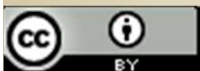


Enseigner l'informatique pour comprendre le numérique

Colin de la Higuera
Société informatique de France
Université de Nantes



Sommaire

(ce slide sautera)

1. Parmi les bonnes raisons d'enseigner l'informatique, il y a le fait que l'informatique est une science et une technique essentielle du 21^e siècle. Egalement que c'est une excellente nouvelle pour l'enseignement lui-même
2. Mais on observe que cet argument ne suffit pas Quelles sont les raisons ?
3. La question posée « former au numérique » : comprendre la question
4. Les positions possibles de l'informatique par rapport à cette question
5. Proposition : l'informatique comme moyen de comprendre le numérique
6. Un exemple complet
7. Conclusion



I Pourquoi enseigner l'informatique ?

- ▶ De nombreuses raisons liées à l'informatique elle-même :
 - ▶ L'emploi
 - ▶ Le besoin de maîtriser la pensée computationnelle
 - ▶ Le fait de pouvoir devenir créateur et non consommateur
- ▶ Des raisons liées à l'apprentissage lui-même
 - ▶ Coding is fun! (video de la BBC, expérience des associations): donne envie d'apprendre
 - ▶ L'enseignement de l'informatique est l'occasion d'enseigner autrement (cf par exemple Daniel Kaplan <http://www.internetactu.net/2014/10/13/jules-ferry-3-0-recit-dune-convergence/>)



SIF

2 Arguments convaincants mais...

- ▶ Les interventions des uns et des autres sur les forums, les blogs
- ▶ Le refus obstiné de différents acteurs institutionnels

montrent que nous (les informaticiens) ne répondons pas à **leur** question.



Raisons de ces difficultés



- ▶ (peut-être ont-ils raison ?)
- ▶ L'âge des intervenants (pas toujours !). Mais combien de décideurs pensent que leurs petits-enfants sont nés informaticiens ?
- ▶ La logique anti-sciences
 - ▶ [...]Je suis d'ailleurs surpris que le Conseil national du numérique entérine l'idée d'un CAPES et d'une agrégation d'informatique. Cela me gêne car ça territorialise l'informatique comme une matière scientifique. Il existe un risque, notamment, que les filles se disent « c'est une matière scientifique, ce n'est pas pour moi ».[...]



Et si on s'intéressait plutôt à la formation au numérique ?

- ▶ Il n'y a pas vraiment de définition de la formation au numérique sans l'informatique
- ▶ B2I, C2I ?
- ▶ **Rapport IG sur les ESPE (oct 2014)**
- ▶ " Le numérique. Que ce soit du côté des étudiants comme de celui des formateurs, sauf exception, le numérique paraît **quasiment absent de la formation** tant sur le plan des préoccupations pédagogiques et disciplinaires, qu'en tant qu'outil au service de la formation.«
- ▶ Or le volet numérique développé en 2012 dans tous les dossiers d'ESPE avait 2 particularités :
 - ▶ Il était très ambitieux
 - ▶ Il excluait l'informatique



3 Se comprendre

Leur question est :

Le monde est devenu numérique. Comment y préparer la jeunesse ?

Notre réponse est perçue comme :

A la place de résoudre ce problème, formez des informaticiens



4 Il faut faire quoi ?

- ▶ Continuer à expliquer qu'il faut former à l'informatique parce que ce sont des connaissances indispensables en 2015 pour
 - ▶ Le futur citoyen
 - ▶ Le futur professionnel
- ▶ Expliquer que leur préoccupation n'a pas de sens ?
- ▶ Démontrer que la simple formation aux usages du numérique ne suffit pas ?



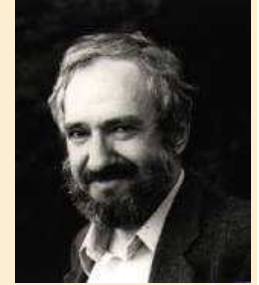
5 Nouvelle proposition

- ▶ Accompagner cette explication de la démonstration que l'informatique non seulement
 - ▶ Prépare à des métiers
 - ▶ Éduque le futur citoyen
 - ▶ Participe au développement de la France
 - ▶ Offre des possibilités de renouveau pédagogique
- Mais aussi
- ▶ Qu'il permet de comprendre le monde numérique



Exemple I

- ▶ Inspiré de Richard Noss (UCL), inspiré par Seymour Papert



- ▶ Combien font

▶ CCCXLVII * IV ?

