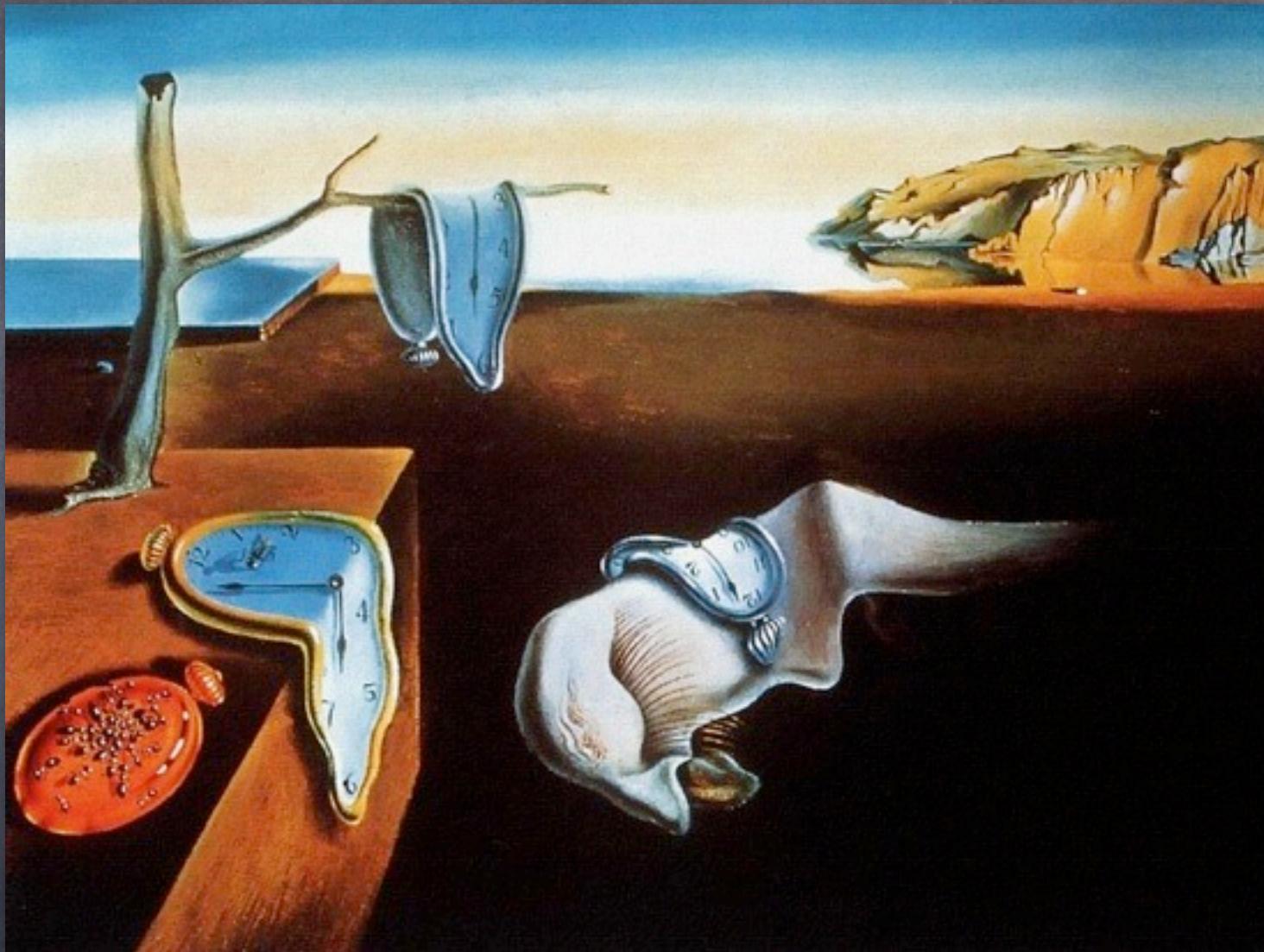
$$m := (d^{e(b)} \bmod n(b))$$

$h(b)$ Exposant secret de Bob
ensuite

$e(a)$ Exposant public d'Alice

Si le message a un sens,
seul Bob peut l'avoir envoyé
et Alice est la seule à
pouvoir le décoder.

