

Projet TransCrypt

Benkiewicz Daniel, Chitry Clémence, Pesquet Gabriel,
Poudade Alex-Pauline

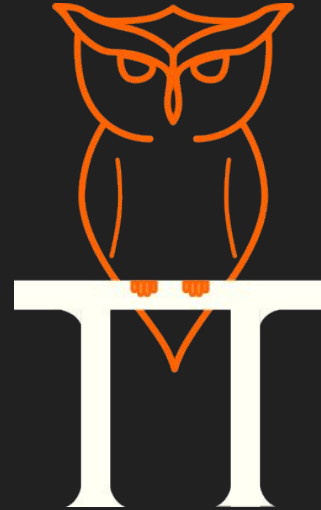
Sommaire

I- Notre méthode de chiffrement : TransCrypt

II - La messagerie TransOwl

- Frontend
- Démonstration
- Backend

III - Organisation de l'équipe

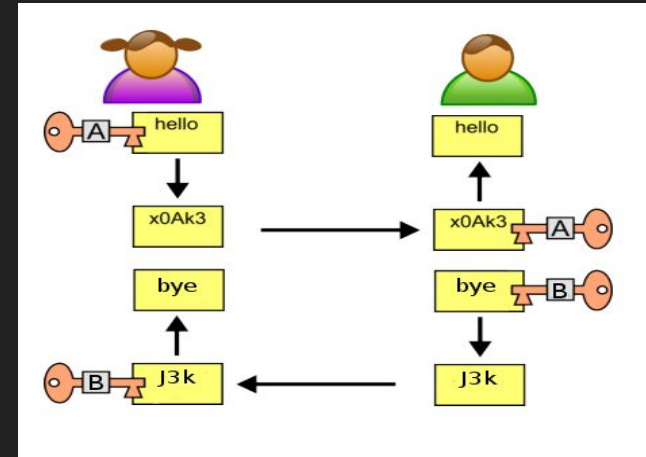


Notre méthode de chiffrement : TransCrypt

- 1 - Un peu d'histoire ...
- 2 - Faiblesses des systèmes actuels
- 3 - En quoi consiste TransCrypt (BBP) ?
- 4 - Pourquoi un n ième algorithme de chiffrement (atouts originaux) ?

Un peu d'histoire ...

- Sécuriser nos communications est nécessaire depuis des millénaires.
- Stéganographie (message caché)
- Cryptologie (message incompréhensible aux non-initiés).
- Algorithmes à clés publiques (ou asymétriques)
- Algorithmes à clés privées (ou symétriques).

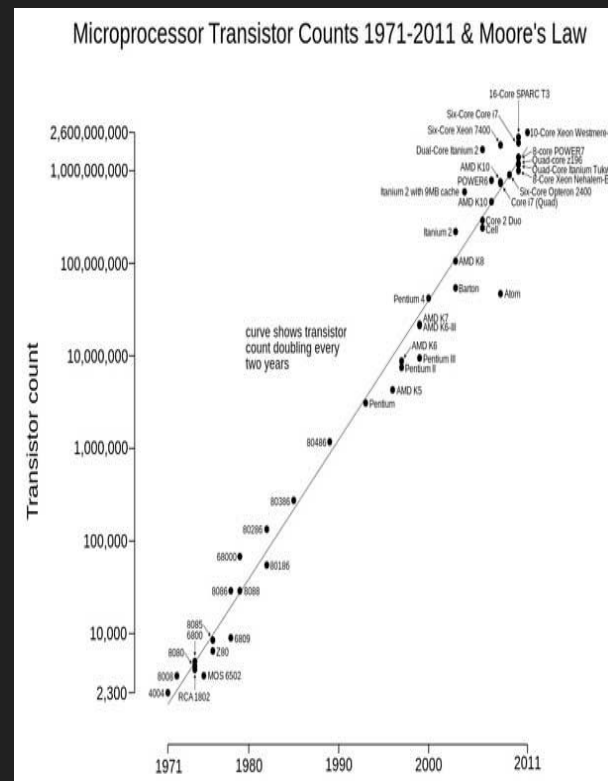


Faiblesses des systèmes actuels

Les systèmes actuels de cryptologie grand public sont :

- Empiriquement linéaires
- Prévisibles
- Soumis à la loi de Moore (microprocesseurs)

Ce qui est confidentiel aujourd'hui ne le sera plus demain !



Qu'est-ce que TransCrypt ?

- Mode de chiffrement original
- Fondé sur la non-périodicité des décimales de pi
- Fondé sur la formule BBP (i)

$$(i) \quad \pi = \sum_{k=0}^{\infty} \frac{1}{16^k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right)$$

Comment un message est-il chiffré ?