(sans convertir)



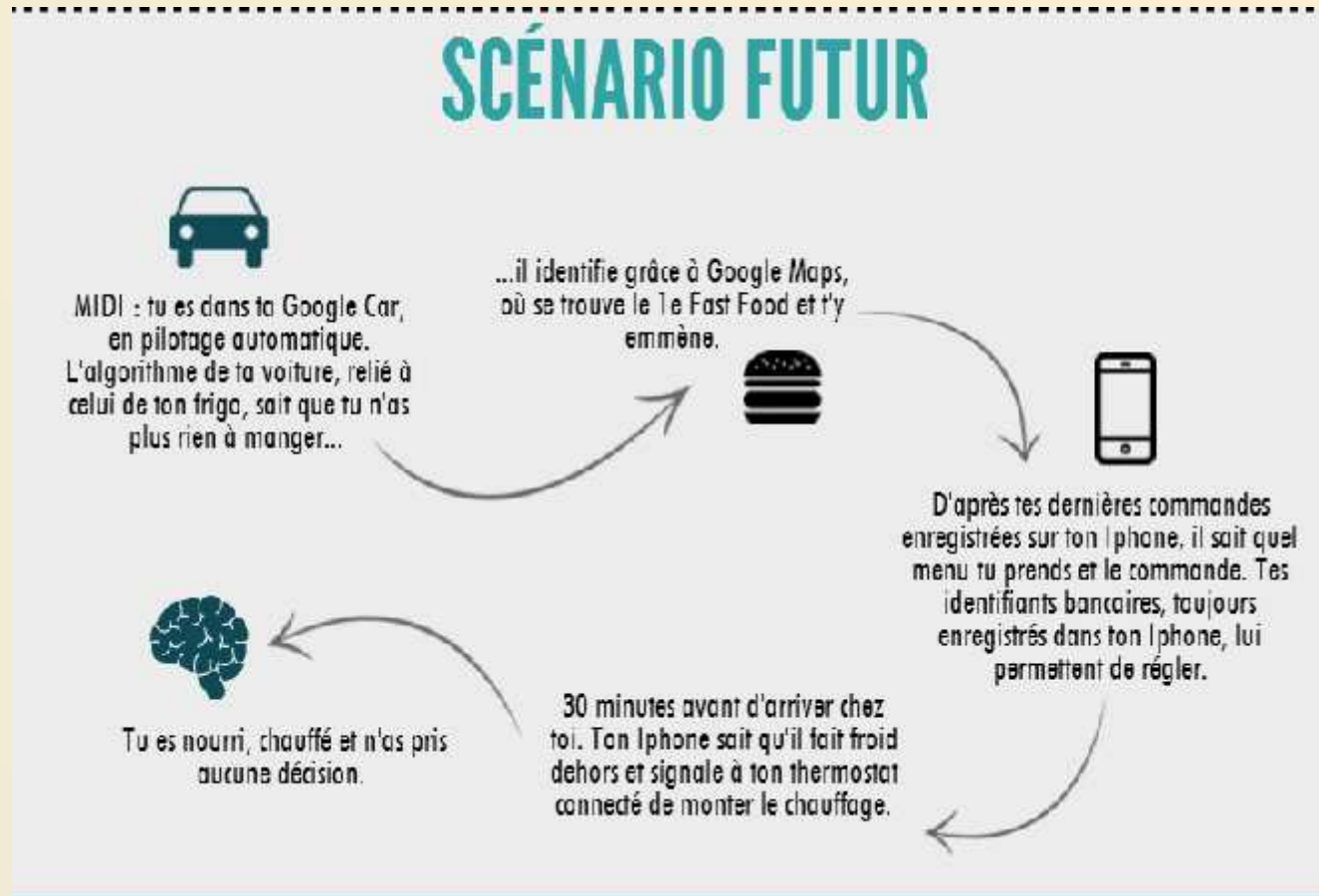
Exemple 2

- ▶ Comment passe-t-on de
- ▶ analyse ce texte
- ▶ À
- ▶ analyse ces textes

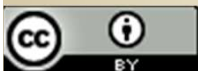
?

SIF

Exemple 3



<http://www.netpublic.fr/2014/06/15-infographies-pour-comprendre-les-enjeux-du-numerique/>





- ▶ Comment éviter que l'algorithme ait un *coût cognitif nul* ?
 - ▶ L'algorithme prend les décisions
 - ▶ L'algorithme décide...

