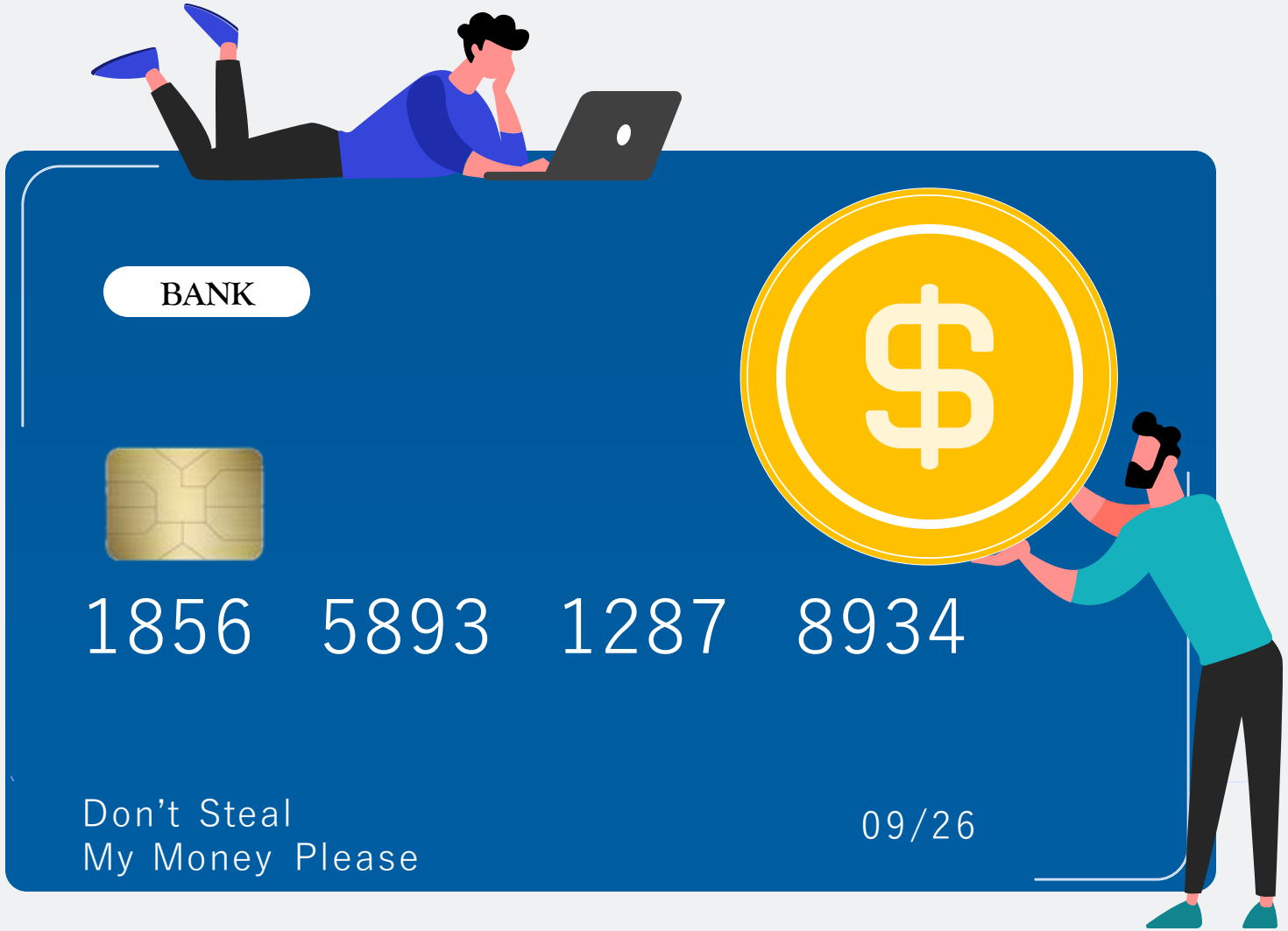
HEH be
Sciences
et technologies

CRYPTOGRAPHIE

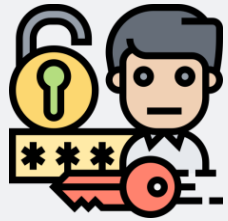
IoE 2023-2024

Tom Deneyer



PROTÉGER L'INFORMATION

Sécurisation et chiffrement des données



Sténographie

Dissimuler dans le visible

Cryptographie

Chiffrer le visible

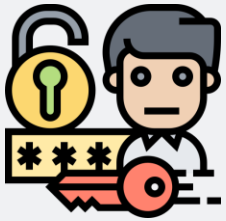
Sténographie

Avec
L'aide
Evidente
D'Eric

Sténographie

Avec
L'aide
Evidente
D'Eric

Cryptographie



Substitution

1. Mot A = Mot B

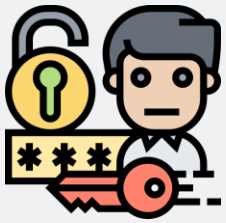
