

Un chercheur :

Valentin Suder

Une enseignante :

Marie-Pierre Cribier

Une classe :

La seconde 7 du lycée Camille
Saint-Saëns

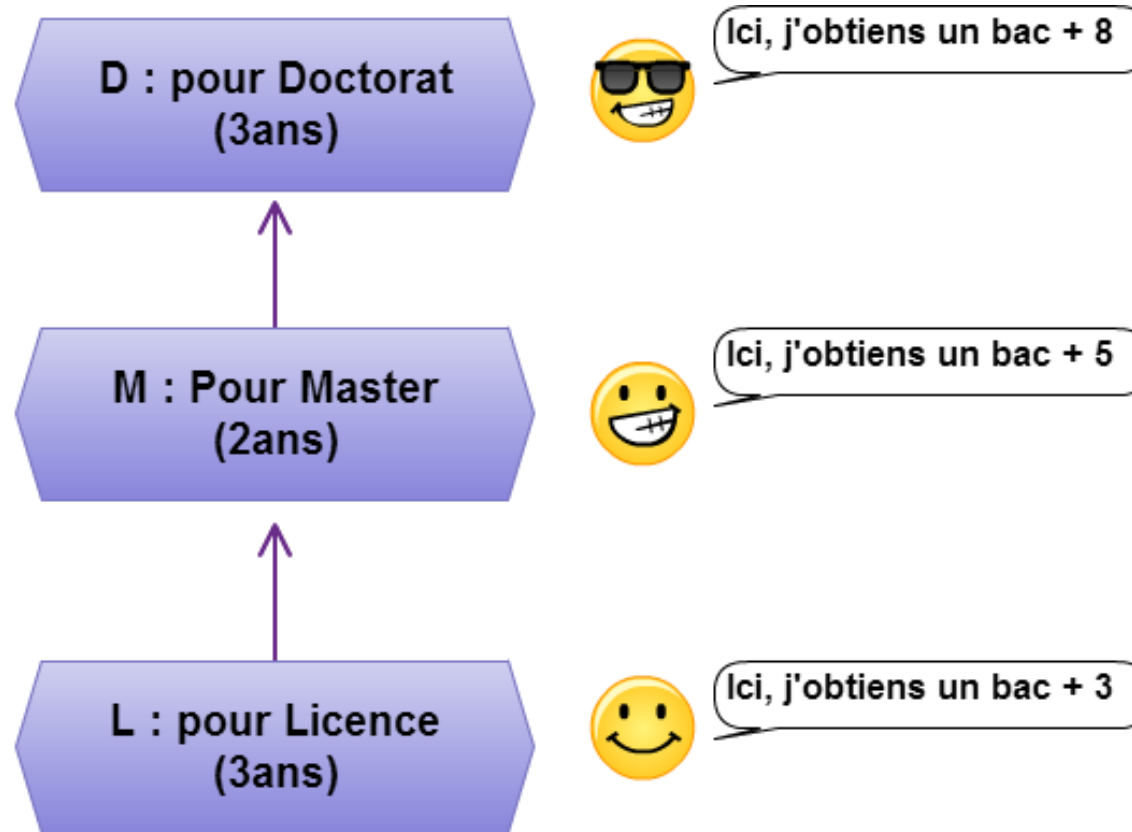


L'université et son fonctionnement



Université de Madrillet

Les diplômes universitaires



Le parcours universitaire

Que faire avec un master ?



Spécialiste en cybersécurité



Enseignante-chercheuse

Qu'est-ce qu'un enseignant chercheur ?

Un métier double

- Enseigne à l'université
- Fait de la recherche scientifique
- Travaille dans un laboratoire
- Transmet et produit des connaissances



illustration : enseignant



illustration : chercheurs dans un laboratoire

Le rôle d'enseignant

Transmettre les connaissances

- Donner des cours
- Préparer les support
- Corriger les copies
- Accompagner les étudiants
- Évaluer les connaissances



illustration : Enseignant donnant des cours

Le rôle de chercheur

Faire avancer la science

- Lire (beaucoup) pour apprendre et comprendre
- Résoudre des problèmes (pas beaucoup)
- Vérifier les solutions des autres (beaucoup)
- Créer des problèmes
- Parler beaucoup (avec les autres chercheurs)



illustration : mener des recherches



illustration : assister à des conférences

Le quotidien et les défis

Un métier exigeant mais passionnant

- Emploi du temps chargé
- Organisation nécessaire
- Pression des résultats
- Travail varié
- Métier de passion
- Beaucoup de café (beaucoup, beaucoup)