En apprenant à construire des algorithmes,
bien sûr !



6 Un exemple complet

- ▶ Un enjeu important du numérique est tout ce qui touche à la sécurité
- ▶ Phishing, phreaking, spamming, pharming, whaling...
- ▶ Une question particulièrement sensible concerne les mots de passe
 - ▶ Changer le mot de passe
 - ▶ Tester son mot de passe
 - ▶ etc



Sécurité et Vie privée

[Accueil](#) [Sécurité](#) [Vie privée](#) [A la maison](#) [Ressources](#)

 [Imprimer](#)

Vérifiez votre mot de passe : est-il fort ?

Vos comptes en ligne, vos fichiers informatiques et vos informations personnelles sont plus en sécurité lorsque vous utilisez des mots de passe forts pour les protéger.

Testez la force de vos mots de passe : Tapez un mot de passe dans la zone.

Password:

Strength:

	Not rated		
--	-----------	--	--

Remarque Ceci ne garantit pas la sécurité du mot de passe. Cela ne doit servir que comme référence personnelle.

Qu'est-ce qu'un mot de passe fort ?

La force d'un mot de passe dépend des différents types de caractères utilisés, de la longueur globale du mot de passe et de la possibilité de trouver le mot de passe dans un dictionnaire. Sa longueur doit être de huit caractères, ou plus.

Pour des conseils sur la façon de créer des mots de passe forts dont il est facile de se rappeler, mais que les autres auront du mal à deviner, lisez [Créez des mots de passe forts](#).

À propos de Password Checker

Comment...

- Protéger mes enfants des risques en ligne
- Me protéger des arnaques
- Protéger mes informations personnelles
- Créer des mots de passe forts

[Vérifiez votre mot de passe](#)
[Créez des mots de passe forts](#)

📌 Tester la solidité d'un mot de passe 🖋️

Cette application est conçue pour évaluer la résistance des mots de passe. La rétroaction visuelle instantanée, caractère par caractère, donne à l'utilisateur un moyen d'améliorer la force de ses mots de passe, en montrant, par les bonus, l'incidence d'une bonne pratique et par les malus, la pénalisation des mauvaises habitudes typiques dans la formulation des mots de passe. Étant donné qu'aucun système de pondération officiel n'existe, nous avons créé nos propres formules pour évaluer la force globale d'un mot de passe.

- 🌟 **Mot de passe solide** : Dépasse les minimas universellement reconnus.
- ✅ **Mot de passe juste correct** : Atteint les minimas universellement reconnus.
- ⚠️ **Mot de passe dangereux** : Mauvaises pratiques dans la construction du mot de passe. Mot de passe faible.
- ❌ **Mot de passe en échec** : N'atteint même pas les minimas universellement reconnus. N'offre aucune protection par authentification.

Mot de passe	••••••••	Minimum requis : 8 caractères et constitué de :
Masquer	<input checked="" type="checkbox"/>	
Solidité	0%	
Complexité	Très faible	

- Majuscules
- Minuscules
- Chiffres
- Caractères spéciaux ou accentués

Dossier : Mots de passe

- [Mots de passe](#)
- [Identifiant](#)
- [Login \(procédure de login\)](#)
- [Test de solidité d'un mot de passe](#)
- [16 formes d'attaques des mots de passe](#)
- [Les types de jeux de caractères utilisés](#)
- [Les hashcodes \(ou condensats\)](#)
- [Exemples de hack de mots de passe](#)
- [Exemples de mots de passe imbéciles](#)
- [Un bon mot de passe - Côté utilisateur](#)
- [Une bonne authentification - Côté autorité](#)

Casser du mot de passe

- [Force brute et le problème du temps](#)
- [Dictionnaire \(construction\) et problème de taille](#)
- [Dictionnaire \(Attaque\)](#)
- [Rainbow Tables Compromis Temps / Mémoire](#)
- [Phishing](#)
- [Ingénierie sociale](#)
- Le loup dans la bergerie (Espionnage humain)**
- [Spyware \(Espionnage robotisé\)](#)
- [Keylogger](#)
- [Attitude négligente](#)
- [Ôter la pile](#)

- [Mots de passe par défaut \(les MDP d'usine\)](#)



Attention !


Qu'est-ce qui vous permet de croire que ce site (Assiste.com) n'est pas un site d'**ingénierie sociale** qui vous conduit à dévoiler vos mots de passe ?