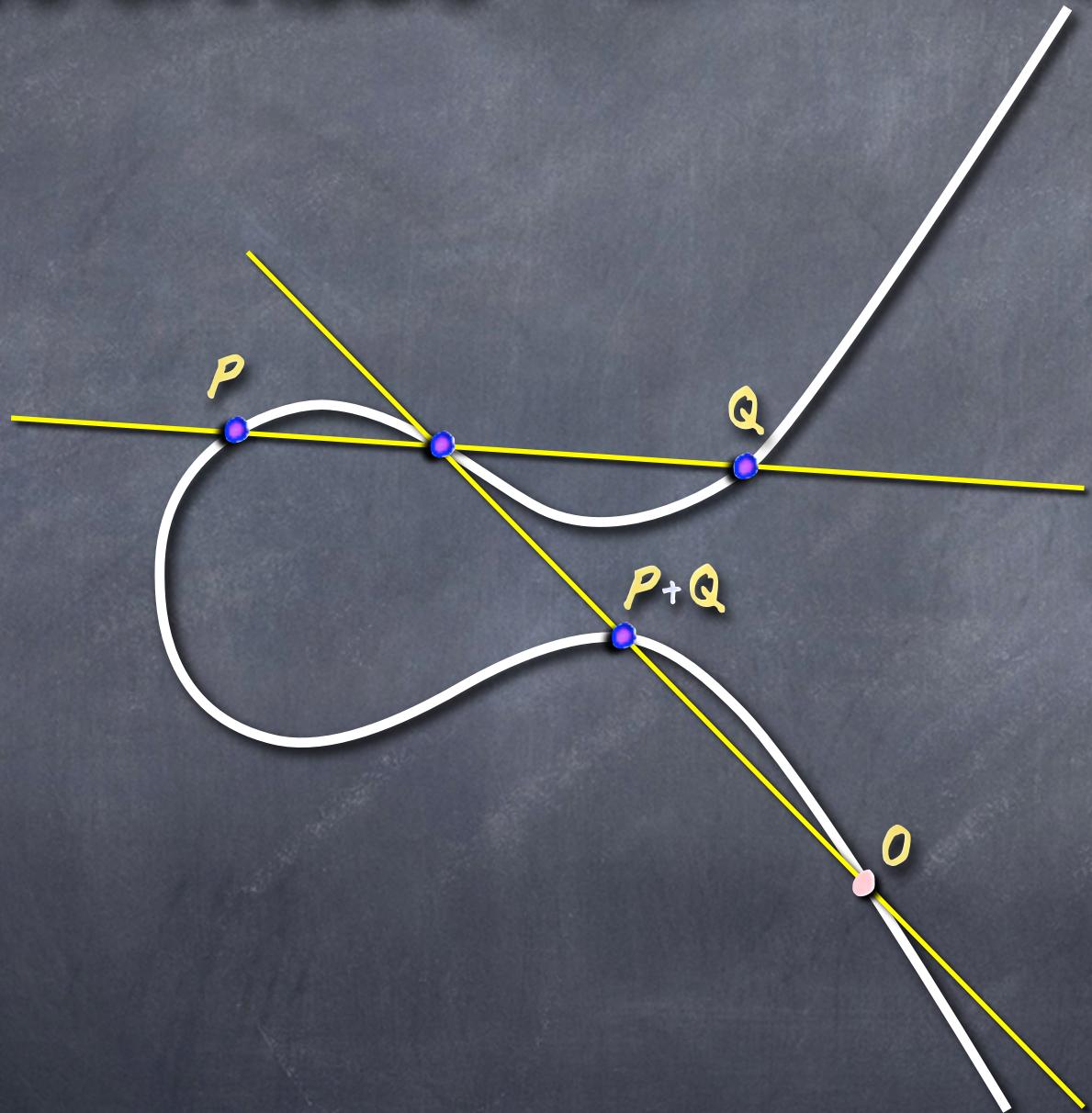
Cryptographie Postmoderne



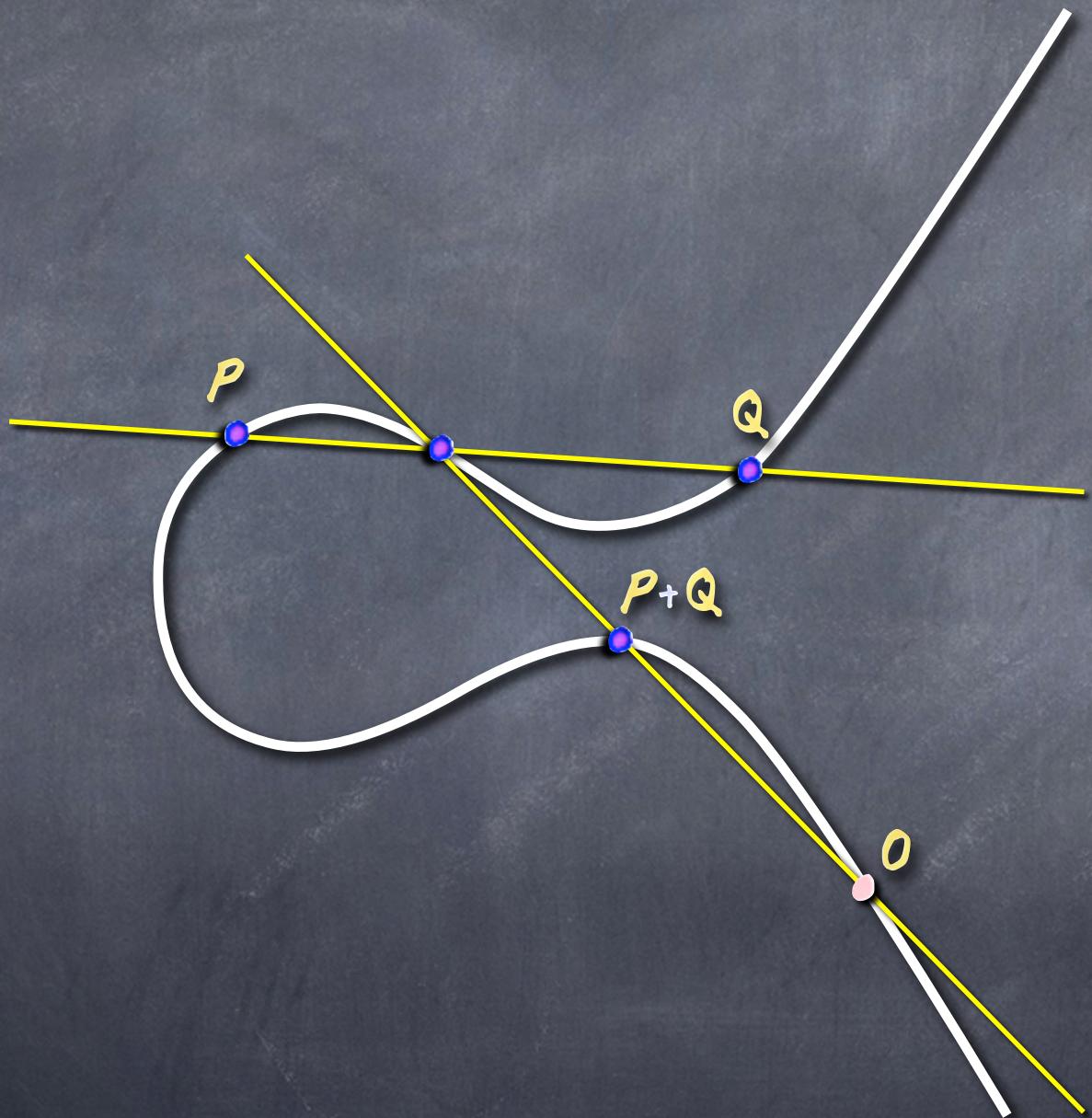
François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

COURBES ELLIPTIQUES



COURBES ELLIPTIQUES



"PROUVER" QUE LE
SYSTÈME EST "INFAILLIBLE".

ALGÈBRE ABSTRAITE
THÉORIE DES GROUPES
CRYPTOGRAPHIE QUANTIQUE

François BERGERON, DEPT. MATH, UQAM

Tuesday, December 3, 13

Fin