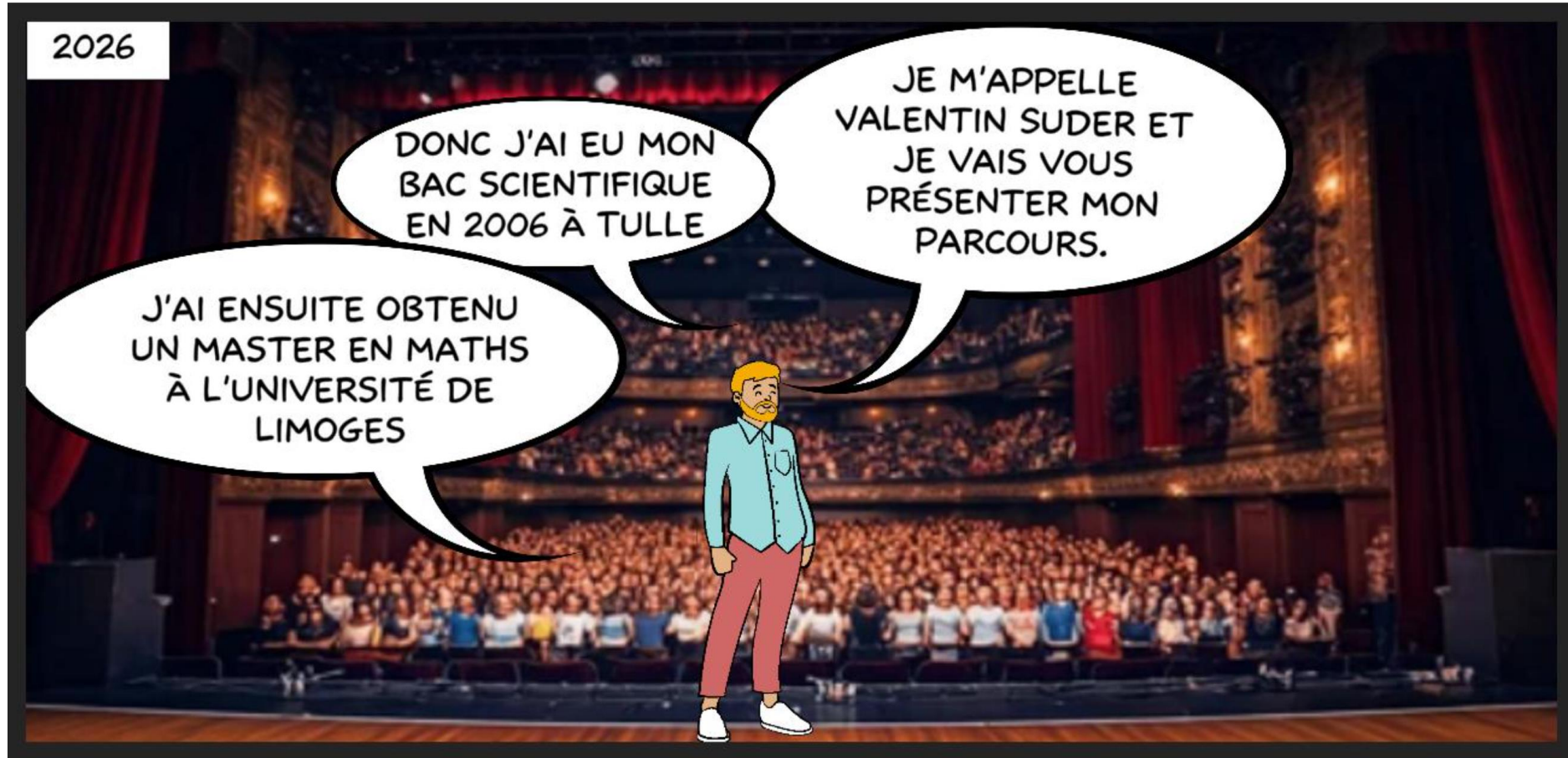


illustration : emploi du temps



illustration : homme avec du café

Notre chercheur : Valentin Suder



PUIS À PARIS J'AI AUSSI
OBTENU MON DOCTORAT
EN CRYPTES



J'AI OCCUPÉ UN POSTE
POSTDOCTORAL À
L'UNIVERSITÉ DE WATERLOO



IL EFFECTUE DES RECHERCHES
AU SEIN DE L'UNIVERSITÉ DE
VERSAILLES SAINT-QUENTIN



Créé avec l'application **BDNF** développée par la { BnF

Les menaces informatiques

- Phishing
- Virus et malwares
- Intrusions réseau
- Vol de données



Bonjour,

Une connexion a eu lieu grâce à FranceConnect :

Merci d'avoir utilisé notre service.

Si ce n'était pas vous, [cliquez ici](#).