2. Lettre x = Lettre y

   Via deux alphabets

Transport

1. A + 2 = C
   B + 2 = D

   Clef = 2

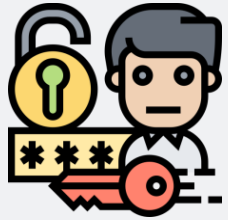


Cryptographie

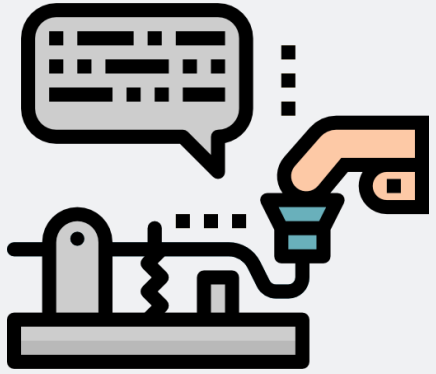
Crypt = caché

Graphy = écriture

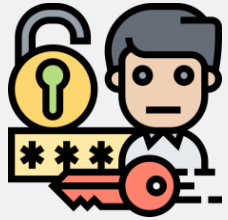
Cryptographie



Manuelle

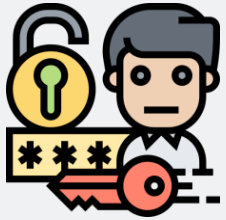


Cryptographie

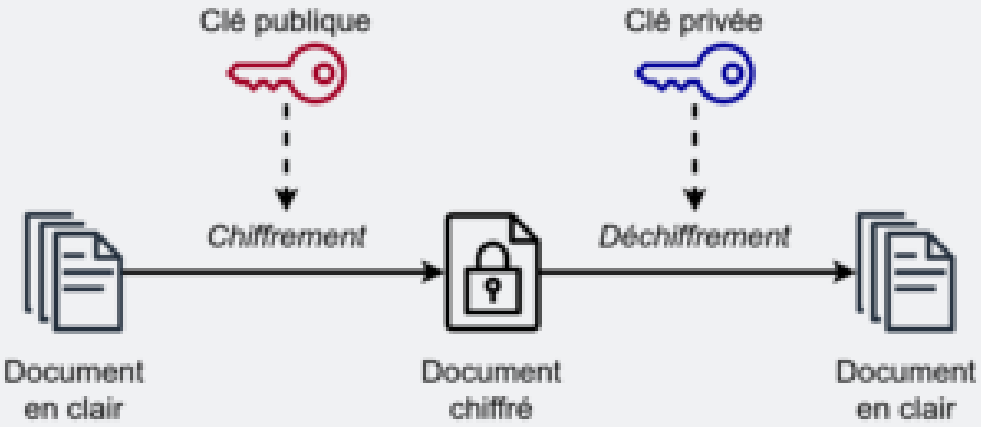


Mécanique

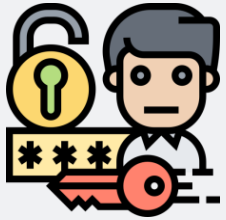
Cryptographie

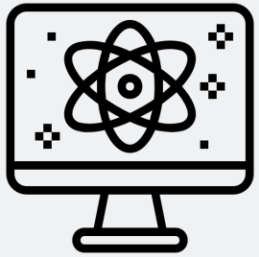


Numérique (asymétrique, rsa)