Pourquoi TransCrypt ?

Quels en sont les atouts ?

- Suite de nombres sans aucune répétition et à l'infini
- Échappe à la loi de Moore
- Solution grand public gratuite
- Se rapproche d'une force stochastique

```
3,141592653589793238462643383279502884197169399375105820974944592307816406286208996628034825342117067982148086
513282306647093846095508223172539408128481174502841027019385211055596462294895493018196482189796659344
4128475648237867631652721201891456485642346034861045426484213394607262429414127724587066603155891748815209
209462825403171536436788259014001133053084892044652128414695194511698433057270365795910539241611738192461
79318011854807446237996274967351895752724891279281880114912983671352403566430860213949435922473713070217
9860943702770539217176293176732384674818467669405132005681271452635608277857713427577896917367178721464409
0122495343014654958537105078227968925892542019561121290219608640344181580136297747713099405187072134999998
3729780499510587313281609618895024458553468083026423223082133446053526193118817101001317838752886575320
8381420472774681413035962349402475646873115954286388235797939315195778185778032171224604430019278746111399
09214202198938095272010654896327886593613318127846230301952035301852968995773622599413891249721775237476131
5155748572424541506958508295331168617278588807509638175467464939319255040400927701671139009488240128836160
35637076601047101819429555961989467678374848402553797742684710404753466208046842590484921233136770289891521
0478216205960040508151019351125398410135587602749467262914199272414098277967823547816360934172164219
52456315030216219245557067490380554958958926956902721079750930285321553448972027539625486065491398
18347975366369807426525278425518181175746728909777279380008164706001614524919217321721472320141419735685
4816136157352521334754184948843852323307304143454772416825189815694856209921922218427250524256867071
790494601534680498627227817860857843838276797681451400953837863610508806422512520511739298489608412848
8629456426194528502218661843067442786207319445847227137948095638437191237487746657573862183908550226
459958133947802759009465764078951269488388325970982052262052489407726719476268486201476909260136394337
45530506820349625451749399651431429808190659250977221694615157098583874105978595977297549993016175392486813
82868386894274455931855925453539543104997252478084598727364469584865383673622262609981246808512438843804512
44136549782789797156314359770012961608941948655584810635342207222848486461584562850616842738452267487
78989522138522549946667278238846596116314886330577454480359362456817432412252507406978410685908402522
88797108931456491368672287489405601501503308617926480920874760917824938589007149675965261365497818931297848
216829989487226580085754401427047755513279641451523746343646248584479526586782105114116473573952113427166
102135969536231442952484937187110145765404590279934037420073101785390621883874478984784896832144571368875194
350443021845310104848105370614680474912781711979995025419636267564484847451217318192199989301058198481646
7514249123074894907134644213961557945278095145502252163888193014203762178558648385778788339608792077346
7221825625996515014215630480384477345495206934465925201474428507125186600213243408819071048633173464965145
39057962685610050801666587969881637473684052571459102870641401109712062804303939759515671577040203378698360
07230587637635942187312814712053028281918261861258671215791984148486929164470609575270495722091756711672291098
4808158017306712748582228783529395395725121083578510868081944221006701303467118147113699485656143
983150190145116801714376716385159508804899868998287452831635007447918538883216048963132930388870
6420447525907915481416548589461637180270891994309244889575712828095923232609729971204443375265489382391193
2537446673058360414281388302038249037589854374417029132768618093773444030707469211201913020303081976211011
0544929321516084244859376698385228684781213525458213144951685726243344189303968462521www.DesktopBackground.org
```


Implémentation de TransCrypt

- Python
- JavaScript

Difficultés rencontrées :

- Prise en compte différente des entiers
- Approximations causées par des conversions



```
const max = Number.MAX_SAFE_INTEGER;  
// → 9_007_199_254_740_991  
max + 1;  
// → 9_007_199_254_740_992 ✓  
max + 2;  
// → 9_007_199_254_740_992 ✗  
BigInt(max) + 2n;  
// → 9_007_199_254_740_993n ✓
```