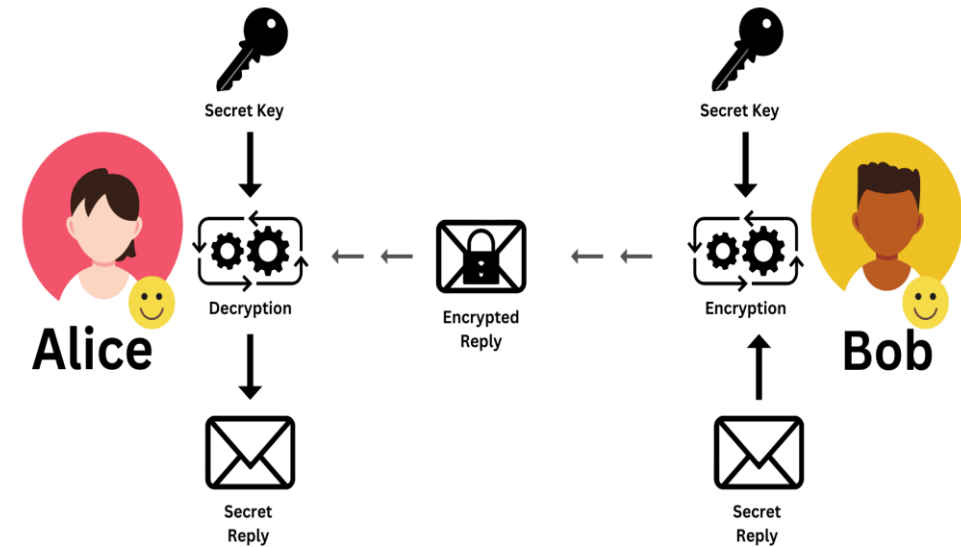
Pour plus d'informations, consultez notre FAQ Usagers à l'adresse suivante :
<https://franceconnect.gouv.fr/faq>

Pour toute autre question en lien avec votre démarche, merci de contacter le support du site www.impots.gouv.fr.

https://www.wiclic.fr/wp-content/uploads/2021/05/phishing_banque.jpg

La cryptologie

- Cryptographie
- Cryptanalyse
- Chiffrement
- Transmissions sécurisée



<https://codimite.ai/wp-content/uploads/2-1.png>

Les 4 Grands Principes

- Confidentialité
- Authenticité
- Intégrité
- Non-répudiation

5 Key Steps for **Cyber Safety Assessment**



<https://www.fortinet.com/fr/resources/cyberglossary/cyber-safety>

@ITLAW avocats



Cryptologie

- Κρυπτός (le secret)
- Λόγος (la science)

