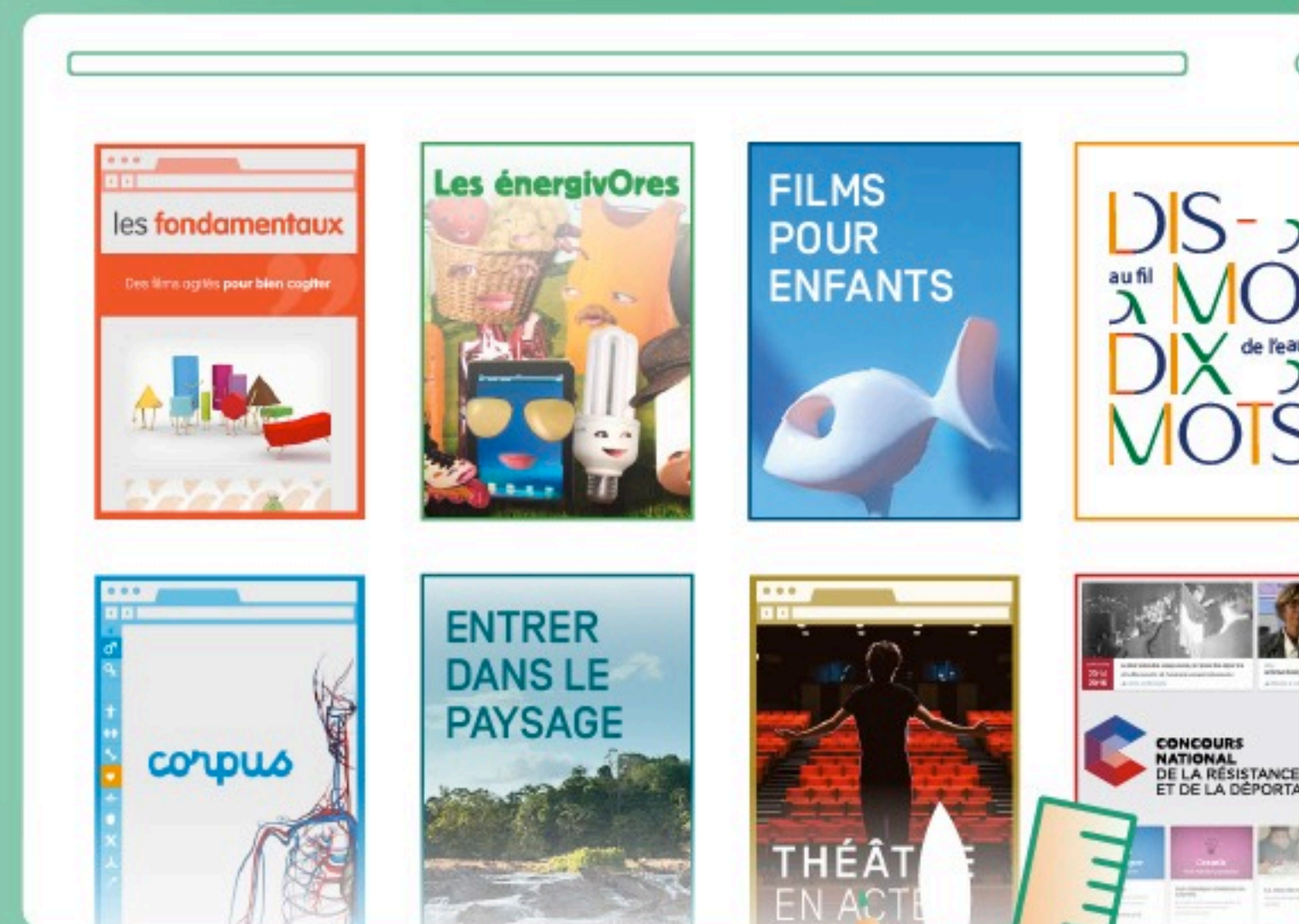


S E F O R M E R



CS Unplugged 5



Bonjour et bienvenue dans cet atelier en direct !

Pendant les activités de démonstration :

- nous vous invitons à couper caméra et micro
- vous pouvez écrire vos questions et réponses dans « conversation »

Afficher la conversation



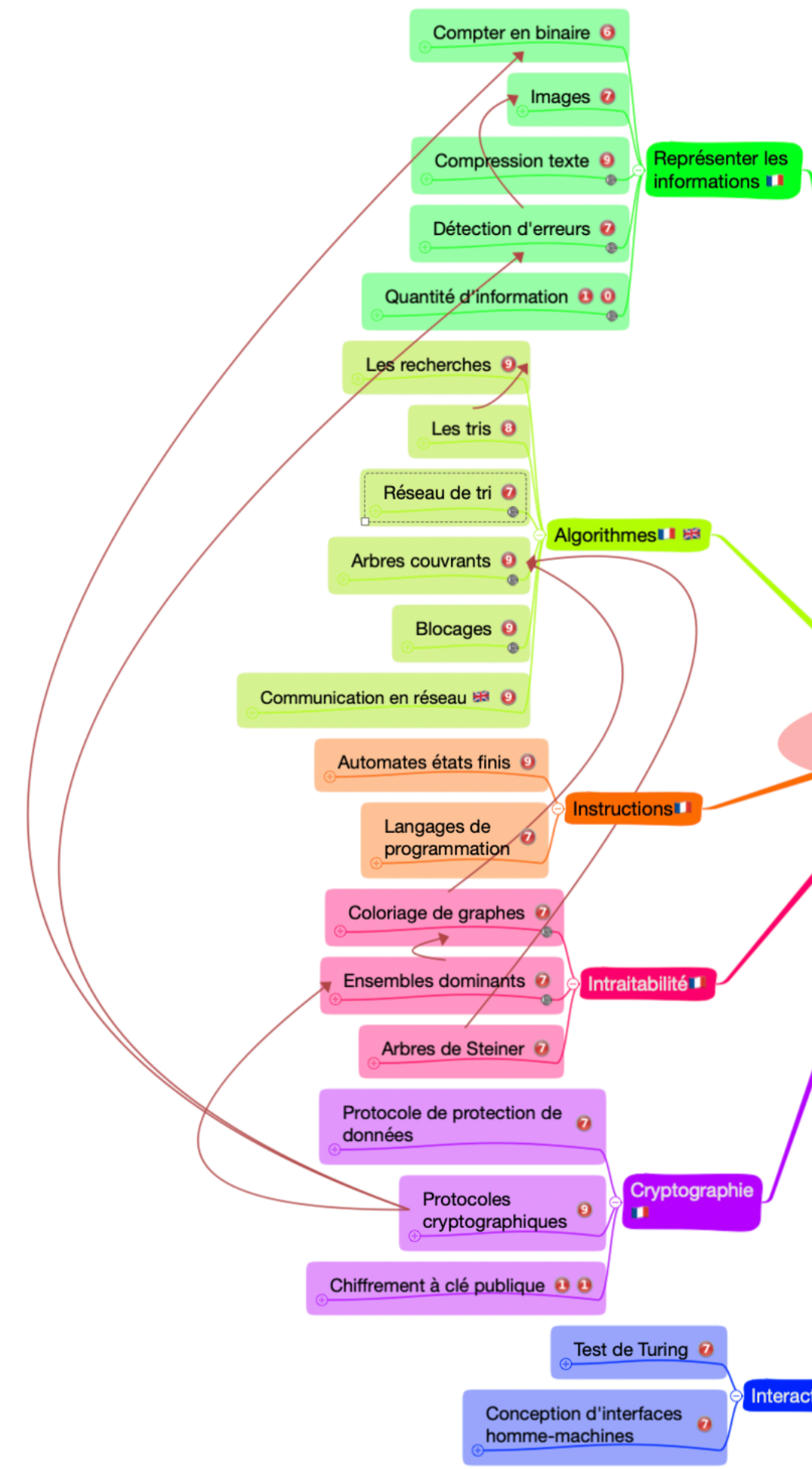
Pendant les temps d'échange :

- nous répondrons aux questions posées dans la conversation
- vous pourrez prendre la parole directement en activant votre micro

Les formateurs :

- Samuel Chalifour, médiateur Atelier Canopé 88
- Sophie Thiébaut, médiatrice Atelier Canopé 88

CANOPÉ



Indication de l'âge minimum

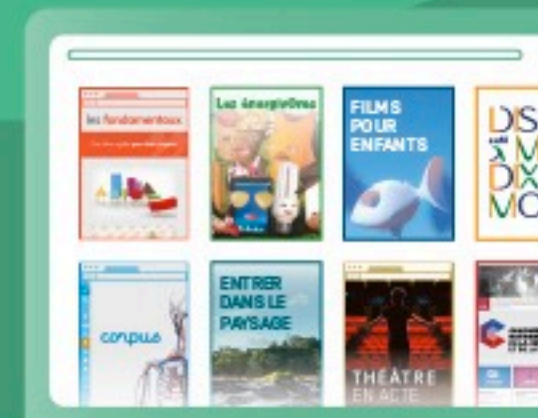
Disponible en français

Disponible en anglais uniquement ou en français sur les versions Apple

CC-BY-SA
Samuel Chalifour

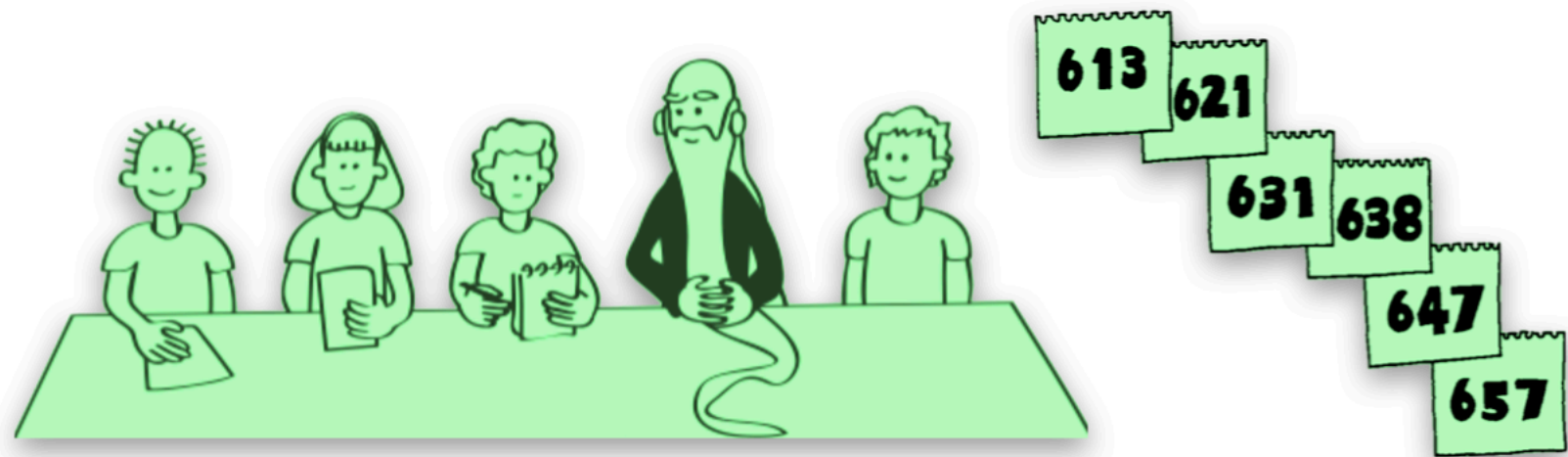
Bibliographie Sitographie

- 1987 : Informatique sans ordinateur
Guy Crozet, Roland Grosperin
Wanted
QR code
- UNPLUGGED
1999-2021 : Livre puis Site officiel
Tim Bell, Ian H. Witten, Mike Fellows
interstices
Interstices INRIA
QR code
- Version interactive (compatible Apple uniquement)
QR code
- IREM
IREM Clermont-Ferrand
QR code
- Scratch
Studio Scratch dédié
QR code
- CANOPROF
10 ateliers avec fiches d'activités pour la classe
YouTube FR
Chaine Youtube 10 Capsules
QR code



Chapitre 5 - Section 1

Partager des secrets



Protocoles de masquage des données

Les techniques cryptographiques permettent de partager des données avec d'autres personnes tout en garantissant un niveau de confidentialité étonnamment élevé. Dans cette activité, nous allons partager des informations sans rien révéler de leur contenu : chaque groupe d'élèves calculera son âge moyen sans qu'aucun des membres ne divulgue son âge.