La messagerie TransOwl

1 - L'architecture de notre
messagerie

2 - La Frontend

a - Fonctionnalités générales
de communications

b - Une prise en main intuitive

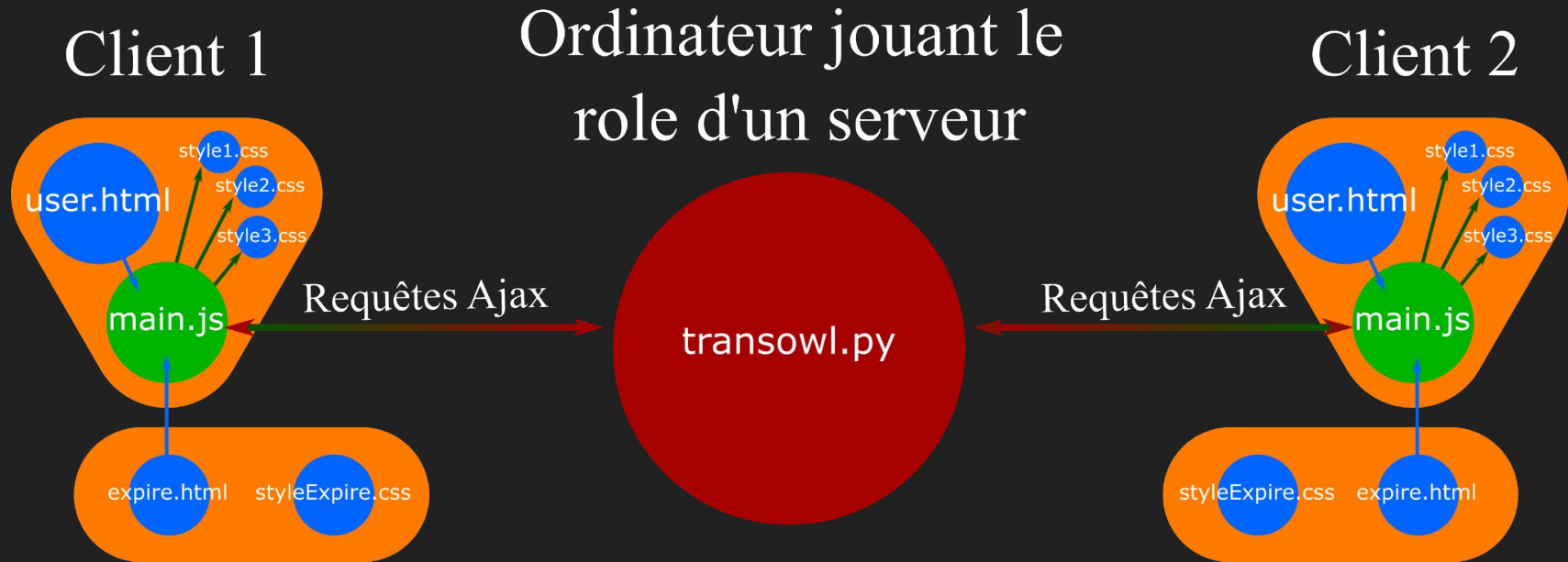
c - Responsive design

3 - DÉMONSTRATION

4 - La Backend



L'architecture de notre messagerie





La Frontend : Fonctionnalités générales de communications



La Frontend : Fonctionnalités générales de communications

Antoine75




TransCrypt 

Public

Privé

User_42657830

Votre ID était: 78945652

Id d'un utilisateur à c... 

User_78459625

Merci beaucoup, à bientôt

User_96542578

Quand veux-tu que nous nous ren...

User_42657830

Ce projet m'a l'air très bien...

Tu ne crois pas si bien dire mon ami, elle est surtout chiffrée de façon innovante et solide. Et en plus, elle ne conserve aucune donnée et elle a été créée par un groupe français.

Si tu veux rencontrer l'équipe qui l'a créée, rends toi sur le lien <https://www.orion-hub.fr/w/c7d2df35-5189-4620-9931-5da432640d2a>