@dreamstime



@THALES

Images représentatives de la cryptologie



@tice-education

Cryptologie

@groupe telecoms de l'ouest

Cryptographie

Illisible sans secret

Clé secrète

Chiffre de César



Message

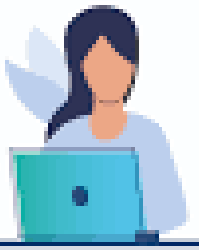
Le chiffrement symétique

Chiffrement



Texte chiffré

Déchiffrement



Message



Clé secrète

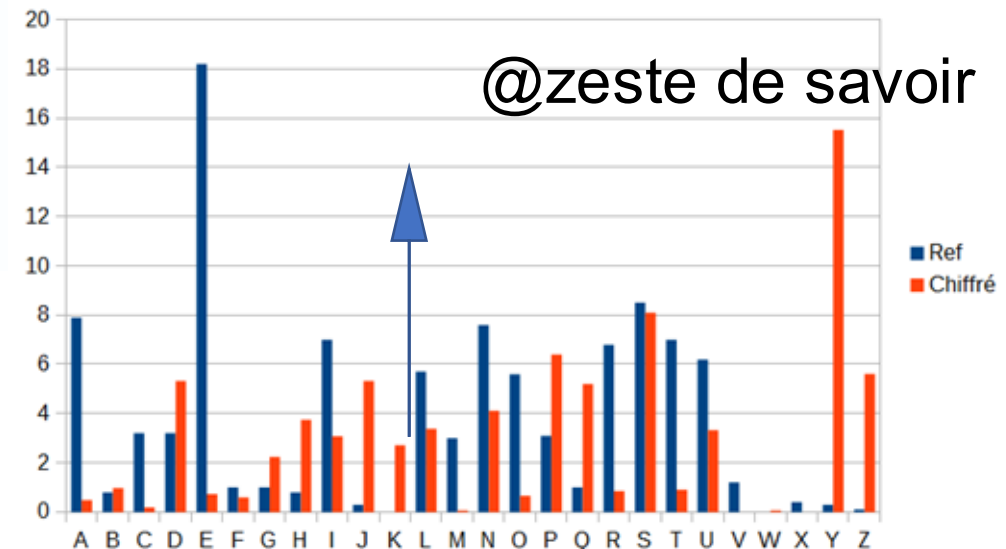
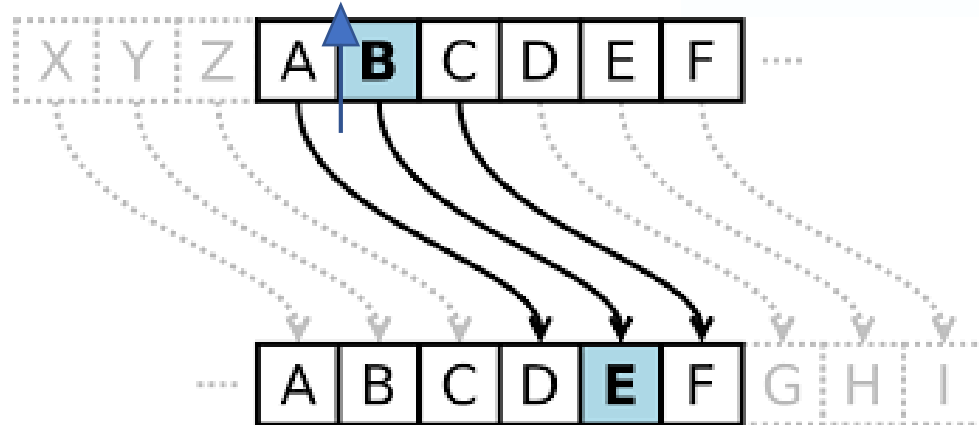
Cryptanalyse

Casser un système

Analyse fréquentielle

Alan Turing

@zeste de savoir



@wikipédia



Cryptologie

@CNIL

Confidentialité

Intégrité

Authentification

Non-répudiation



@kinsta

@medium

1 — Qu'est-ce que le binaire ?

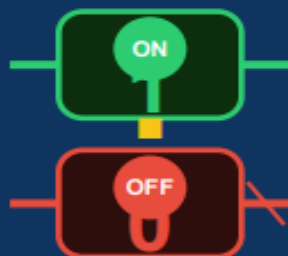
Les bases du fonctionnement d'un ordinateur

TRANSISTOR



Composant de base

COURANT



2 états possibles

BINAIRE vs DÉCIMAL

Décimal

10 chiffres (0→9)

0 1 2 3 4

5 6 7 8 9

Binaire

2 chiffres

0

1

VS

"bi" = deux
en latin

Système de numération

LE BIT

bit
binary digit

0

1

Plus petite unité d'info

ON PEUT REPRÉSENTER...

123 Nombres

ABC Lettres

IMG Images

Musique

N'importe quelle information

2 — Les 8 bits : l'octet

Bit	7	6	5	4	3	1	0
Valeur	128	64	32	16	8	2	1

0	0	1	0	1	0	1	0
---	---	---	---	---	---	---	---



32



8



2

$$32 + 8 + 2 = 42$$

3 — La table ASCII

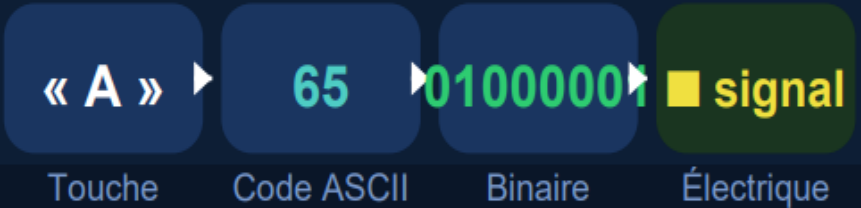
Caractère	Décimal	Binaire
A	65	0 1 0 0 0 0 0 1
a	97	0 1 1 0 0 0 0 1
espace	32	0 0 1 0 0 0 0 0
!	33	0 0 1 0 0 0 0 1



ASCII → 128 caractères

ASCII étendu

UTF-8 → 140 000+ caractères



Le jeu « Qui est-ce ? »