Liens pédagogiques

- Mathématiques : sommes et moyennes

Compétences

- Calculer une moyenne
- Nombres aléatoires
- Coopération


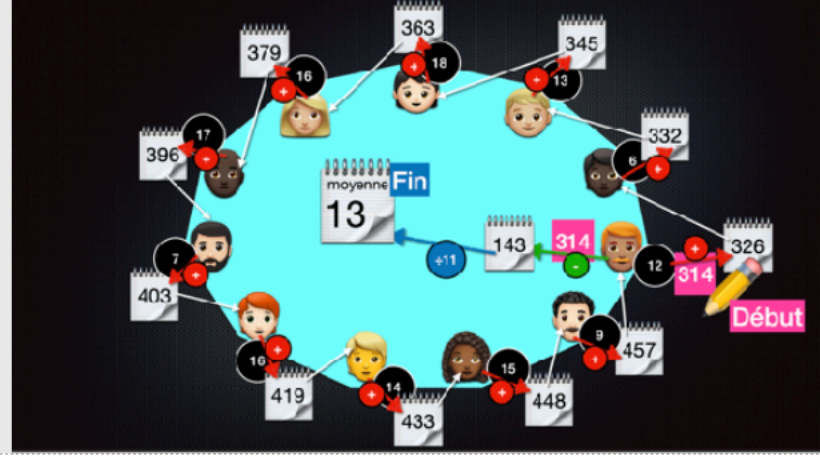
Âge

- 7 ans et plus

Matériel

- Pour chaque élève :
 - Un petit bloc-notes
 - Un stylo

Chapitre 5 - Section 1

Étape	Instruction	Réponse
1	Présentation de l'historique très rapide de la cryptographie.	
2	Présenter la situation : Les participants veulent calculer la moyenne de leurs âges/salaires/notes de leur dernier devoir de mathématiques sans qu'aucun participant ne révèle sa note à aucun autre participant.	Matériel nécessaire ? Explication du protocole
3	Si une méthode complète a été proposée, elle doit être testée (si besoin avec de fausses informations, pour la vérification).	
4	On propose si besoin la méthode du formateur : Constitution de la chaîne de communication	<p>Le premier participant choisit un nombre aléatoire (rose) avec un chiffre de plus que la donnée à « partager ».</p> <p>Il note ce nombre. Dans le chat privé, il envoie la somme de ce nombre et de la donnée à partager à son voisin.</p> <p>Son voisin fait de même.</p> <p>Le dernier participant fait de même vers le premier. Le premier peut alors retrancher le nombre aléatoire noté au début, diviser par le nombre de participant et ainsi obtenir la moyenne.</p> 
5	On teste. Vérification des défauts et avantages de ce protocole.	Le protocole, même s'il est bien exécuté, n'empêche pas les erreurs de calcul ou les « triches ».
6	Rédaction des grands principes mis en œuvre et applications dans la vie réelle.	Stratégie du noyade de poisson et de cohérence des données. Si la protection des données est un sujet central de la vie numérique actuelle, elle a de nombreux impacts sur la vie privée, entre les informations bancaires, médicales, scolaires. Et la balance avec les possibilités légales des états ou d'autres organismes publics ou privés est en constant débat politique, économique voire philosophique.

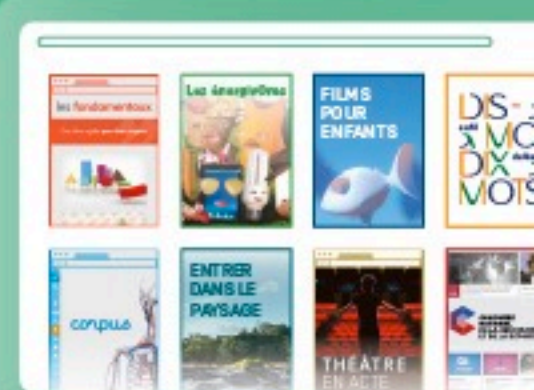




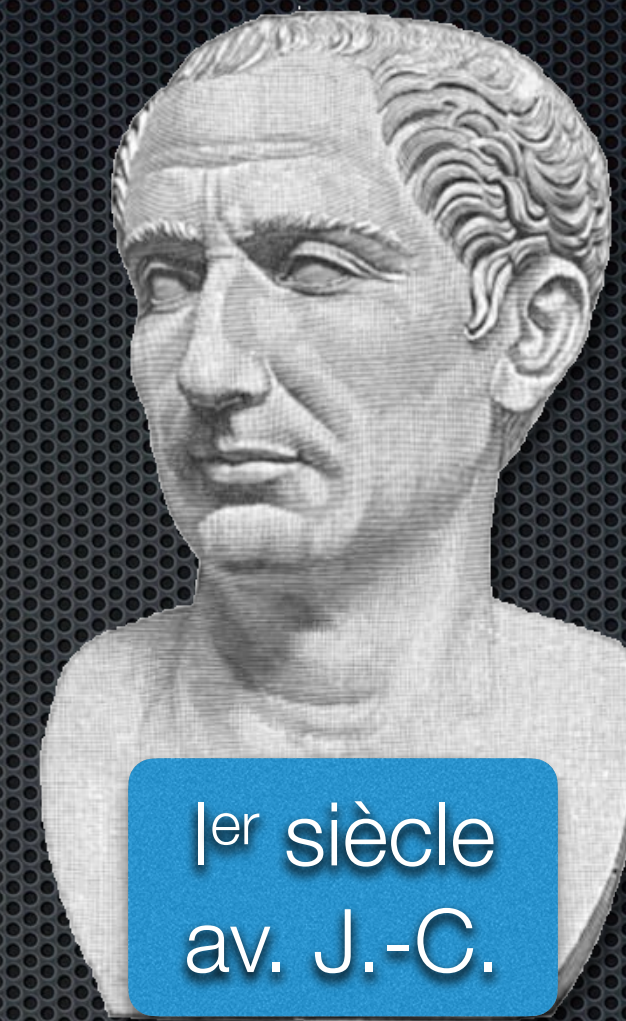
Image par Gerd Altmann de Pixabay

Les protocoles de masquage de données

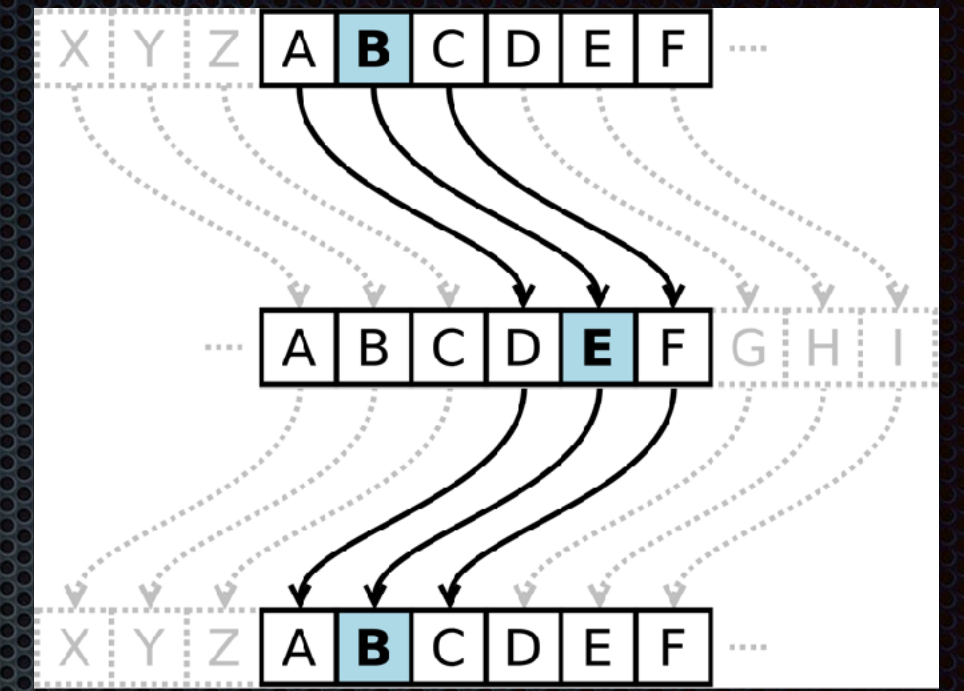
Science informatique débranchée



XVI^e siècle
av. J.-C.



I^{er} siècle
av. J.-C.



1916-2001



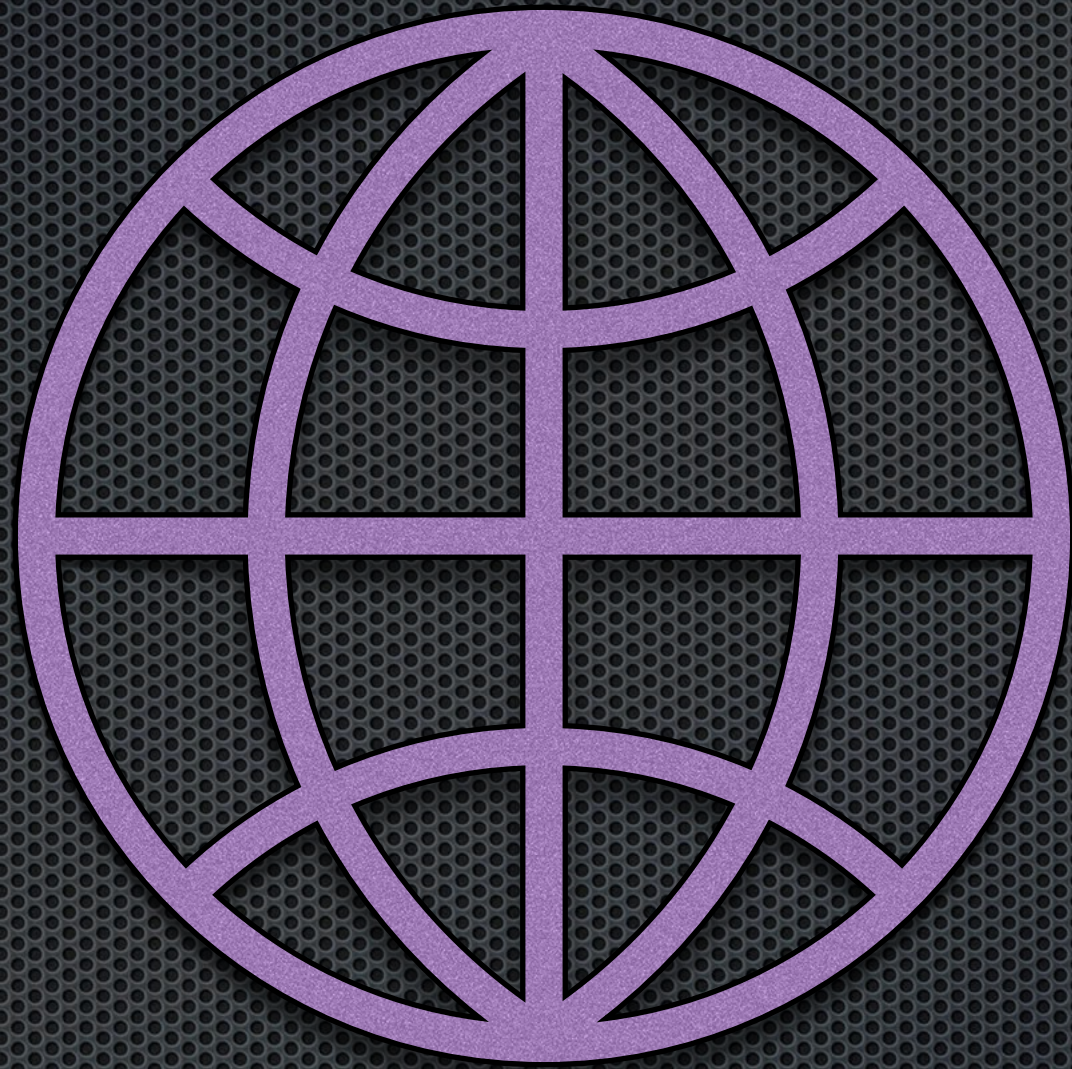
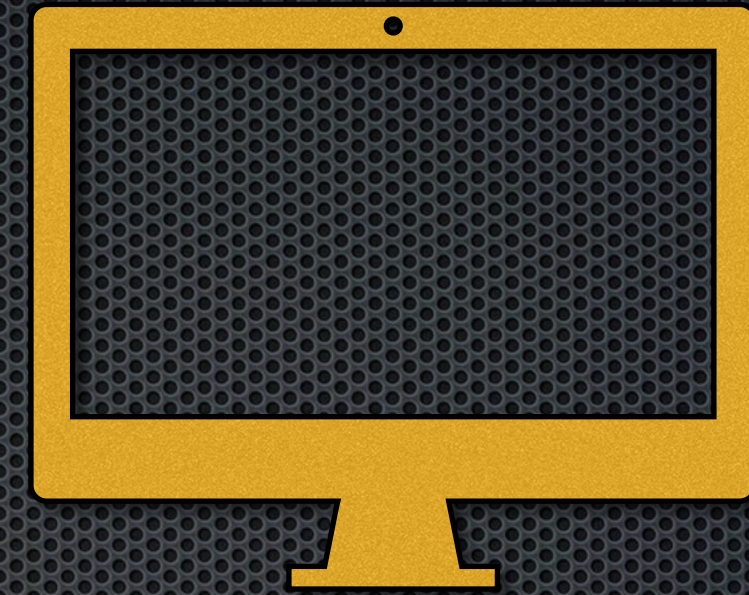
XV^e siècle