Ça va très bien, merci

Quelle belle messagerie

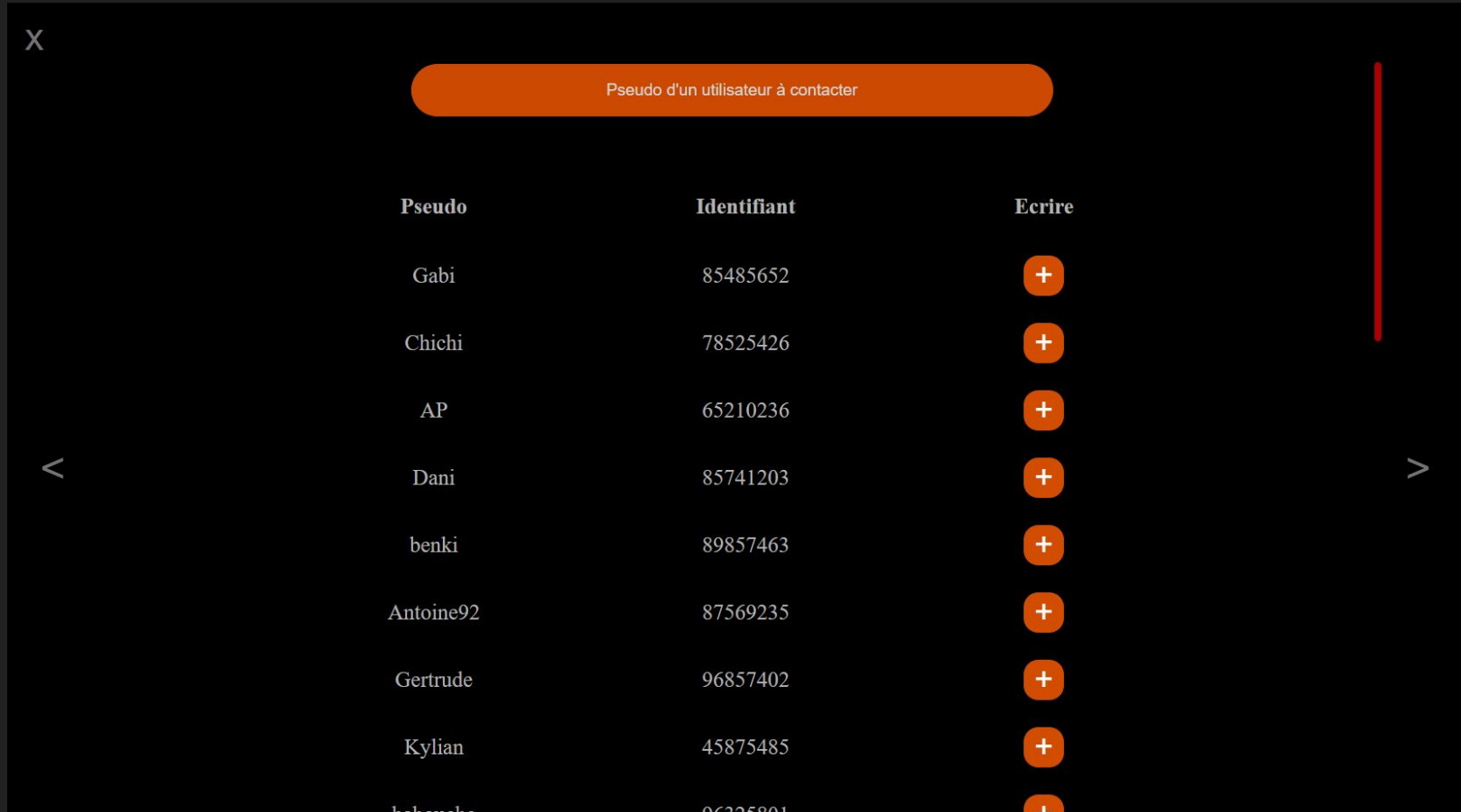
C'est super !

Ce projet m'a l'air très bien...