Merci de faire confiance à Assiste.com mais soyez toujours prudent, même avec les sites dits "de sécurité".

Si vous avez simplement vérifié, ici, la solidité d'un mot de passe similaire à votre vrai "mot de passe", alors vous avez agi avec prudence, sinon, consultez [cette page](#).

Ce test de solidité est fait avec un script en JavaScript qui s'exécute localement, dans votre ordinateur, sans aucune communication avec l'extérieur.





Il est impossible d'expliquer *les mots de passe* à une personne qui n'a pas étudié

- ▶ L'algorithmique
- ▶ Les machines : leur fonctionnement
- ▶ Les langages (et donc les protocoles)
- ▶ Les données : et en particulier, ici, les codages

?

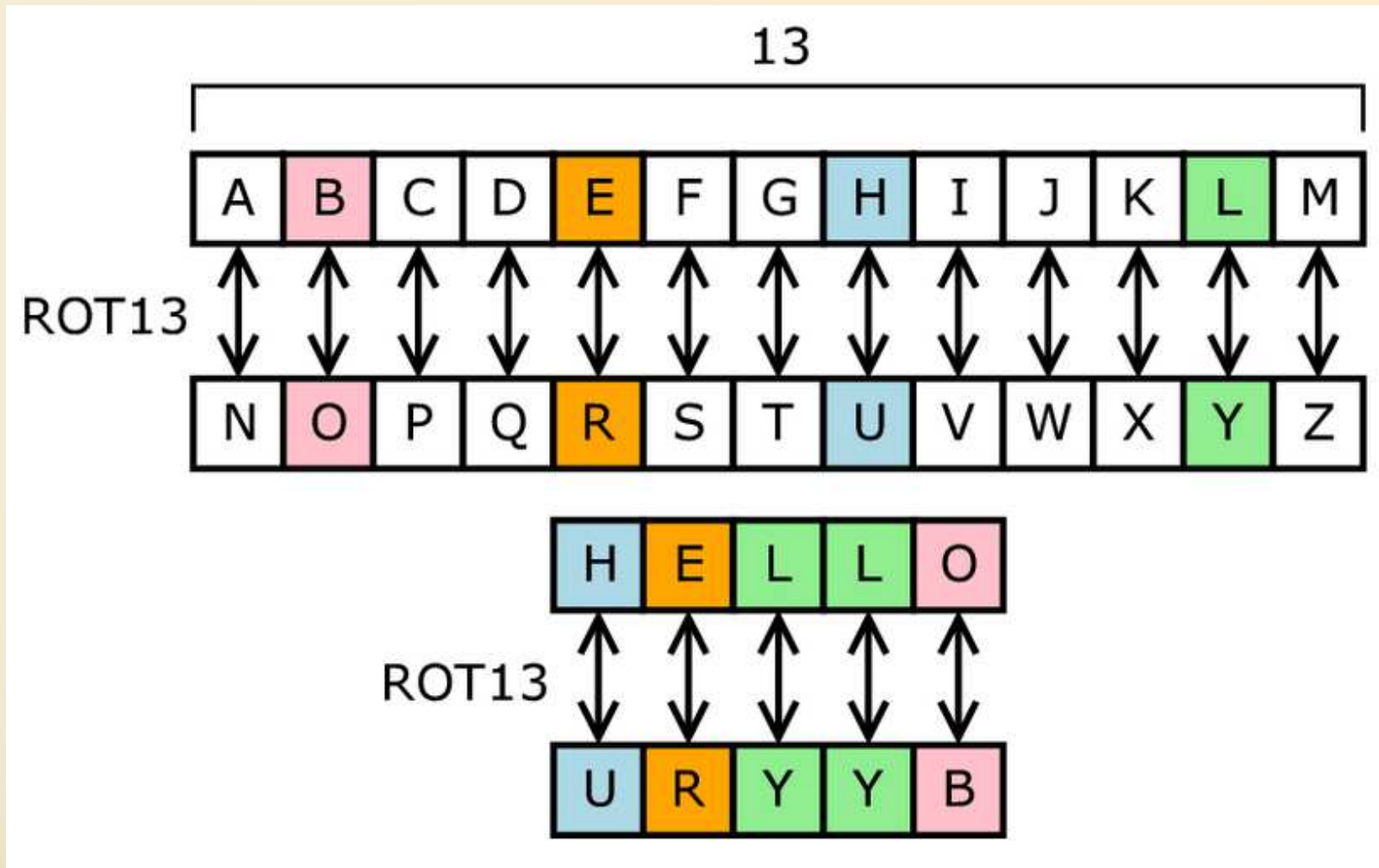



Supposons par contre qu'on puisse s'appuyer sur des compétences (croissantes) en informatique