1919

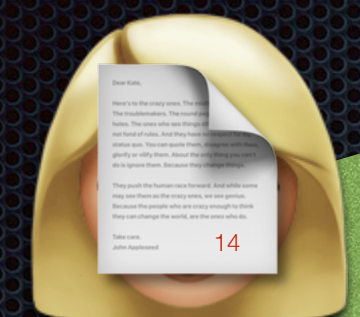
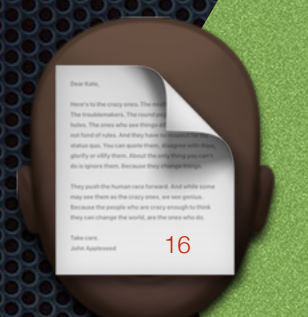
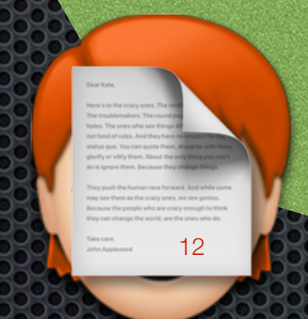
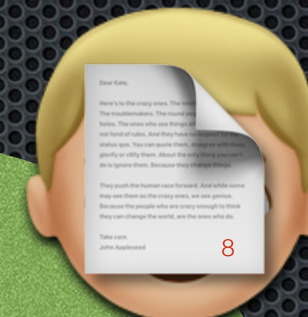
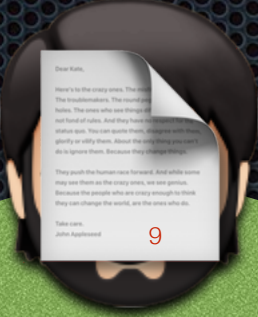


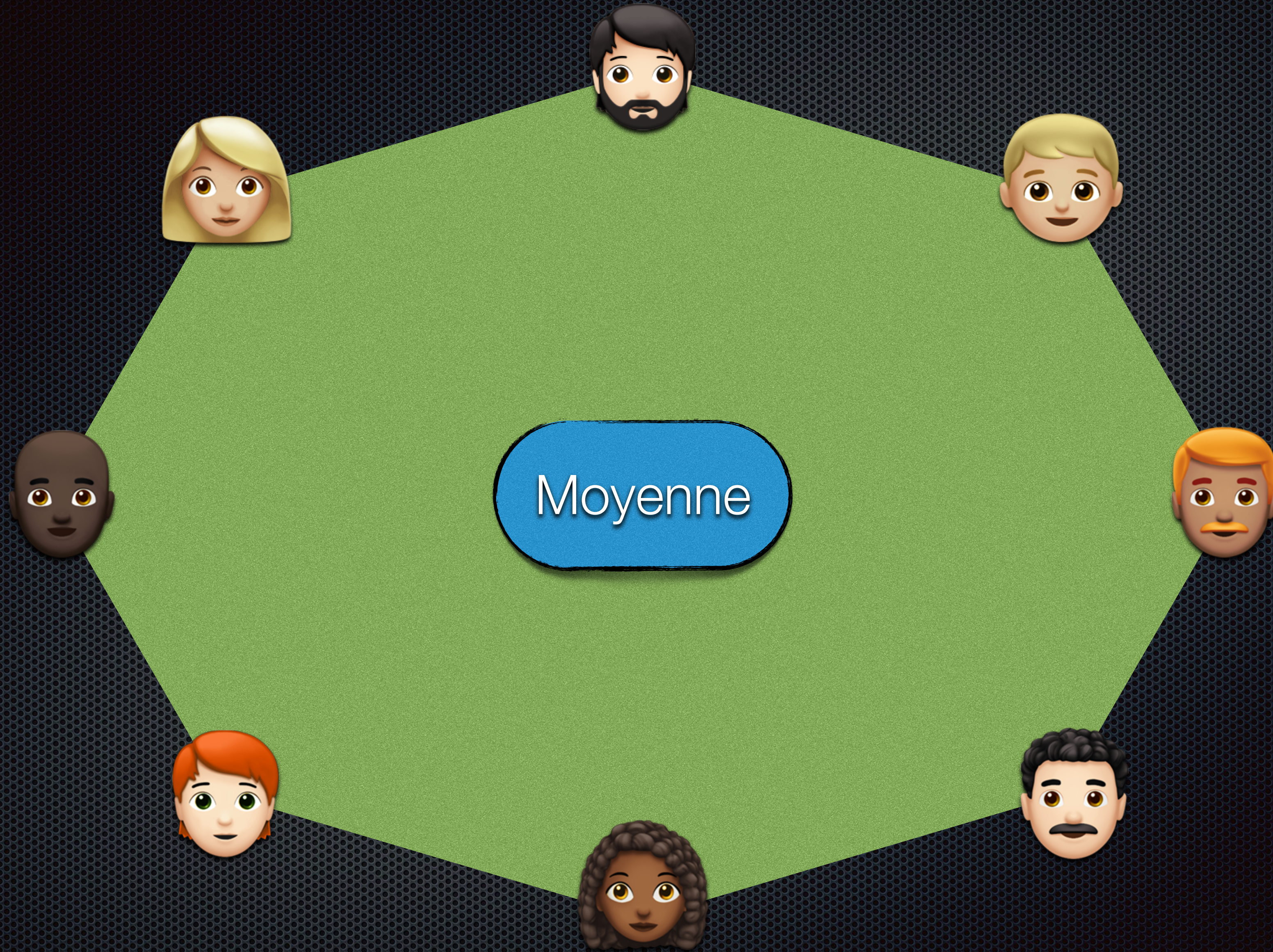
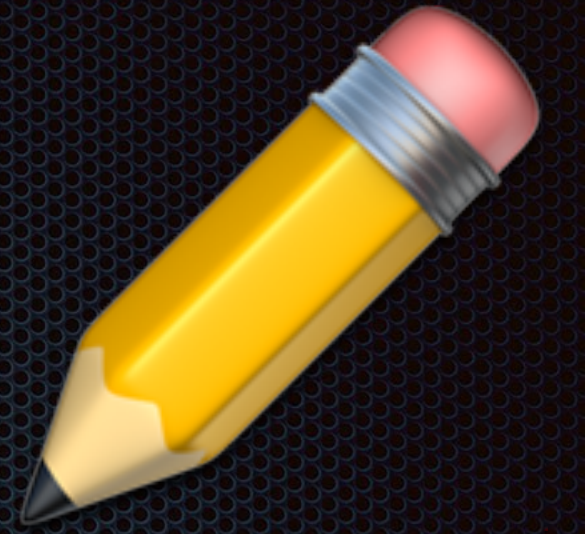
Rama