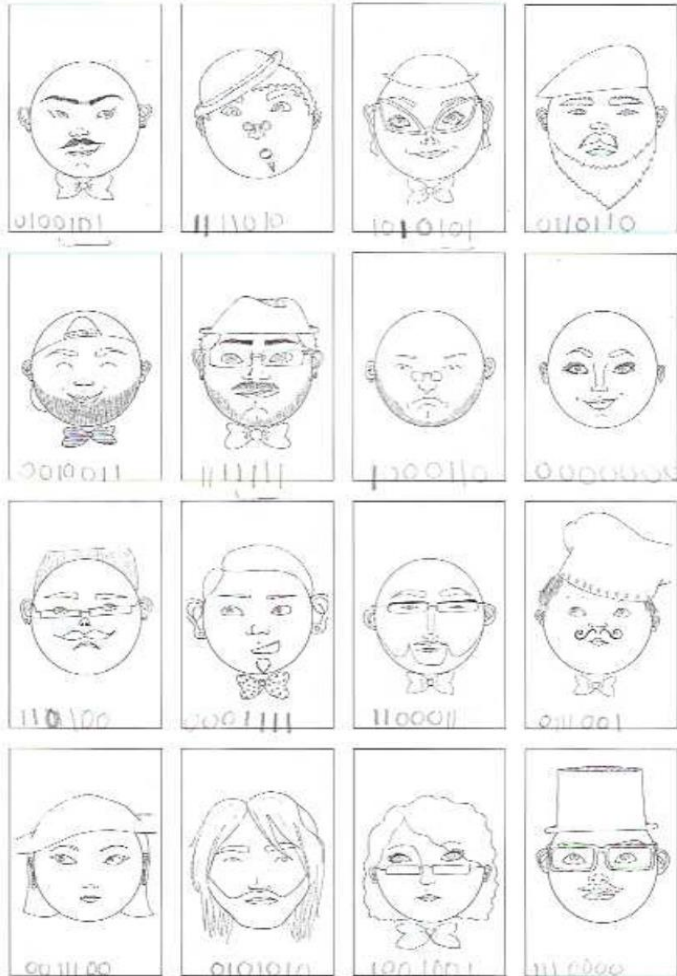
- Jouer en codant les personnages
- Tricher
- Corriger les erreurs

Qui est-ce ?



Jouer en codant les personnages

Voici tous les personnages du jeu :



16 personnages =
16 codes à
déterminer



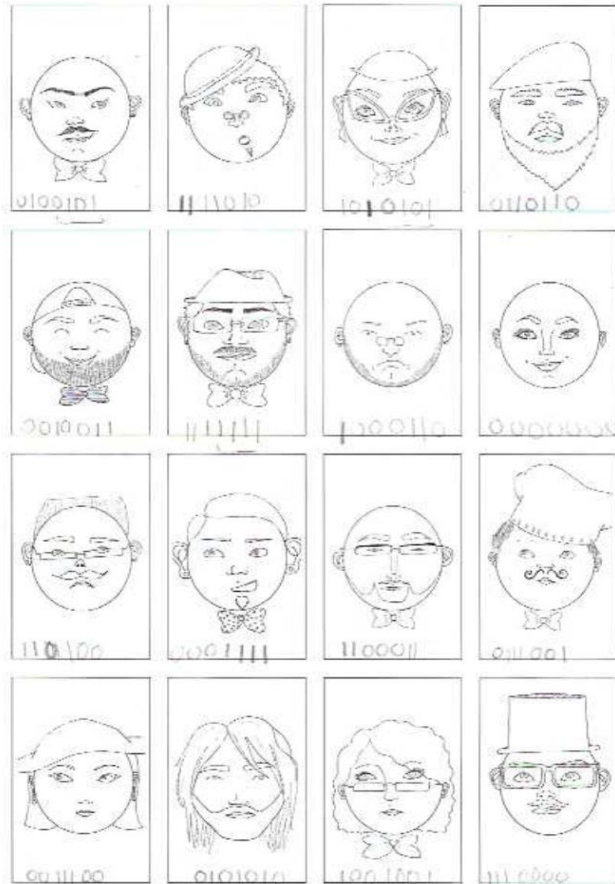
4 critères (2) + 3 critères de différenciation
(distance minimale) = 7 critères

lunettes : non ; moustache : oui ; chapeau : oui ;
cheveux : oui ; boucle d'oreille : non ;
barbe : non ; noeud papillon : oui

=> 0111001

Tricher

Voici tous les personnages du jeu :



Le joueur A triche :
1111111 => 0111111
1 seul mensonge

Le joueur B compare ce code avec les autres codes :
le code qui se rapproche le plus est 1111111
(6e personnage)
La triche passe *inaperçue*