- ▶ On peut apprendre :
 - ▶ À coder, décoder
 - ▶ À écrire un programme qui code et qui décode un code simple (le code de César)
 - ▶ À écrire un programme encore plus simple qui décode le code de César dont on n'a pas la clé
 - ▶ À écrire un programme qui décode un code encore plus compliqué
 - ▶ À mesurer comment et pourquoi certains codes sont meilleurs que d'autres
 - ▶ À retrouver l'importance des codes en histoire
 - ▶ À utiliser les mêmes idées de programmes sur les codes pour étudier du français, des mathématiques,...



Le code de César



- 
- ▶ Il semble que César n'utilisait qu'un décalage de 3. Son neveu Auguste, ne faisait qu'un décalage de 1 mais ne connaissait pas le modulo. Le chiffrement de z était aa.

(source : wikipedia)

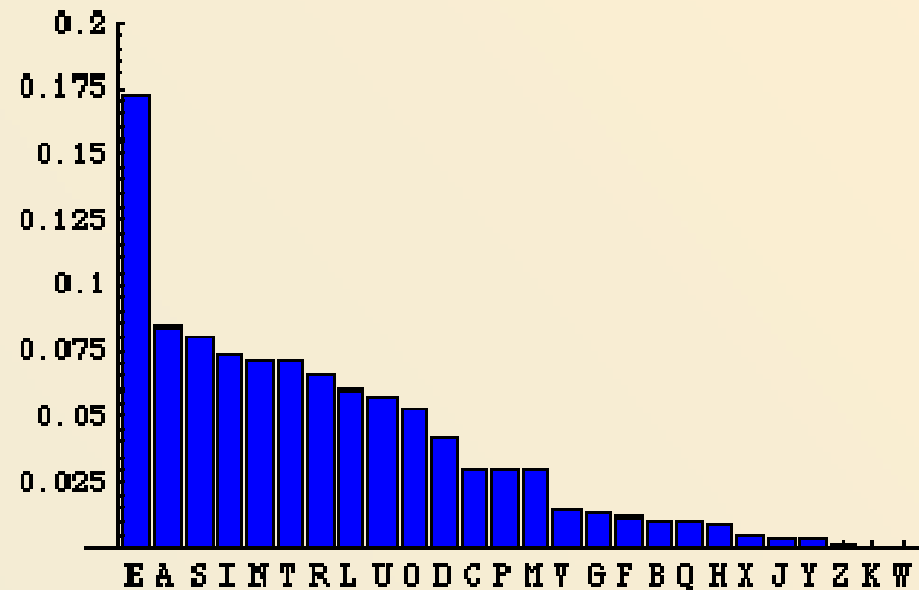


Autres chiffrements par substitution monoalphabétique

- ▶ ABCDEFGHIJKLMNOPQRSTUVWXYZ
AZERTYUIOPQSDFGHJKLMWXCVBN
- ▶ le message *SUBSTITUTION* devient *LWZLMOMWMOGF*.
- ▶ Nombre de clés possibles $26! \approx 2^{88.4}$ soit environ 88 bits



Analyse des fréquences en français



SIF

Analyse des fréquences en français

Les 20 bigrammes les plus fréquents

Bigrammes ES DE LE EN RE NT ON ER TE EL AN SE ET LA AI IT ME OU EM IE

Nombres 3318 2409 2366 2121 1885 1694 1646 1514 1484 1382 1378 1377 1307 1270 1255 1243 1099 1086 1056 1030

Les 20 trigrammes les plus fréquents

Trigrammes ENT LES EDE DES QUE AIT LLE SDE ION EME ELA RES MEN ESE DEL ANT TIO PAR ESD TDE

Nombres 900 801 630 609 607 542 509 508 477 472 437 432 425 416 404 397 383 360 351 350



Intégration dans les programmes

- ▶ Question : à quel âge peut-on enseigner aux enfants à casser ces codes ?
- ▶ Question : en quoi est-ce intéressant ?
- ▶ Ecole
- ▶ Collège
- ▶ Lycée