Moyenne

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$$



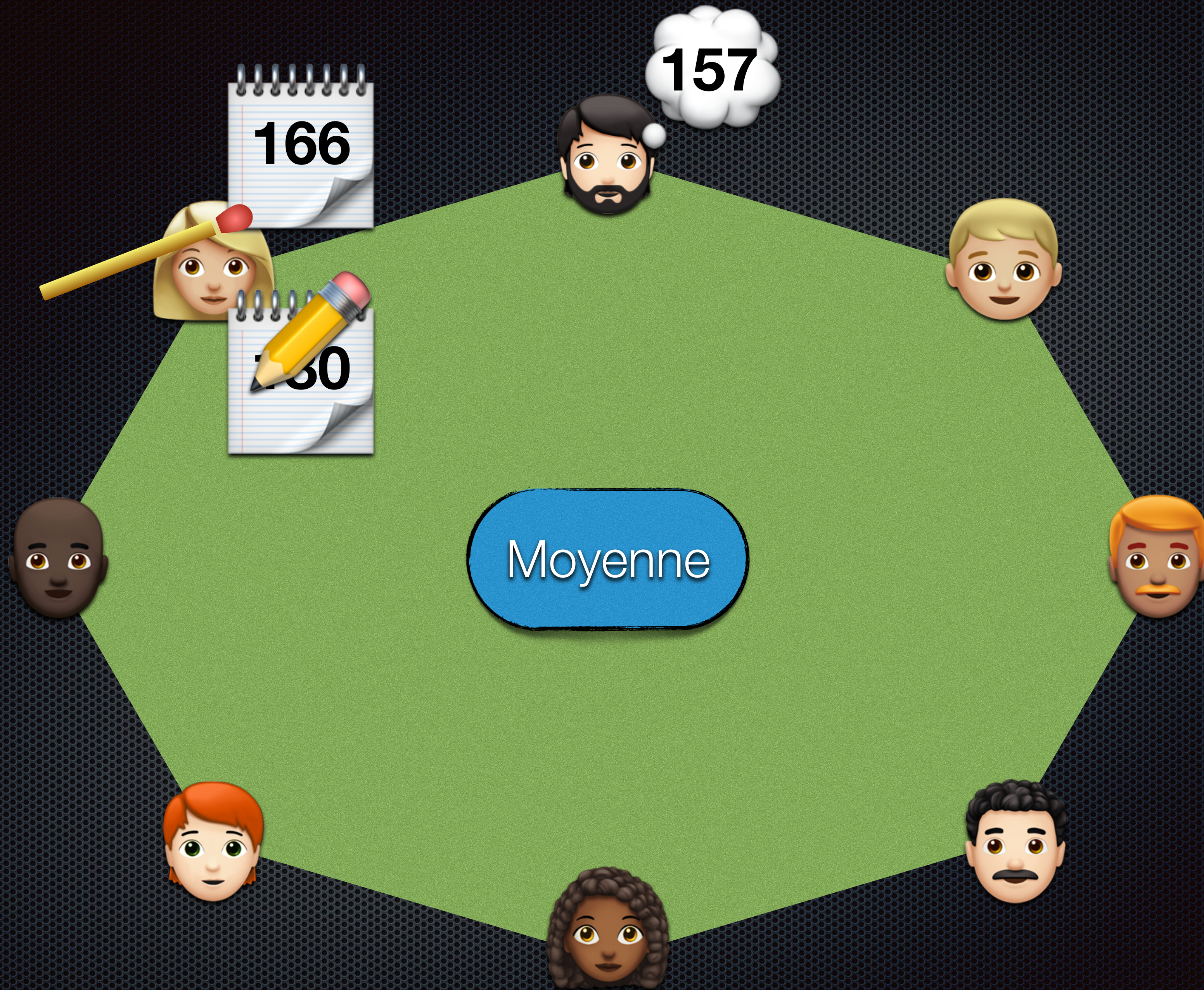


Moyenne

157



Moyenne



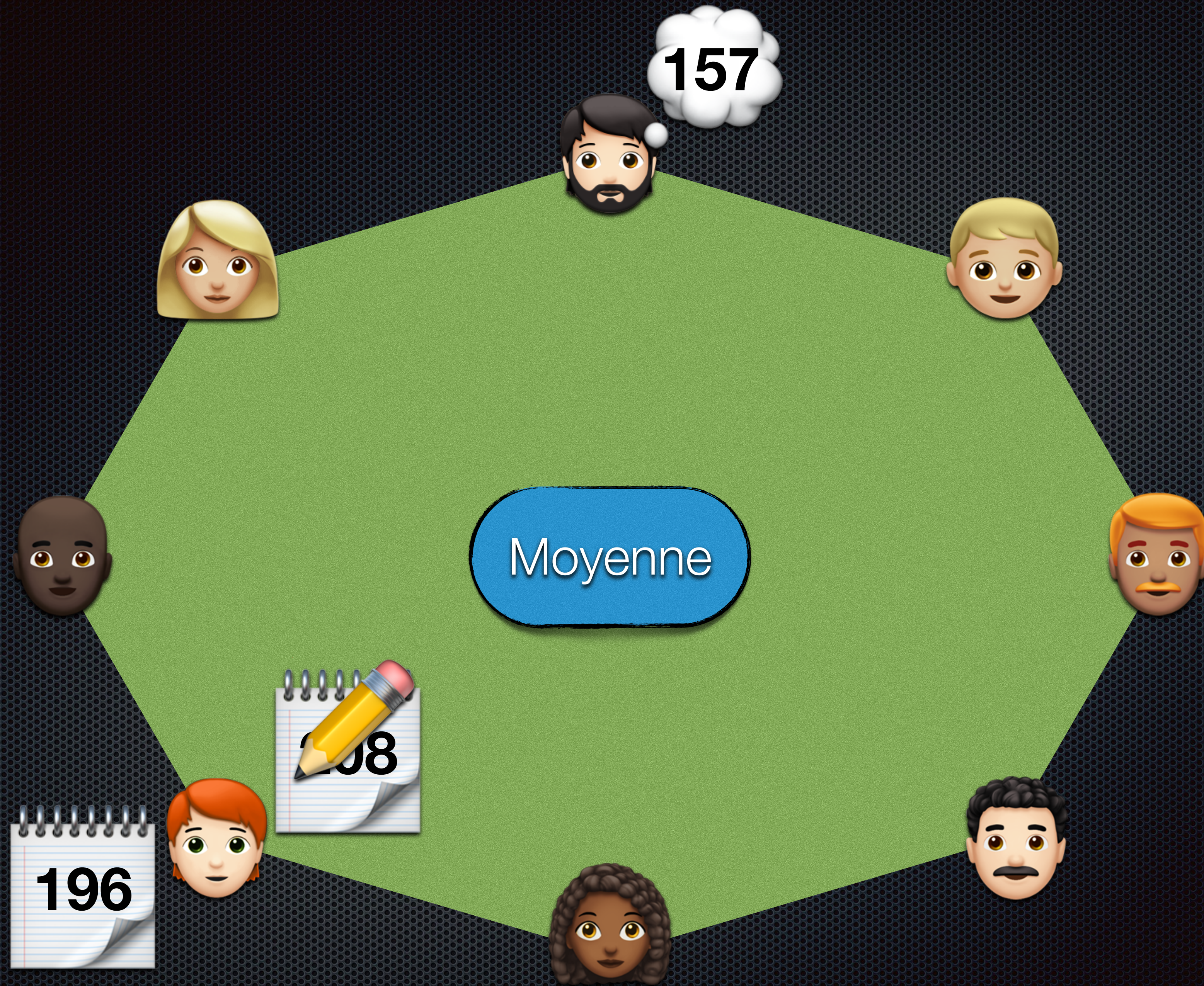
180

196

157

Moyenne





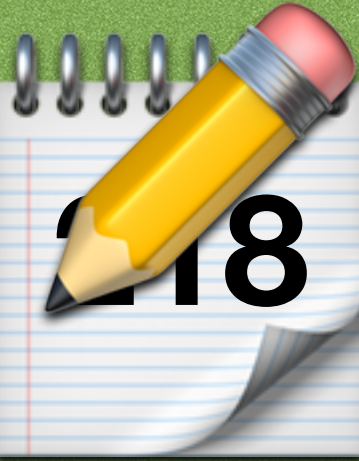
157



Moyenne



218



208



157



Moyenne

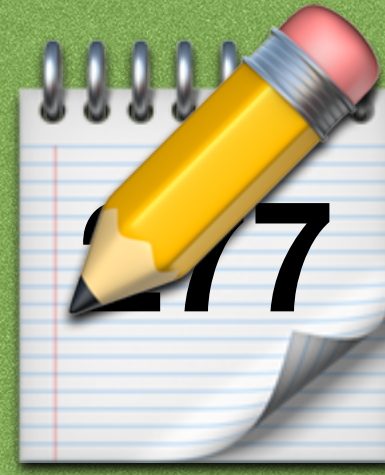


260

218

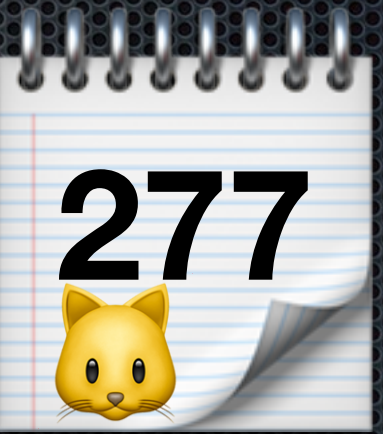
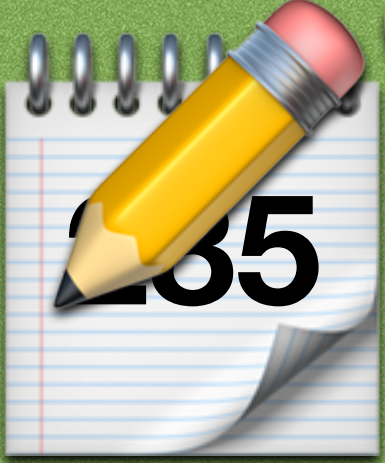