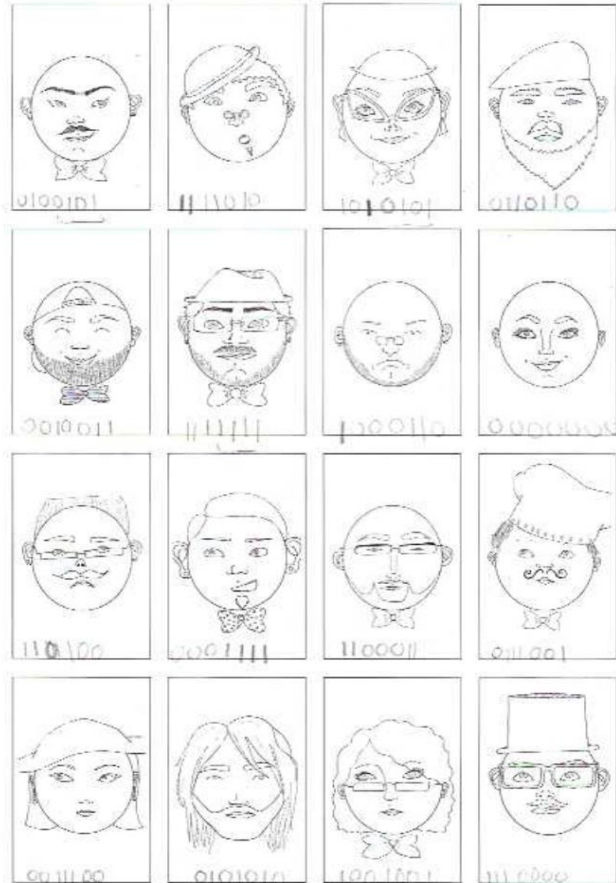
$$t=(d-1)/2$$

← $(3-1)/2$ soit $t^*=1$

*nombre max. de mensonges

Corriger les erreurs

Voici tous les personnages du jeu :



Code initial : 1111111

Code reçu : 0111111

$S1 = 0 + 1 + 1 + 1 = 3 \Rightarrow 1$

$S2 = 1 + 1 + 1 + 1 = 4 \Rightarrow 0$

$S3 = 1 + 1 + 1 + 1 = 4 \Rightarrow 0$

$(S3, S2, S1) = 001$ soit 1 en numération décimale :

$\Rightarrow$ le bit n°1 est erroné, on change le 0 en 1 et on obtient le code corrigé 1111111

Le Concours Al-Kindi

- Mathématicien arabe Al-Kindi.
- Concours de cryptographie.
- Élèves de quatrième, troisième et seconde.
- Trois tours suivis d'une finale.



Logo du concours (source : DRANE)



Portrait d'Al-Kindi
(source :Wikipédia)

Un Exemple d'Exercice

- Défi type premier tour du concours.
- « Chiffrement double ».
- Plusieurs niveaux de difficulté.

VERSION ☆ | VERSION ☆☆ | VERSION ☆☆☆ | VERSION ☆☆☆☆

VOTRE MISSION

Alice a chiffré le texte *SECRET*. Puis Bob a appliqué une deuxième opération.

Changez l'ordre des lettres dans la zone de déchiffrement pour retrouver le message d'origine.