A l'école

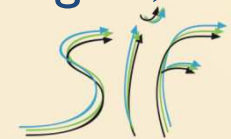
- ▶ A l'école primaire (milieu) découper le codeur de César ci-dessous et l'utiliser pour coder et décoder des textes courts
- ▶ A l'école primaire (fin), apprendre à écrire un codeur et un décodeur. Peut accompagner le cours d'histoire : le code de César (si les Romains sont encore au programme)



Sif

Au collège

- ▶ Ecrire des algorithmes d'analyse fréquentielle de texte : permet de compter le nombre d'occurrences d'un caractère.
- ▶ Écrire des algorithmes de recherche rapide, permettant de rechercher si un mot appartient à une base de données. Ecrire une version rusée de l'algorithme permettant de vérifier si un mot écrit avec des majuscules et des minuscules appartient à un dictionnaire. Le faire sur des dictionnaires réels.
- ▶ Voir que sur certains problèmes l'algorithme ne peut pas résoudre : on voit vraiment que le problème n'est pas résolu. Si l'élève a appris à programmer, il peut tenter de trouver quand même une solution, échouer, ce qui le confortera dans cette connaissance qu'il y a effectivement des problèmes non solvables, des mots de passe increquables.
- ▶ En histoire (des sciences) : qui était Turing, la machine Enigma, l'invention de l'ordinateur



Au lycée

- ▶ D'autres codes peuvent être étudiés. Des liaisons peuvent être faits en mathématiques avec
 - ▶ Les statistiques (il faut effectuer des tests statistiques)
 - ▶ La théorie des nombres (puisque ce sont ces idées qui sont au cœur des questions de cryptographie)
 - ▶ Le Français : l'analyse fréquentielle peut être utilisée pour étudier les auteurs :
 - ▶ Les phrases de Proust sont-elles vraiment plus longues ?
 - ▶ Quelles sont les tailles de vocabulaires de différents auteurs ?
- ▶ Un projet possible en ISN : construire soi même son vérificateur de mots de passe. Possibilité de se comparer aux autres (mon détecteur détecte ton mot de passe).



Risque de former de futurs escrocs du net ?

- ▶ Autant que de former des futurs délinquants en enseignant le judo
- ▶ Autant que de former des futurs obèses en enseignant la cuisine
- ▶ Au fur et à mesure que les technologies évolueront, le jeune aura appris à comprendre les enjeux



A surveiller

- ▶ L'ébauche de programme qui précède n'a pas été discuté avec les autres disciplines
- ▶ En le faisant, il y a fort à parier
 - ▶ Que de nouvelles idées émergeront
 - ▶ Que parmi celles énoncées ici, plusieurs seront remplacées par d'autres meilleures



7 Quelques propositions

- ▶ Enseigner l'informatique
- ▶ Le faire enseigner par des enseignants formés pour cela
- ▶ Que ces enseignants soient particulièrement attentifs à leur rôle pédagogique :
 - ▶ Projets
 - ▶ Interaction nécessaire avec les autres disciplines
 - ▶ Nouvelles modalités éducatives
- ▶ Ces enseignants doivent comprendre les objectifs de leur enseignement !



Objectifs de l'éducation

- ▶ Il s'agit de donner aux élèves (puis étudiants citoyens) les moyens de
 - ▶ Modéliser
 - ▶ Traiter une information de plus en plus complexe et hétérogène
 - ▶ Comprendre le fonctionnement d'un système numérique
 - ▶ Créer ses propres outils de simulation, animation, calcul, représentation,...
 - ▶ Continuer à apprendre



Ca implique

- ▶ Savoir **coder**
- ▶ Savoir comment se représente **l'information**
- ▶ Savoir comment on utilise un **langage** pour transmettre et traiter l'information
- ▶ Savoir comment une **machine** traite ces informations
- ▶ Toutes choses que l'on peut enseigner (à condition de disposer d'enseignants formés –ce qui prend du temps-) dès l'école



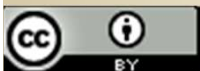
Il est possible que tout ceci tienne
d'une vérité de La Palice



Wikipedia.fr

Tant mieux

SIF



Annexes



Vincent Bardeau

Ce slide ne passera pas

- ▶ Vous nous ils, 10 octobre
- ▶ [...] Je suis d'ailleurs surpris que le Conseil national du numérique entérine l'idée d'un CAPES et d'une agrégation d'informatique. Cela me gêne car ça territorialise l'informatique comme une matière scientifique. Il existe un risque, notamment, que les filles se disent « c'est une matière scientifique, ce n'est pas pour moi ». [...]