157



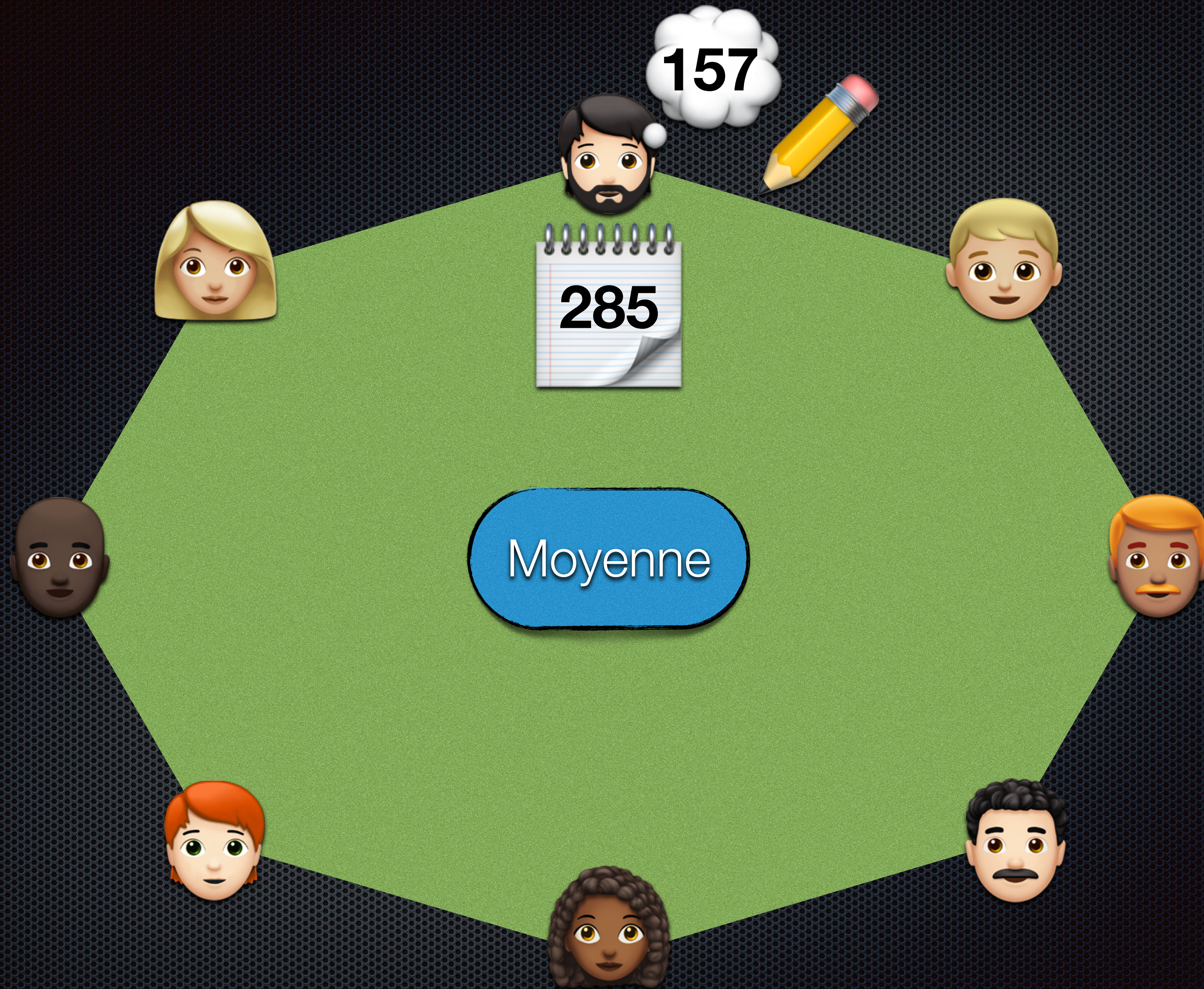
Moyenne

157

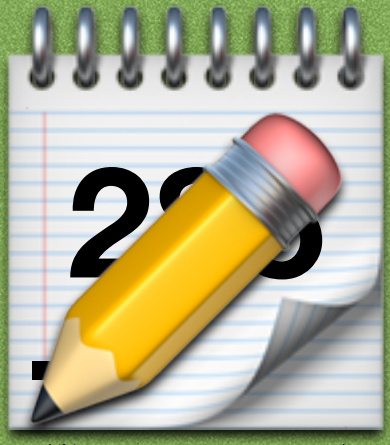


Moyenne





157



$$\begin{array}{r|l} 128 & 8 \\ \hline & 16 \end{array}$$

Moyenne



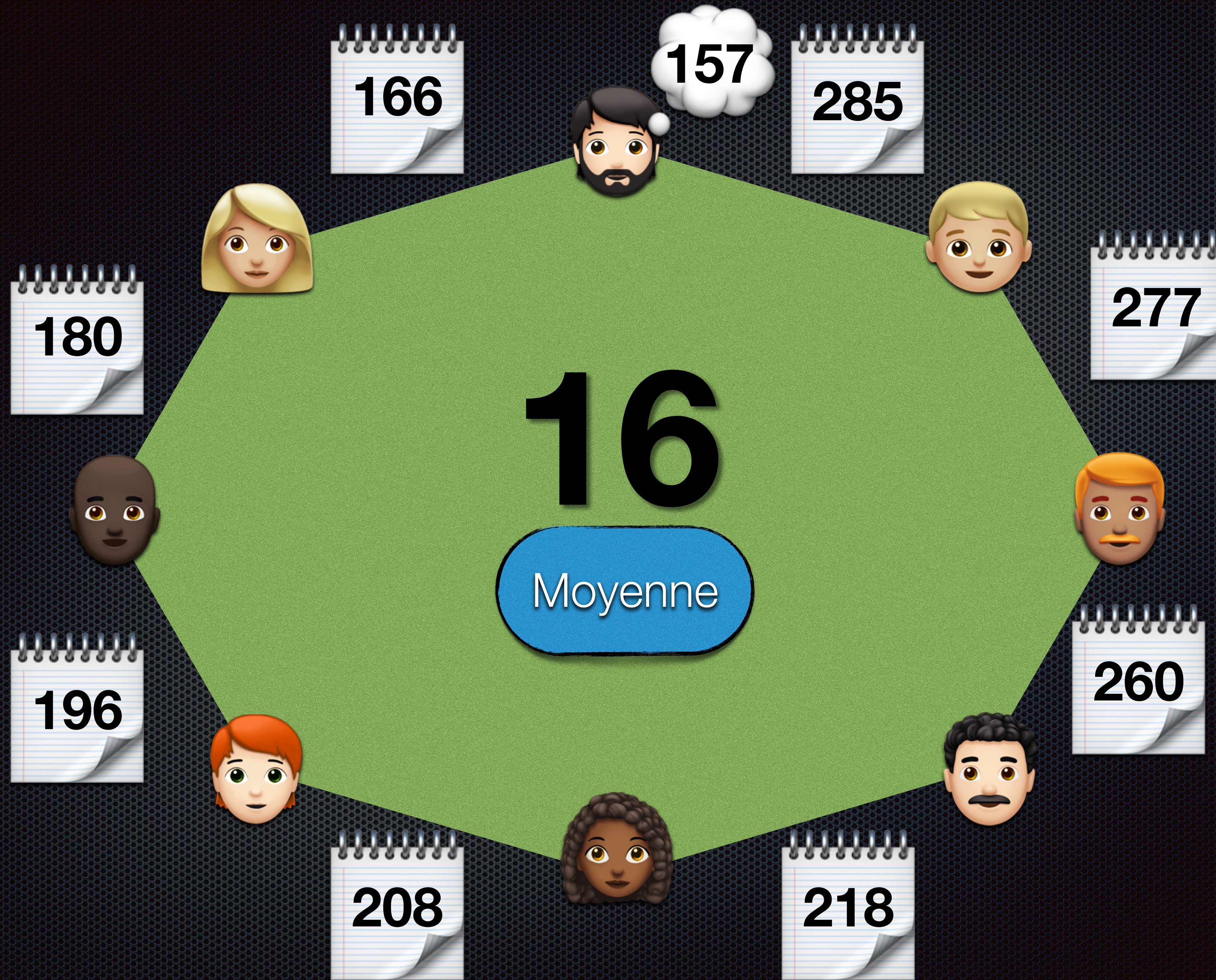
157

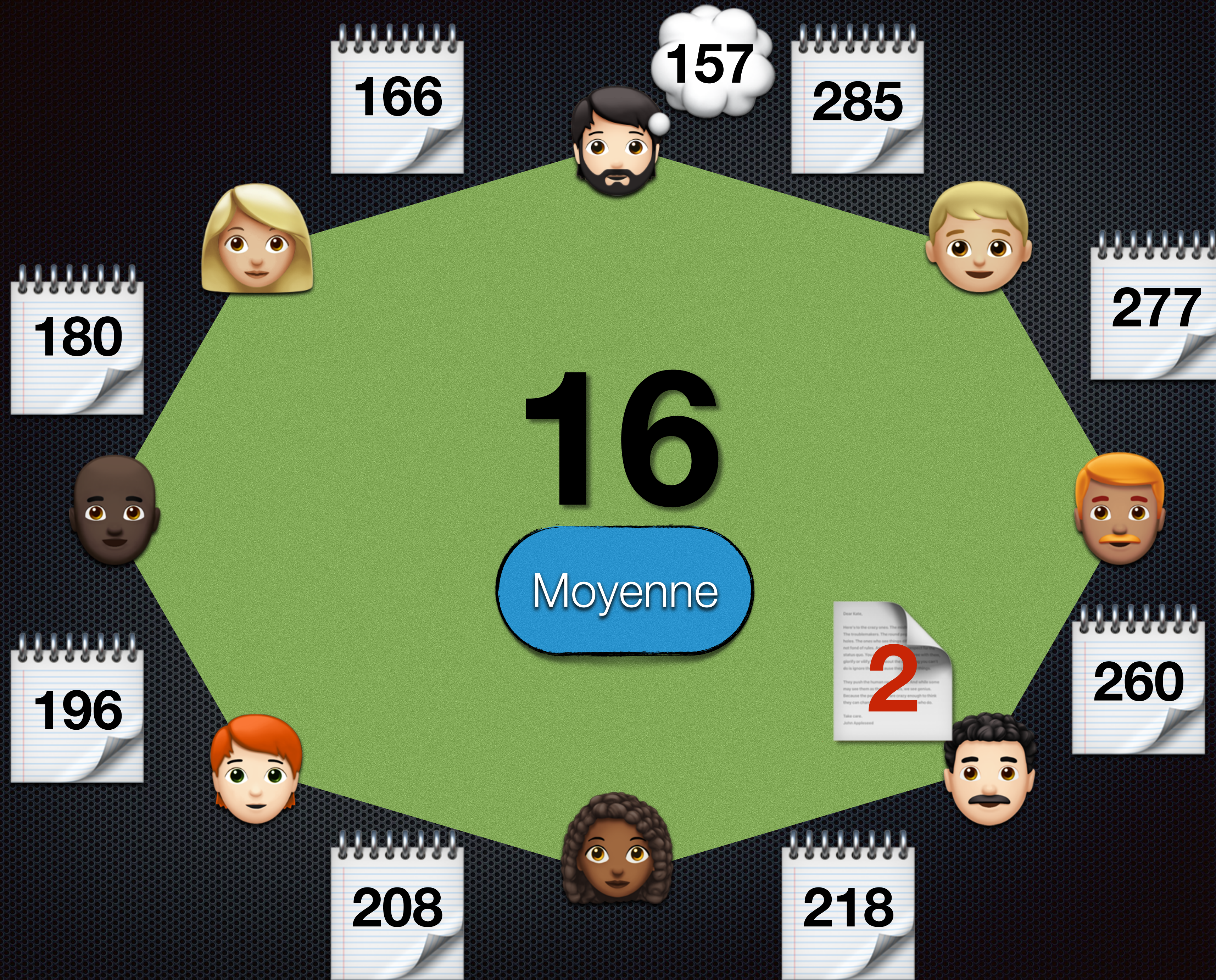


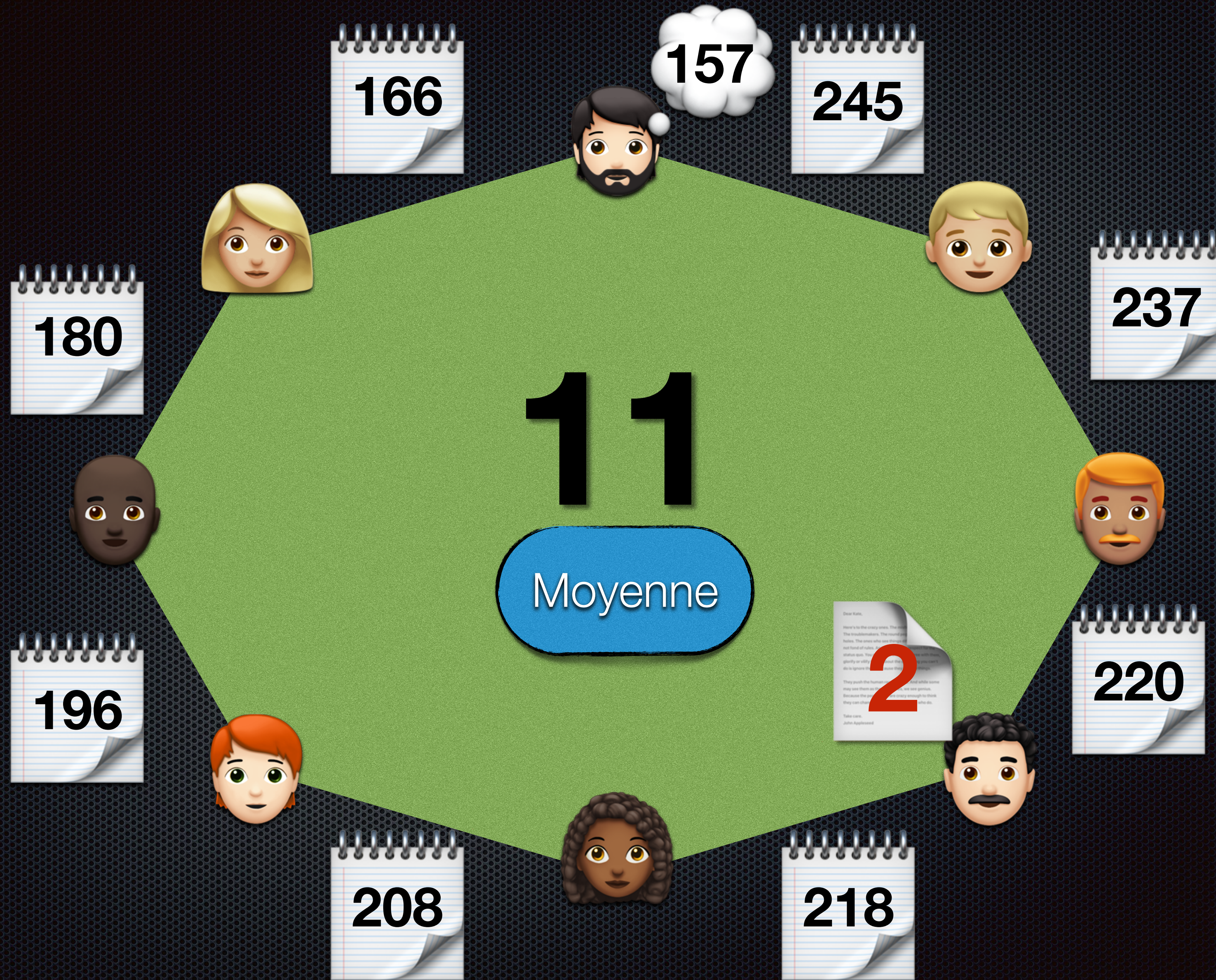
16

Moyenne









CRYPTOLOGIE

Science du secret

CRYPTOGRAPHE

Écriture secrète

Vocabulaire

Analyse et attaque
de la cryptographie