ALICE

S	E	C	R	E	T
S	E	C	R	E	T
S	E	R	E	C	T

BOB

S	E	R	E	C	T
E	S	E	R	T	C

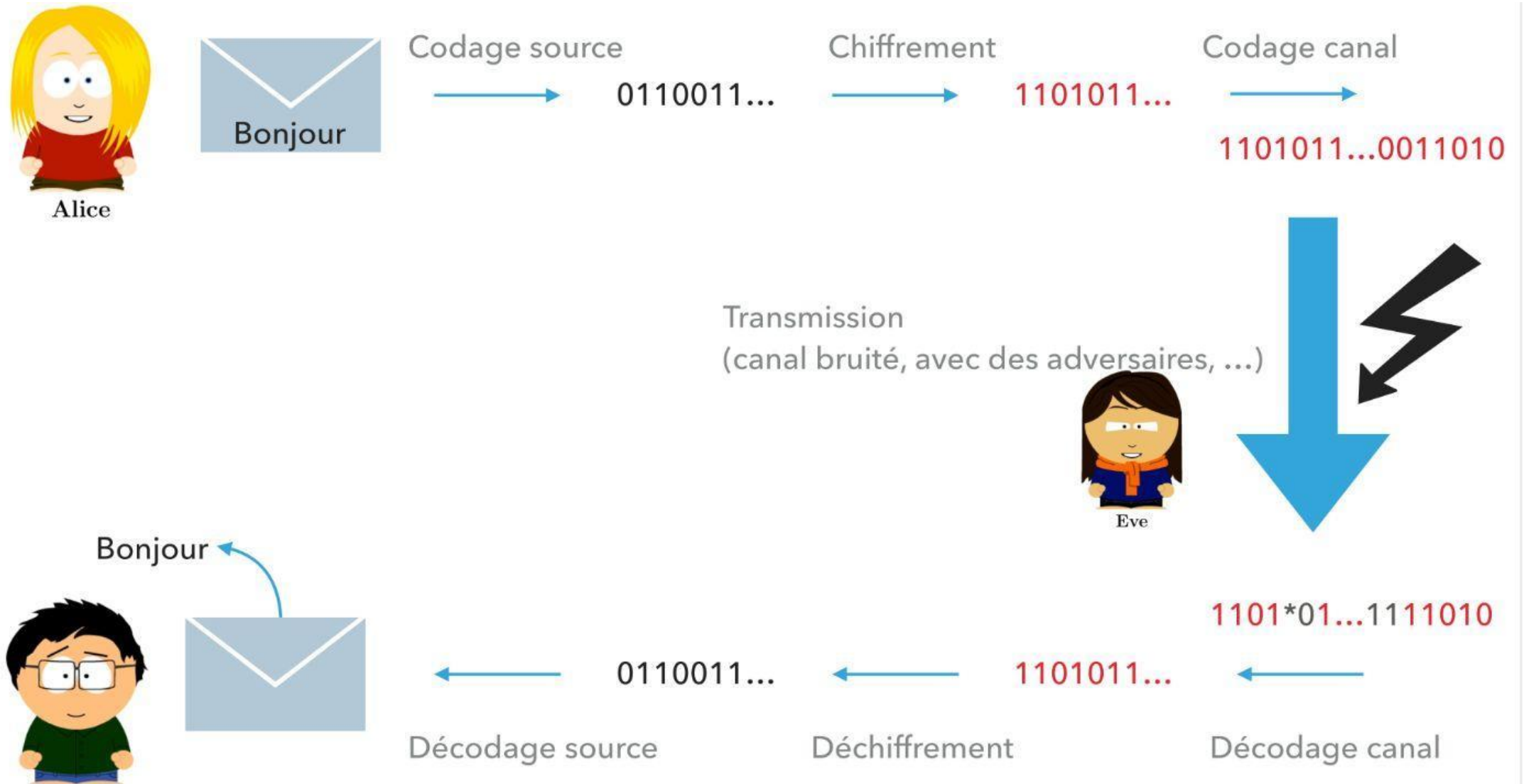
DÉCHIFFREMENT

E	S	E	R	T	C
E	S	E	R	T	C
E	S	E	R	T	C

Recommencer Valider

Exemple de défi (source : Concours Alkindi)