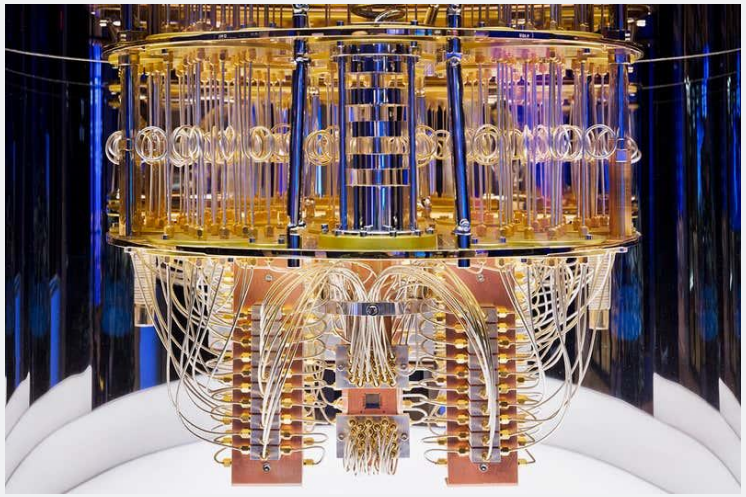


Cryptographie

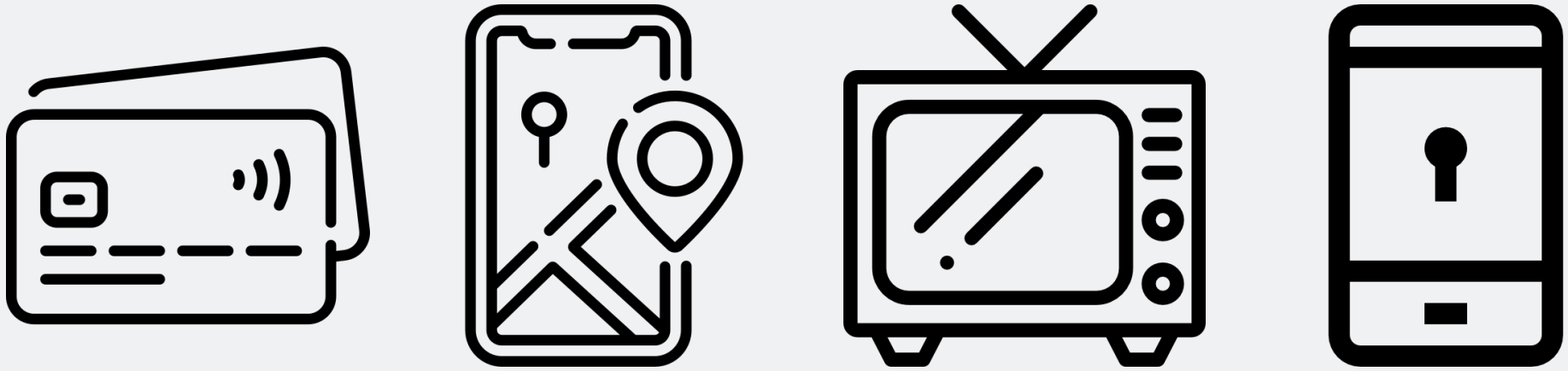




Quantique



APPLICATIONS



Au quotidien quel est l'utilité?

SYSTÈME RSA

$$N=3x7=21$$

$$\Phi 21=(3-1)x(7-1) =12$$

$$e=7$$

$$d=7$$

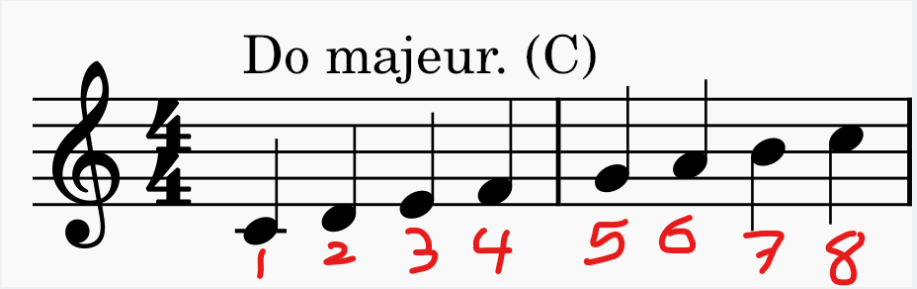
Clef publique: (21,7) Clef privée: (3,7,7)

1. Choisir p et q, deux nombres premiers distincts ;
2. calculer leur produit $n = pq$, appelé *module de chiffrement* ;
3. calculer $\varphi(n) = (p - 1)(q - 1)$ (c'est la valeur de l'indicatrice d'Euler en n) ;
4. choisir un entier naturel e premier avec $\varphi(n)$ et strictement inférieur à $\varphi(n)$, appelé *exposant de chiffrement* ;
5. calculer l'entier naturel d, inverse modulaire de e pour la multiplication modulo $\varphi(n)$ et strictement inférieur à $\varphi(n)$, appelé *exposant de déchiffrement* ; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

Le couple (n, e) — ou (e, n)[3] — est la *clé publique* du chiffrement, alors que sa *clé privée* est[4] le nombre d, sachant que l'opération de déchiffrement ne demande que la clef privée d et l'entier n, connu par la clé publique (la clé privée est parfois aussi définie comme le couple (d, n)[3] ou le triplet (p, q, d)[5]).