STÉGANOGRAPHIE

Art de la
dissimulation

confidentialité

authenticité

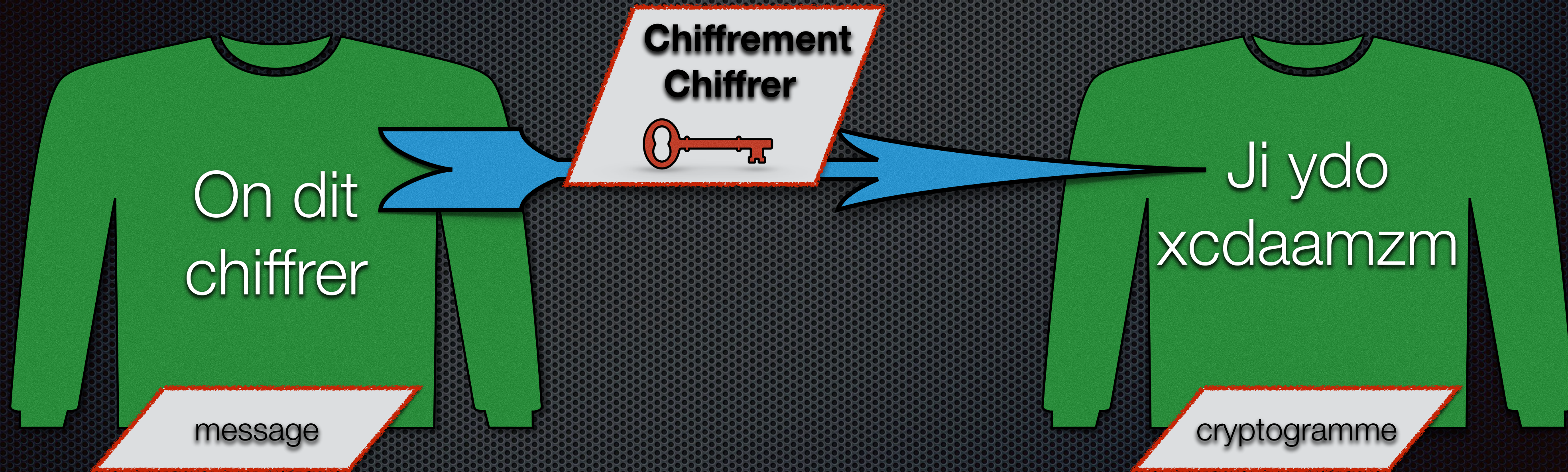
intégrité

CRYPTOGRAPHIE

Écriture secrète

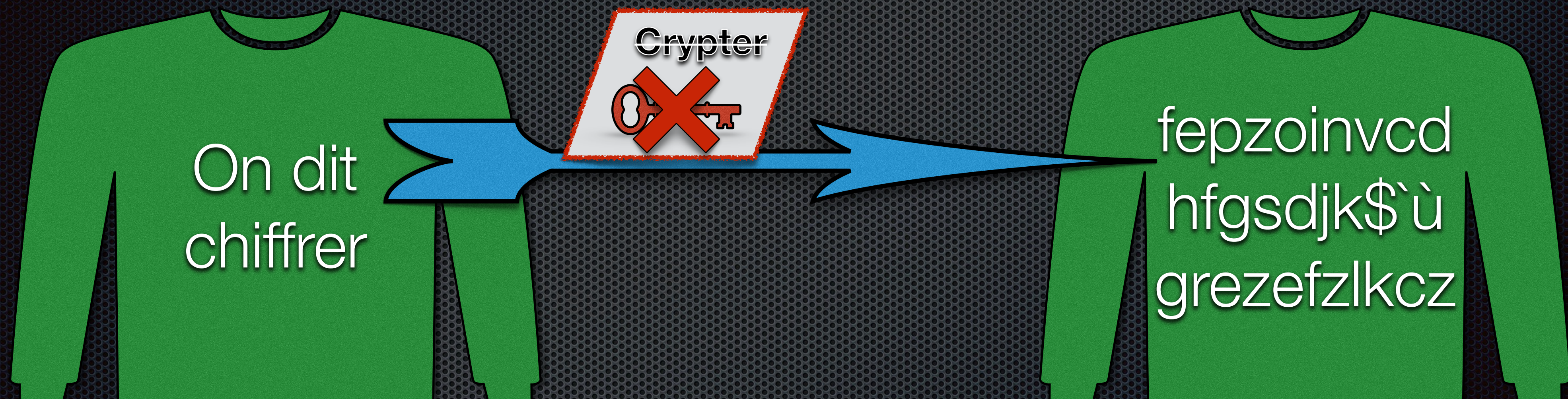


chiffre / cryptosystème



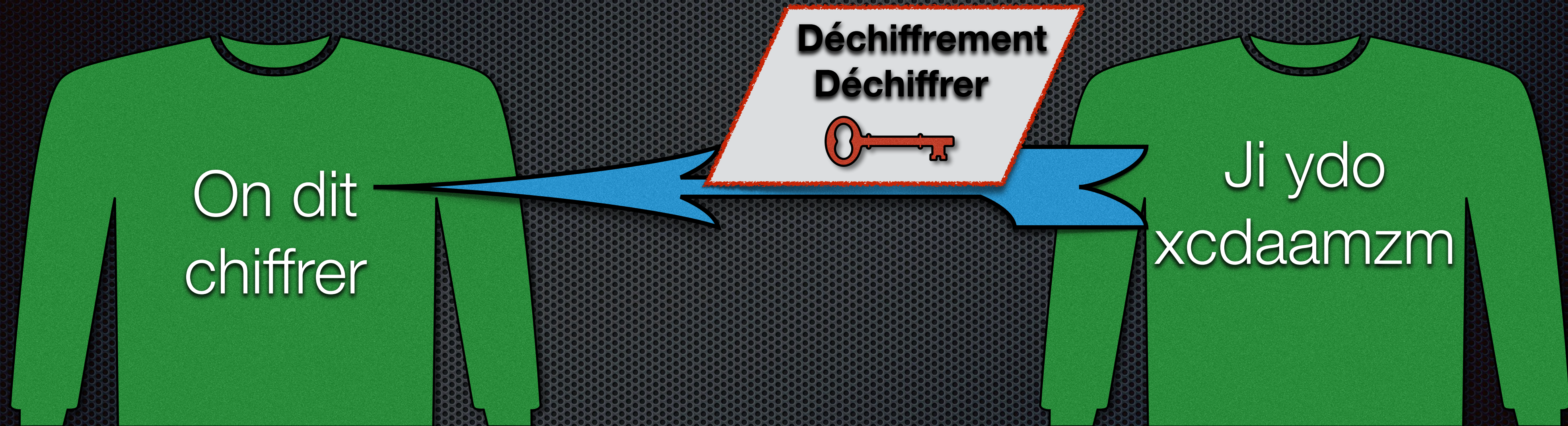
CRYPTOGRAPHIE

Écriture secrète



CRYPTOGRAPHIE

Écriture secrète

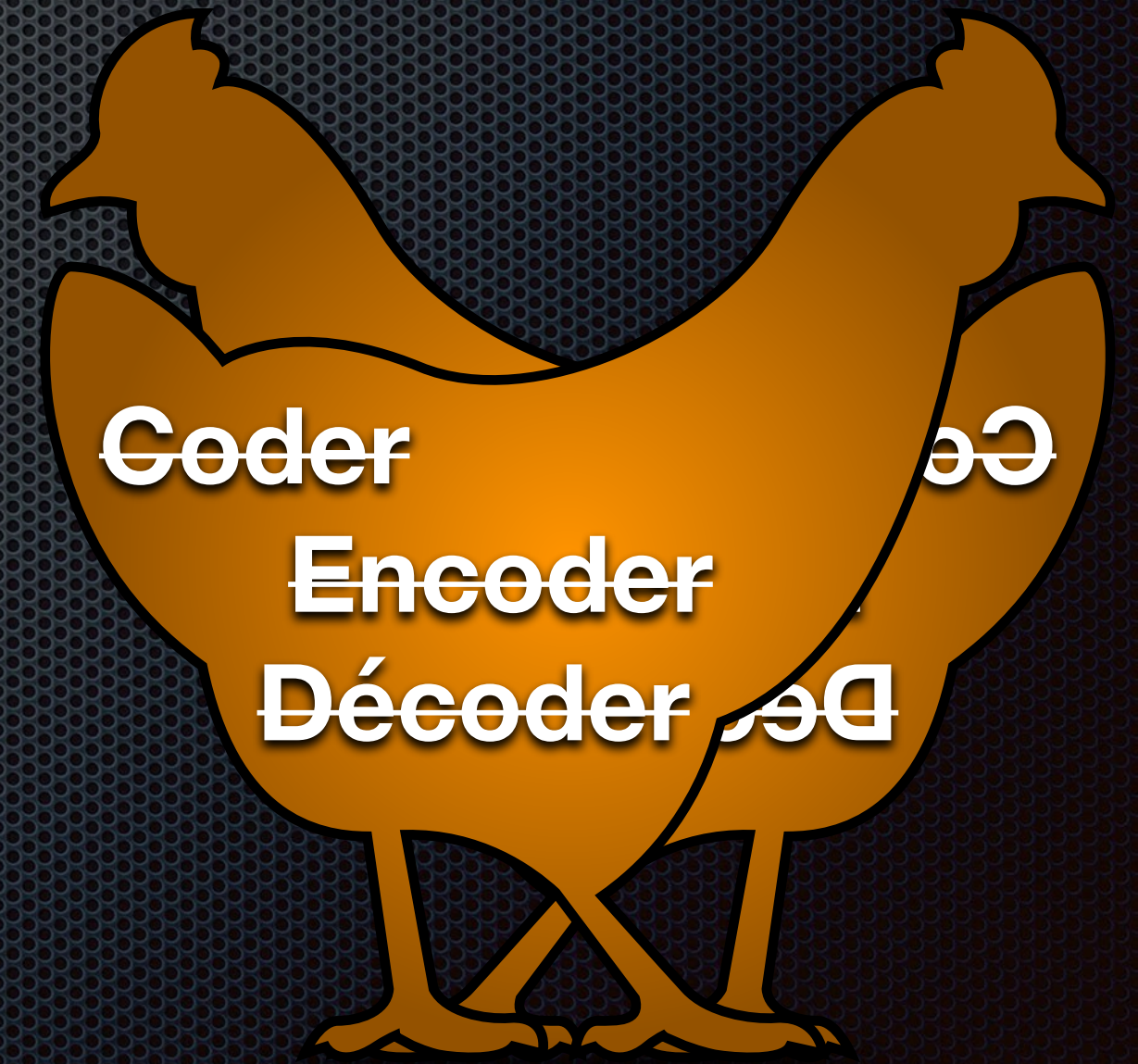
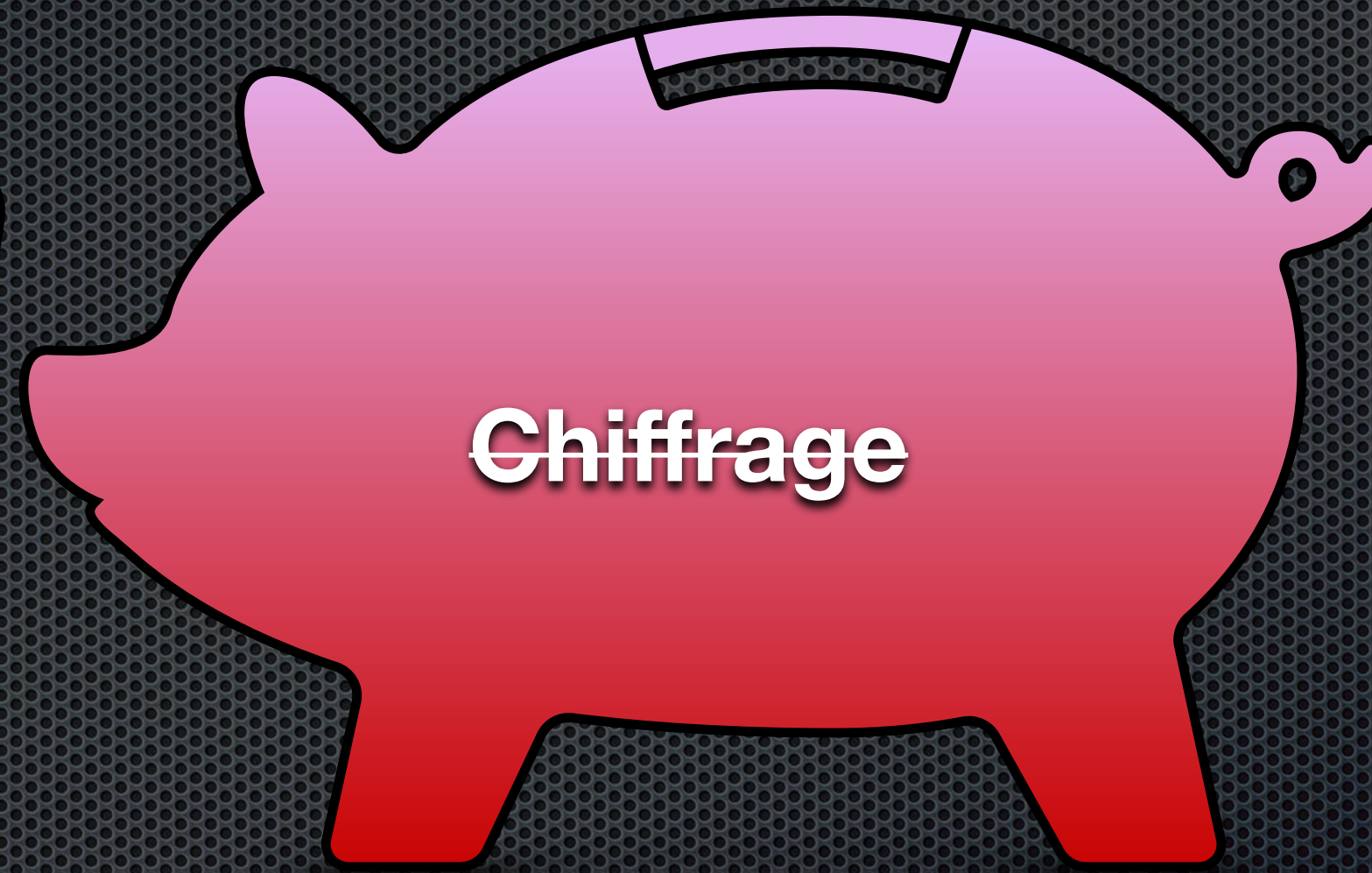
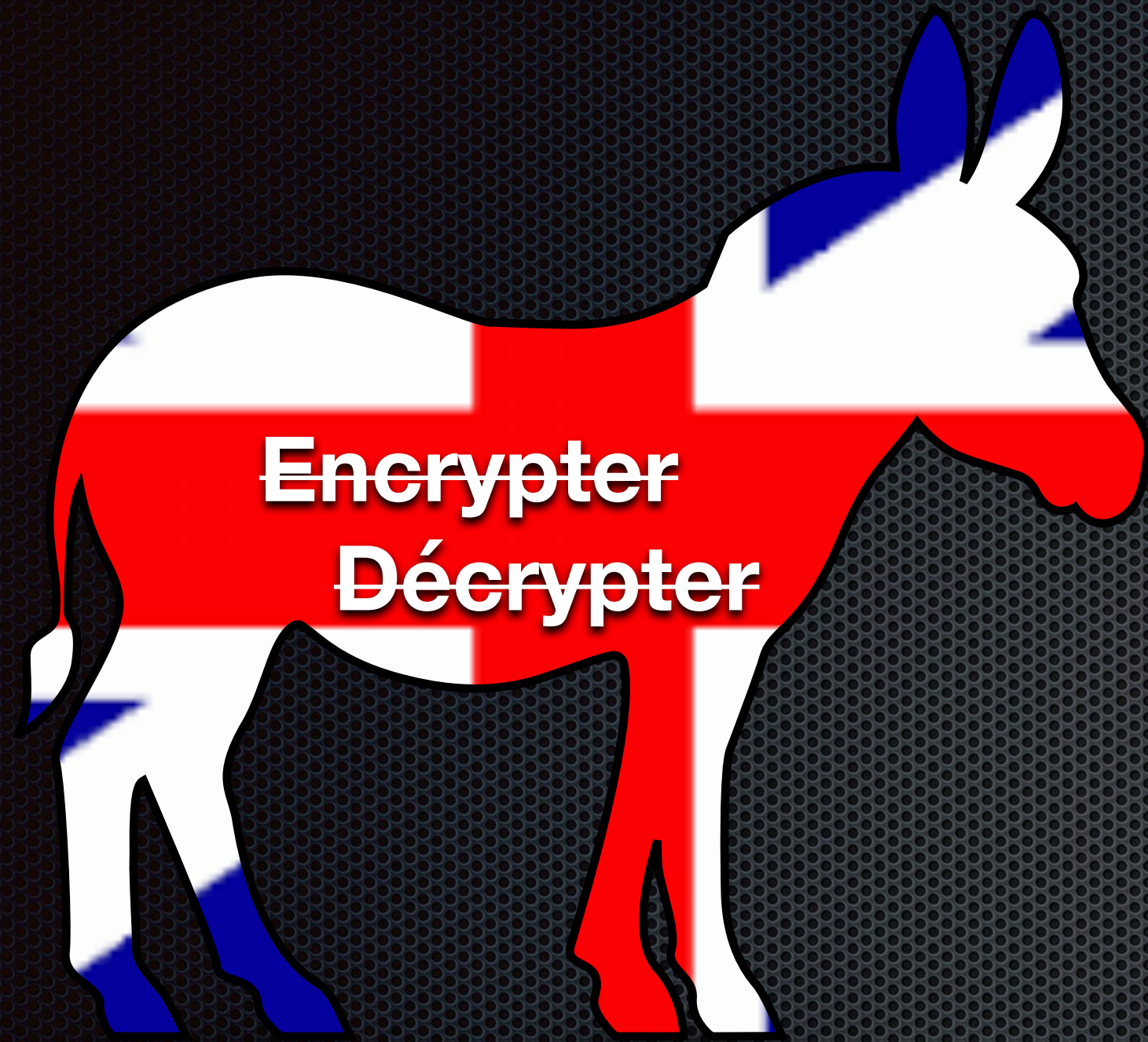