Le schéma de communication



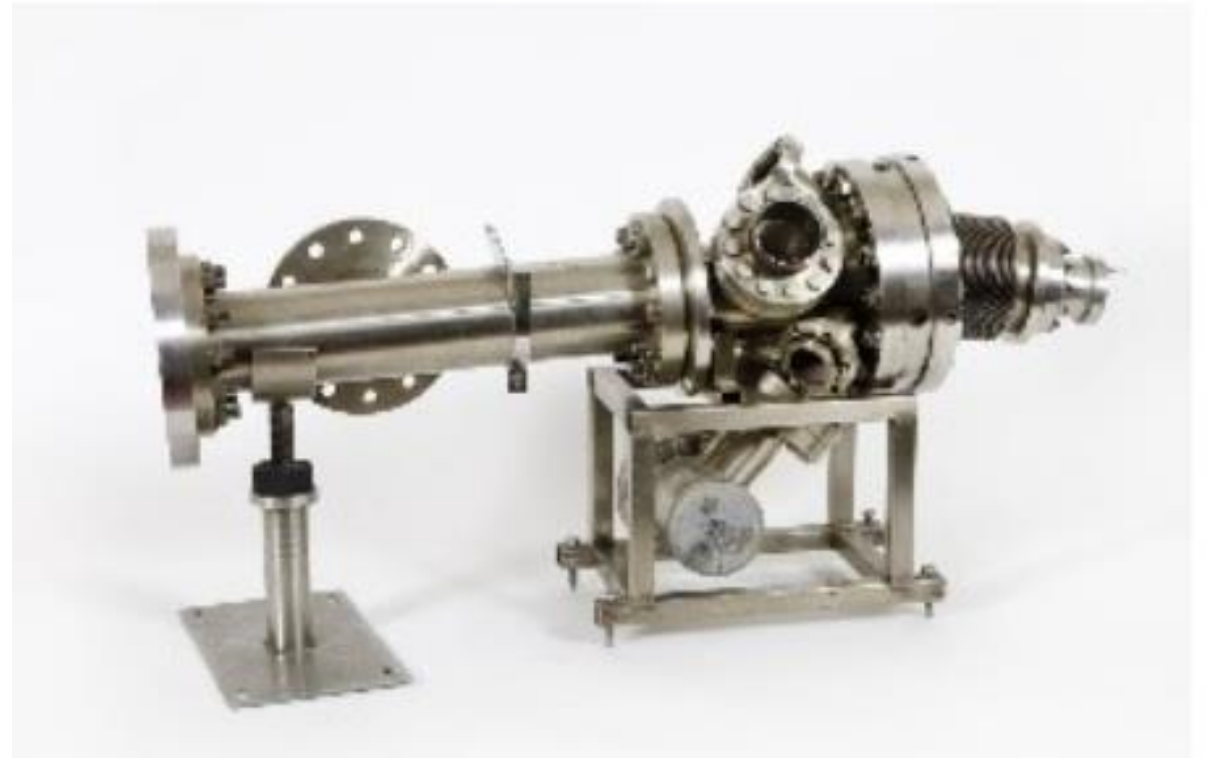
La visite de la réserve à l'université

La Sonde Atomique

Microscope ionique

analyse des matériaux métallique et
semi-conducteurs

spectrométrie a temps de vol



Le Plasmatron

Flammes de Plasma

Plusieurs milliers de Degrés Celsius

Tester différent matériaux



Le Pyromètre Ribaud

instrument optique

Gustave Ribaud



Le Chiffrement

Communiquer en toute sécurité — NSI 2^{nde}

Définition

Le chiffrement transforme un message lisible (texte clair) en texte illisible (texte chiffré) grâce à une clé secrète. Seul celui qui possède la clé peut déchiffrer.

Pourquoi chiffrer ?

Confidentialité

→ personne ne peut lire vos données

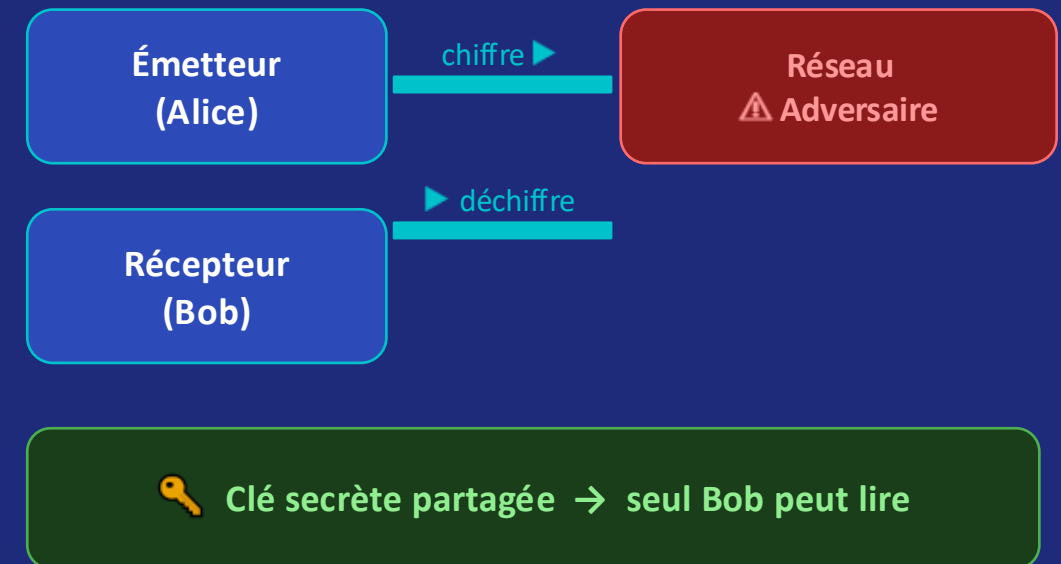
Intégrité

→ message non modifié

Authentification

→ vérifier l'identité de l'émetteur

Schéma de communication



Exemple : $clef = 5 \rightarrow "Bonjour" \rightarrow "Gpsnpvs"$

Chiffrement en Python

Fonctions chiffrer / déchiffrer — et attaque par force brute

```
def chiffrer(msg, clef, chiffre):  
    msg_chiffre = ""  
    for k in msg:  
        msg_chiffre += chr(  
            (ord(k) + clef) % 255  
        )  
        clef = pow(3, clef, 10000001)  
    return msg_chiffre
```

```
def déchiffrer(chiffre, clef):  
    msg = ""  
    for k in base64.b64decode(  
        chiffre.encode()).decode():  
        msg += chr(  
            (ord(k) - clef) % 255  
        )  
        clef = pow(3, clef, 10000001)  
    return msg
```

Comment ça marche ?

1. Chaque lettre est décalée selon la clé
2. La clé évolue à chaque caractère (pow)
3. Le résultat est encodé en Base64
4. Fichier sauvegardé : ex. 8_camille.txt

Attaque par force brute

Tester toutes les clés possibles :

```
clef_test = 10^(len_clef-1)  
while résultat illisible :  
    clef_test += 1
```

→ Plus la clé est longue, plus c'est difficile !

MERCI !