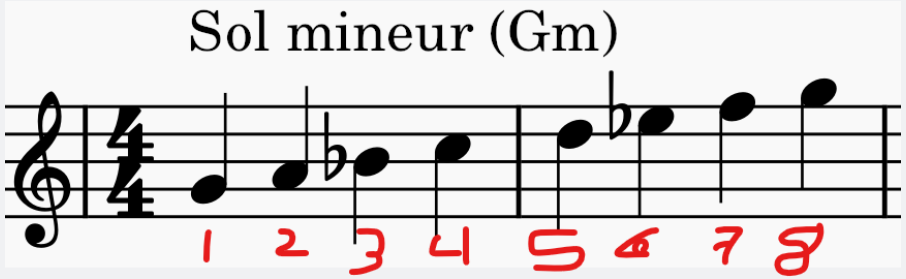
$$3\ 574\ 406\ 403\ 731 = 1\ 299\ 709 \times 2\ 750\ 159$$

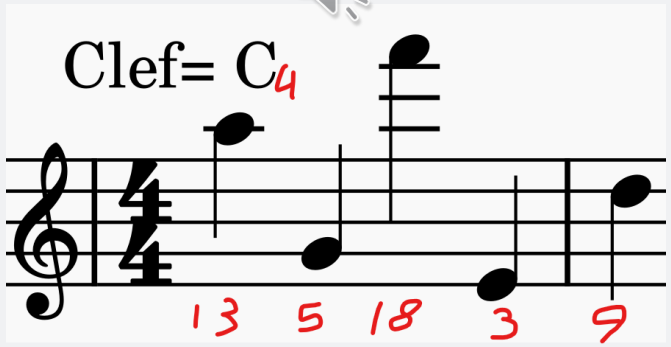
SYSTÈME MUSICAL?



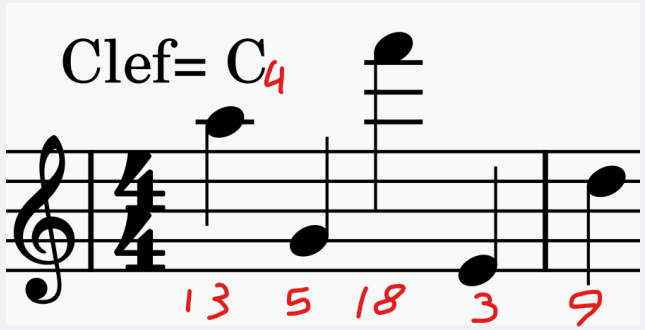
M E R C I

13 5 18 3 9





A G F E D



SYSTÈME MUSICAL?

M E R C I
A5 G4 F6 E4 D5

Valeur de la fréquence des notes (en hertz)

Do	Ré	Mi	Fa#	Sol#	La#
16.351	18.354	20.601	23.124	25.956	29.135
32.703	36.708	41.203	46.249	51.913	58.270
65.406	73.416	82.406	92.498	103.826	116.540
130.812	146.832	164.813	184.997	207.652	233.081
261.625	293.664	329.627	369.994	415.304	466.163
523.251	587.329	659.255	739.988	830.609	932.327
1046.502	1174.059	1318.510	1479.976	1661.218	1864.654
2093.004	2344.318	2637.020	2959.952	3322.436	3729.308
4186.008	4698.636	5274.040	5919.904	6644.872	7458.616
8372.016	9397.272	10548.080	11839.808	13289.744	14917.232
16744.032	18794.544	21096.160	23679.616	26579.488	29834.464

Do#	ré#	Fa	Sol	La	Si
17.323	19.445	21.826	24.499	27.500	30.867
34.647	38.890	43.653	48.999	55.000	61.735
69.295	77.781	87.307	97.998	110.000	123.470
138.591	155.563	174.614	195.997	220.000	246.941
277.182	311.126	349.228	391.995	440.000	493.883
554.365	622.253	698.456	783.991	880.000	987.766
1108.730	1244.507	1396.912	1567.982	1760.000	1975.532
2217.460	2489.014	2793.824	3135.964	3520.000	3951.064
4434.920	4978.028	5587.648	6270.928	7040.000	7902.128
8869.840	9956.056	11175.296	12541.856	14080.000	15804.256
17739.680	19912.112	22350.592	25083.712	28160.000	31608.512

880
391
1396
329
587

Merci = 880 391 1396 329 587

Clef = C4

Nomenclature des clefs:
Note/hauteur/détail

Ex: A2, B5m, D#3m