CRYPTANALYSE

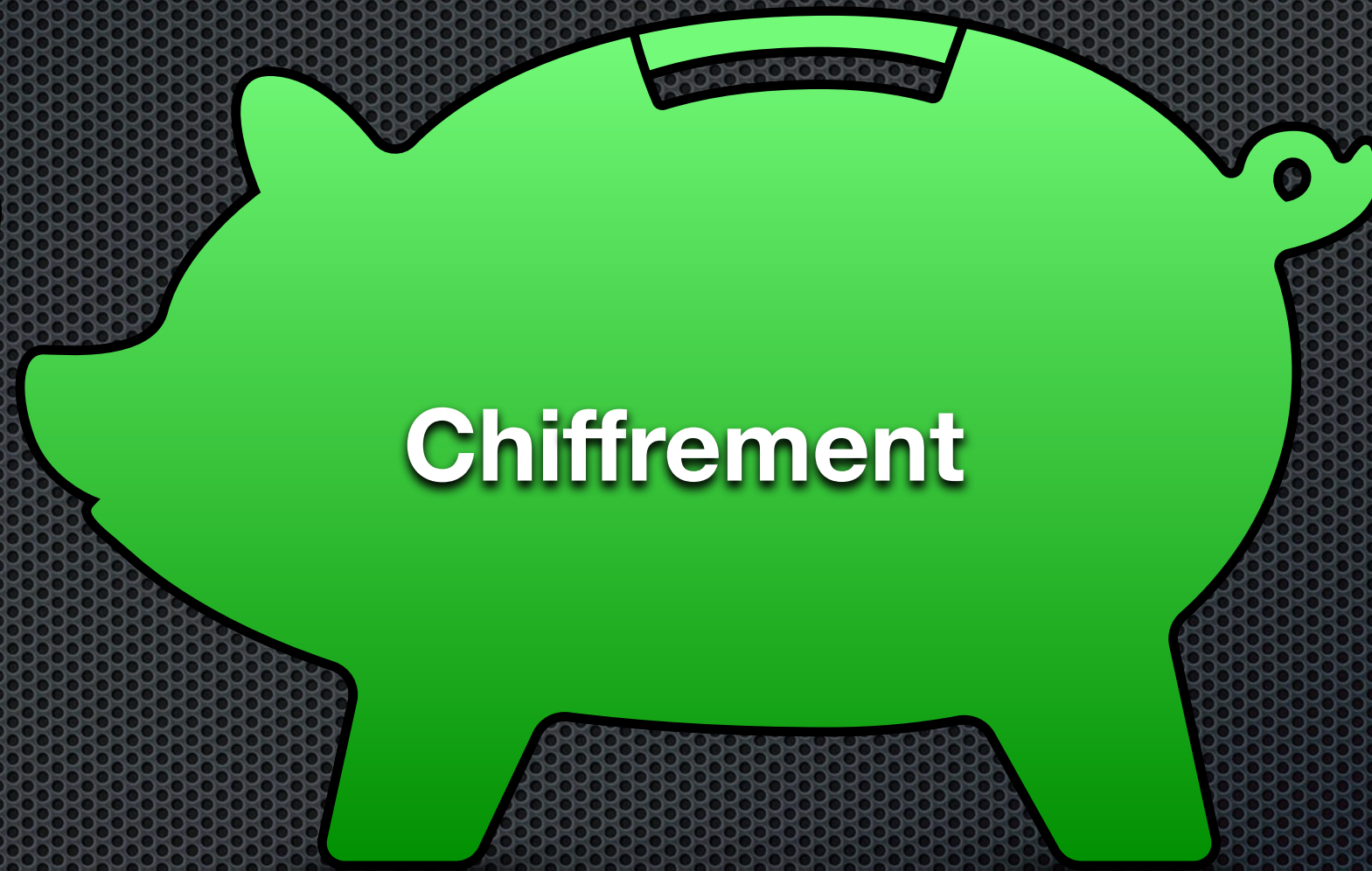
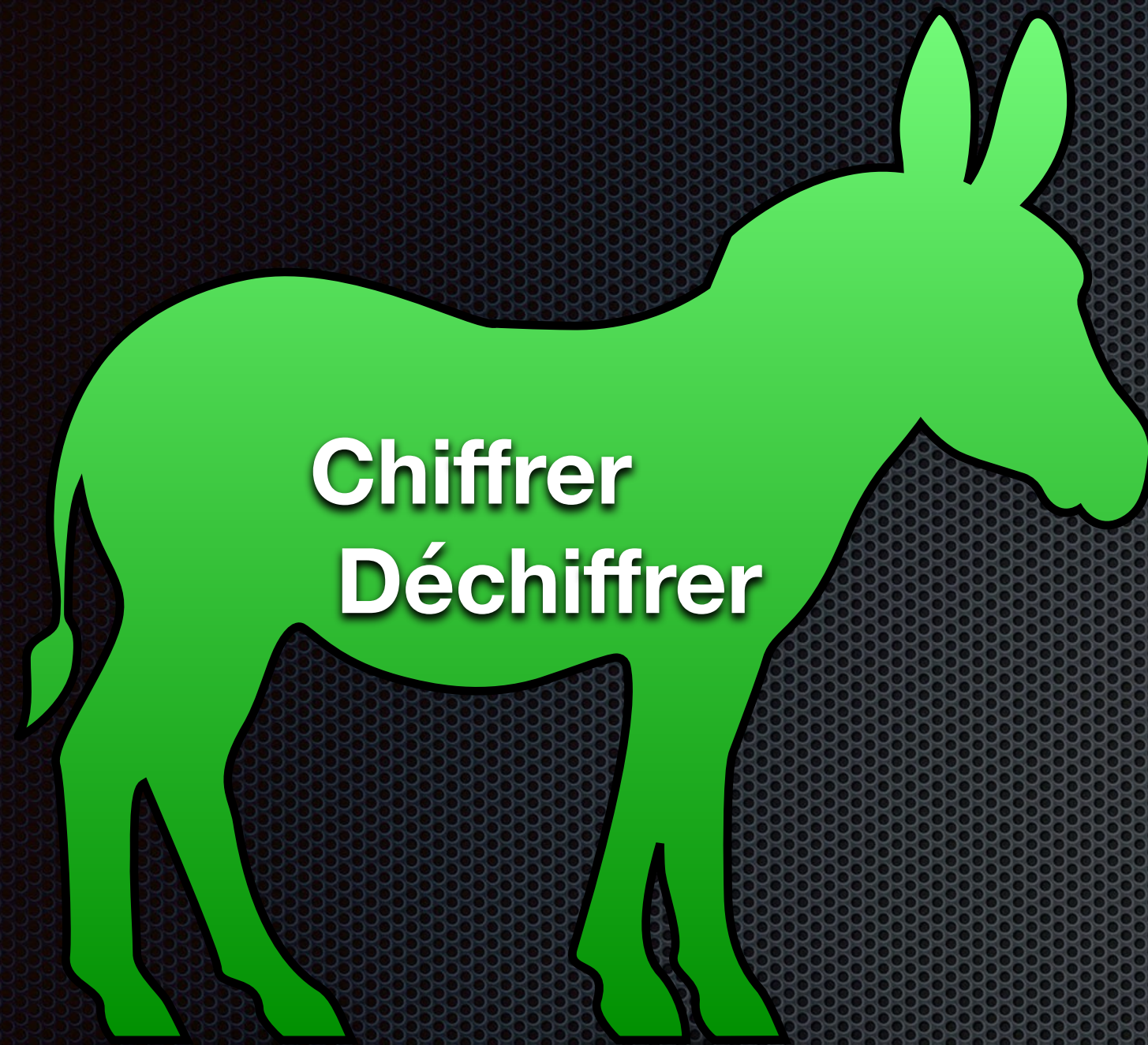
Analyse et attaque de la
cryptographie



On ne dit pas



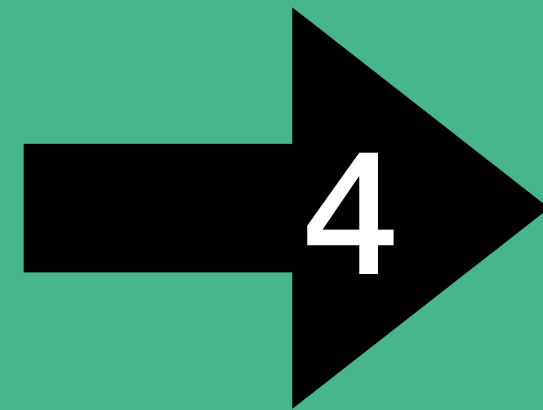
On dit



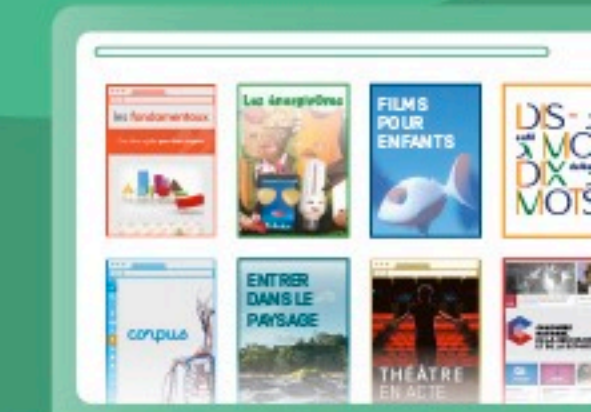
Exemple décryptement

Du code de César par la fréquence des lettres dans une langue

« La science du secret c'est la cryptologie. On y retrouve, la cryptographie qui s'intéresse à l'écriture secrète, la cryptanalyse qui nous permettrait de comprendre en message secret et la stéganographie (à ne pas confondre avec la sténographie) qui est l'art de dissimuler des secret dans des message qui n'en ont apparemment pas. »



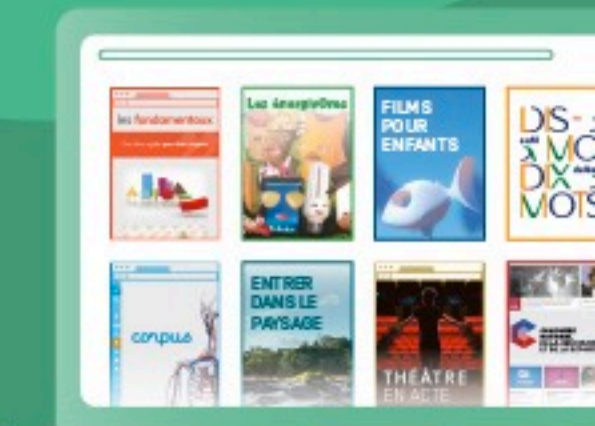
Pe\$wgmirgi\$hy\$wigvix\$g"iwx\$pe\$gv}
txspskmi2\$Sr\$}\$vixvsyzi0\$pe\$gv}
txskvetlmi\$uym\$w"mrxíviwwi\$ä\$p"ígv
mxyvi\$wigvixi0\$pe\$gv}
txerepmwi\$uym\$rsyw\$stivqixxvemx\$hi\$
gsqtvirhvi\$ir\$qiwweki\$wigvix\$ix\$pe\$wx
íkerskvetlmi\$,ä\$ri\$stew\$gsrjsrhvi\$ezig\$p
e\$wxírskvetlmi-
\$uym\$iwx\$p"evx\$hi\$hmwwmqypiv\$hiw
\$wigvix\$herw\$hiw\$qiwweki\$uym\$r"ir\$s
rx\$etteviqqirx\$stew2



Exemple décryptement

Du code de César par la fréquence des lettres dans une langue

Pe\$wgmirgi\$hy\$wigvix\$g"iwx\$pe\$gv}
txspskmi2\$Sr\$}\$vixvsyzi0\$pe\$gv}
txskvetlmi\$uym\$w"mrxiwwi\$ä\$p"ígv
mxyvi\$wigvixi0\$pe\$gv}
txerepmwi\$uym\$rsyw\$stivqixxvemx\$hi
\$gsqtvirhvi\$ir\$qiwweki\$wigvix\$ix\$pe\$
wxíkerskvetlmi\$,ä\$ri\$stew\$gsrjsrhvi\$ezi
g\$pe\$wxírskvetlmi-
\$uym\$ix\$p"evx\$hi\$hmwwmqypiv\$hi
w\$wigvix\$herw\$hiw\$qiwweki\$uym\$r"i
r\$srx\$etteviiqqirx\$stew2



Exemple décryptement

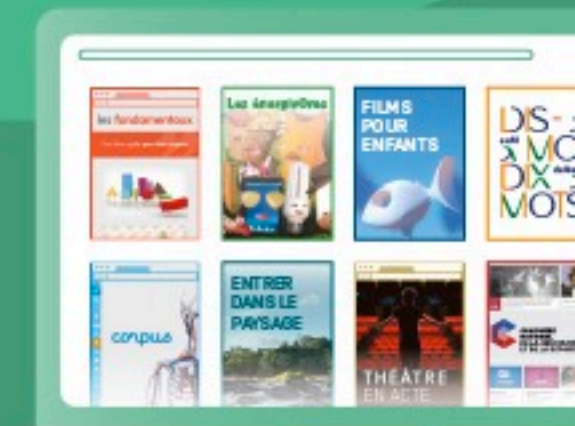
Du code de César par la fréquence des lettres dans une langue

Pe\$wgmirgi\$hy\$wigvix\$g"iwx\$pe\$gv}
txspskmi2\$Sr}\$vixvsyzi0\$pe\$gv}
txskvetlmi\$uym\$w"mrxiwwi\$ä\$p"ígv
mxyvi\$wigvixi0\$pe\$gv}
txerepmwi\$uym\$rsyw\$tiqixxvemx\$hi
\$gsqtvirhvi\$ir\$qiwweki\$wigvix\$ix\$pe\$
wxíkerskvetlmi\$,ä\$ri\$stew\$gsrjsrhvi\$ezi
g\$pe\$wxírskvetlmi-
\$uym\$ix\$pe\$evx\$hi\$hmwwmqypiv\$hi
w\$wigvix\$herw\$hiw\$qiwweki\$uym\$r"i
r\$srx\$etteviiqirx\$stew2

i → ? e

h g f

→ -4



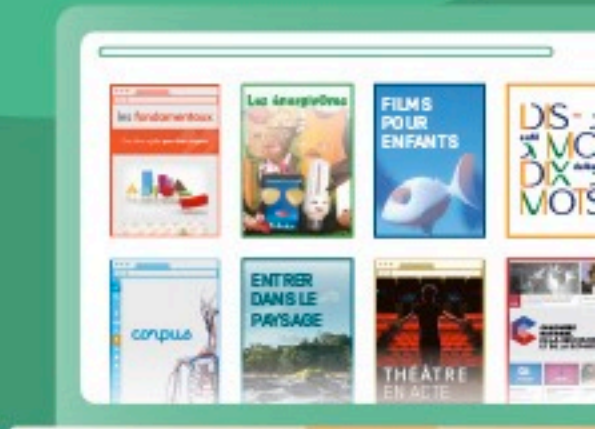
Exemple décryptement

Du code de César par la fréquence des lettres dans une langue

Pe\$wgmirgi\$hy\$wigvix\$g"iwx\$pe\$
gv}txspskmi2\$Sr\$}
\$vixvsyzi0\$pe\$gv}
txskvetlmi\$uym\$w"mrxíviwwi\$ä\$p
"ígvmxyvi\$wigvixi0\$pe\$gv}
txerepmwi\$uym\$rsyw\$stivqixxvem
x\$hi\$gsqtvirhvi\$ir\$qiwweki\$wigvix
\$ix\$pe\$wxíkerskvetlmi\$,ä\$ri\$tew\$
gsrjsrhvi\$ezig\$pe\$wxírskvetlmi-
\$uym\$iwx\$p"evx\$hi\$hmwwmqypi
v\$hiw\$wigvix\$herw\$hiw\$qiwweki\$
uym\$r"ir\$srx\$etteviqqirx\$tew2



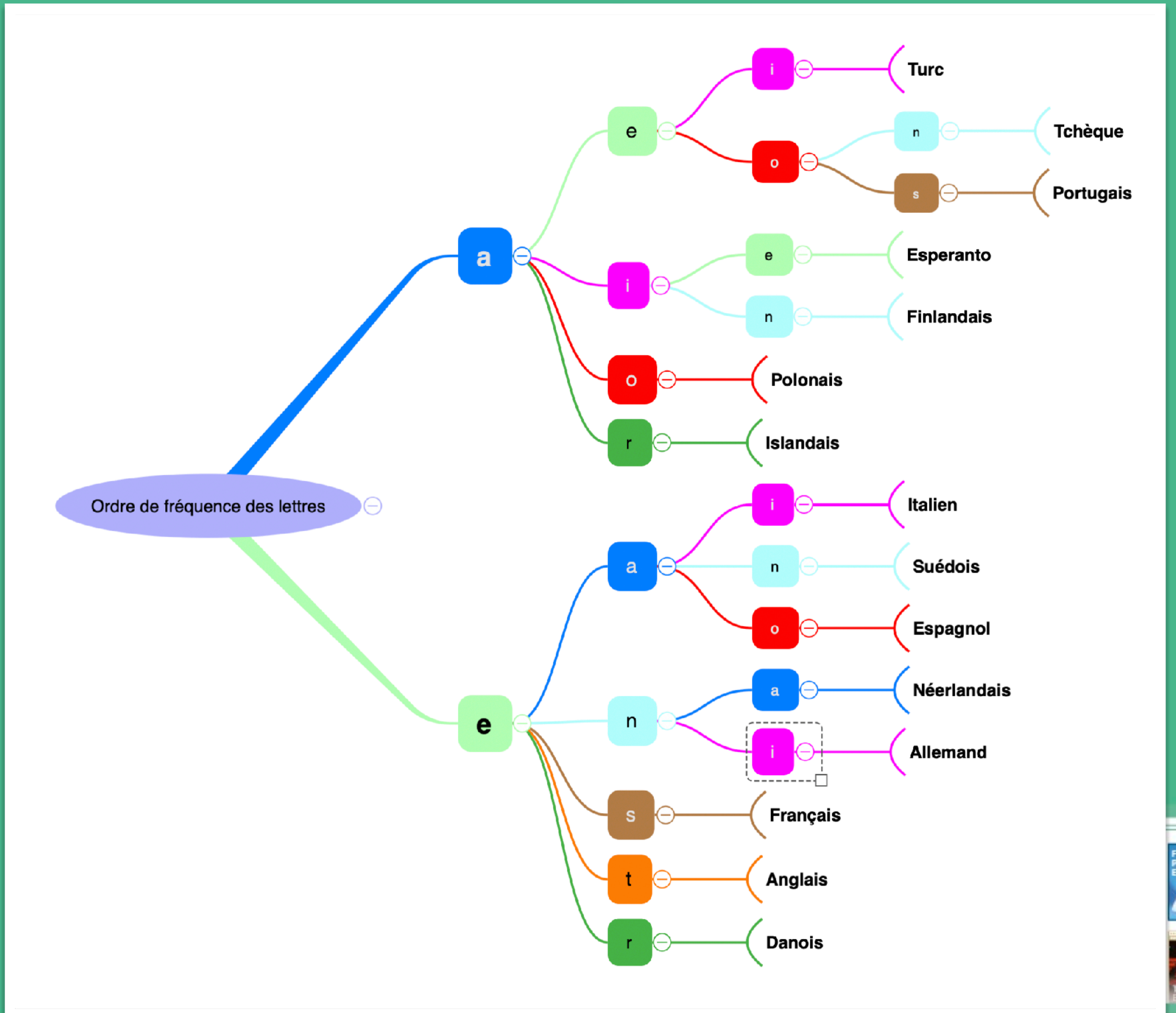
La science du secret c'est la cryptologie. On y retrouve, la cryptographie qui s'intéresse à l'écriture secrète, la cryptanalyse qui nous permettrait de comprendre un message secret et la stéganographie (à ne pas confondre avec la sténographie) qui est l'art de dissimuler des secrets dans des messages qui n'en ont apparemment pas.



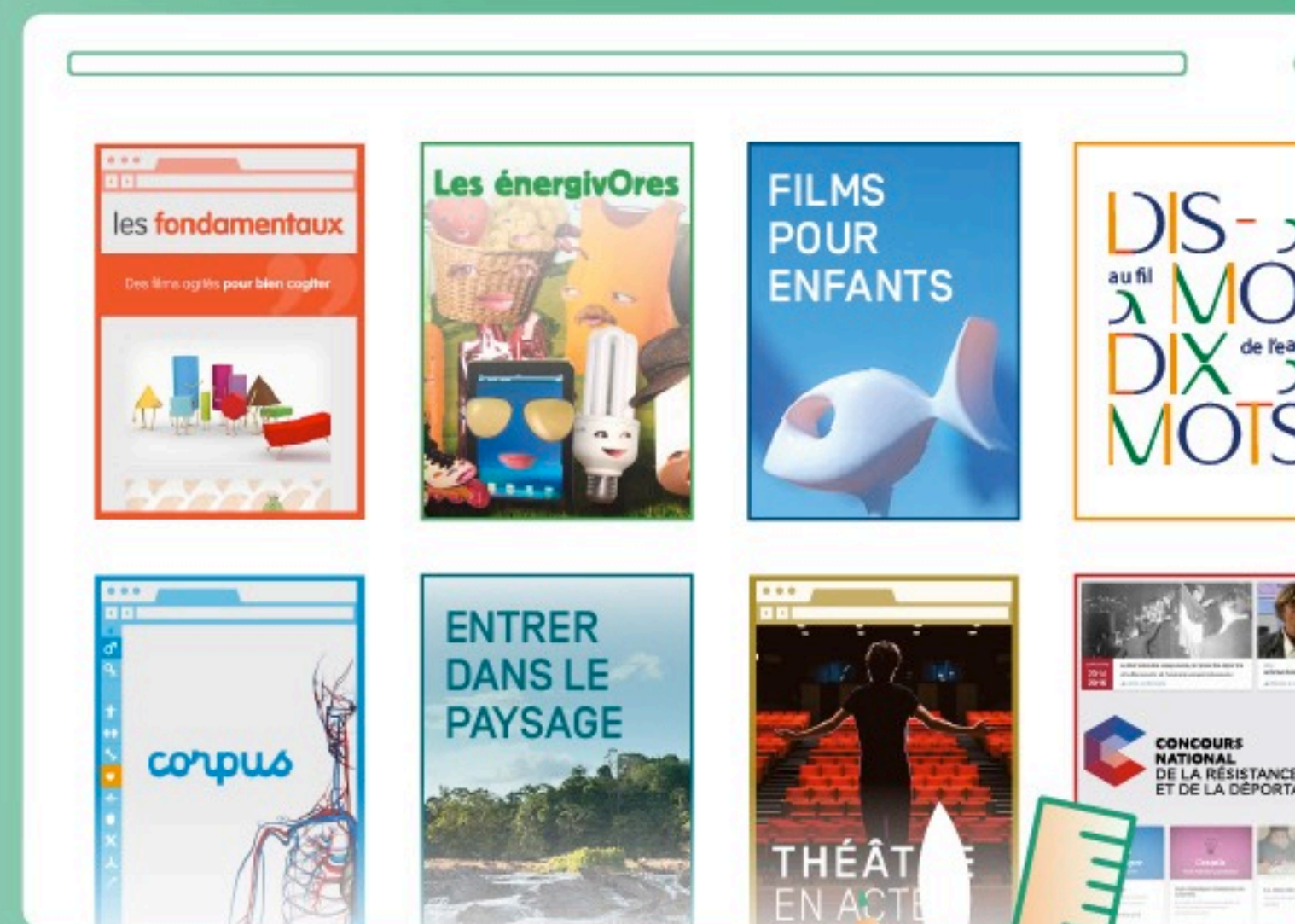
Fréquence des lettres dans ≠ langues

allemand 🇩🇪
anglais 🇬🇧
danois 🇩🇰
espagnol 🇪🇸
esperanto 🇪🇸
finlandais 🇫🇮
français 🇫🇷
islandais 🇮🇸
italien 🇮🇹
néerlandais 🇳🇱
polonais 🇵🇱
portugais 🇵🇹
suédois 🇸🇪
tchèque 🇨🇪
turc 🇹🇷

a e i o n s r t



SE FORMER



Merci à tous !

Vos attestations de présence et les liens vers les ressources citées seront prochainement dans votre espace MON AGENDA du site

<https://www.reseau-canope.fr/>

Retrouvez d'autres ressources sur

<https://www.reseau-canope.fr/canotech.html>