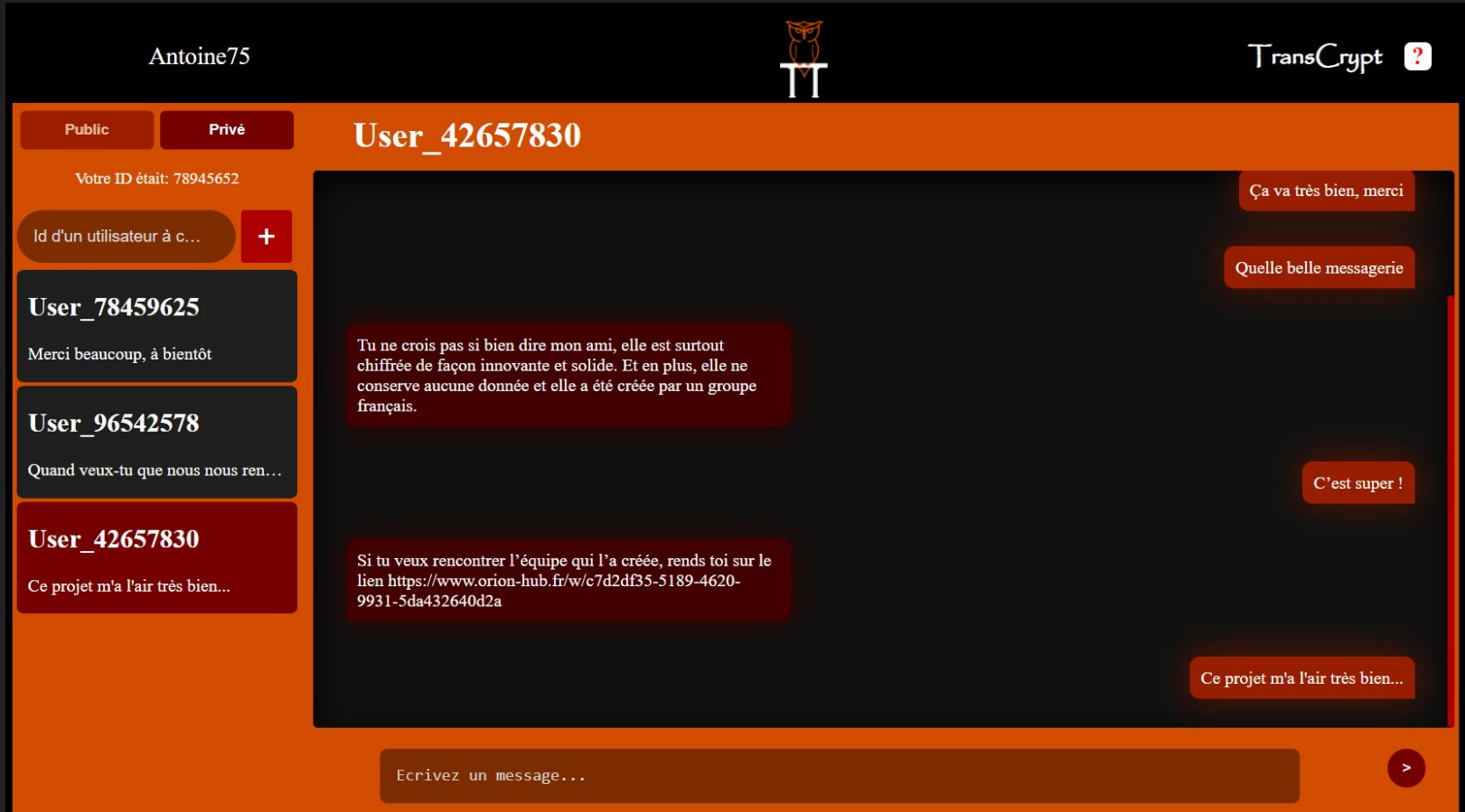
Ecrivez un message...




La Frontend : Fonctionnalités générales de communications



La Frontend : Une prise en main intuitive



Antoine75



TransCrypt 2

Public

Privé

Vous ID était: 78945652

Id d'un utilisateur à c... +

User_78459625

Merci beaucoup, à bientôt

User_96542578

Quand veux-tu que nous nous ren...

User_42657830

Ce projet m'a l'air très bien...

User_42657830

Ça va très bien, merci

User_42657830

Quelle belle messagerie

User_42657830

Tu ne crois pas si bien dire mon ami, elle est surtout chiffrée de façon innovante et solide. Et en plus, elle ne conserve aucune donnée et elle a été créée par un groupe français.

User_42657830

C'est super !

User_42657830


Si tu veux rencontrer l'équipe qui l'a créée, rends toi sur le lien <https://www.orion-hub.fr/w/c7d2df35-5189-4620-9931-5da432640d2a>

User_42657830

Ce projet m'a l'air très bien...

Ecrivez un message...

User_12345678



TransCrypt 2

Public

Privé

Vous ID était: 78945652

Id d'un utilisateur à c... +

User_78459625

Merci beaucoup, à bientôt

User_96542578

Quand veux-tu que nous nous ren...

User_42657830

Ce projet m'a l'air très bien...

User_42657830

Ça va très bien, merci

User_42657830

Quelle belle messagerie

User_42657830

Tu ne crois pas si bien dire mon ami, elle est surtout chiffrée de façon innovante et solide. Et en plus, elle ne conserve aucune donnée et elle a été créée par un groupe français.

User_42657830

C'est super !

User_42657830


Si tu veux rencontrer l'équipe qui l'a créée, rends toi sur le lien <https://www.orion-hub.fr/w/c7d2df35-5189-4620-9931-5da432640d2a>

User_42657830

Ce projet m'a l'air très bien...

Ecrivez un message...

Antoine75



TransCrypt 2

Public

Privé

Vous ID était: 78945652

Id d'un utilisateur à c... +

User_78459625

Merci beaucoup, à bientôt

User_96542578

Quand veux-tu que nous nous ren...

User_42657830

Ce projet m'a l'air très bien...

User_42657830

Ça va très bien, merci

User_42657830

Quelle belle messagerie

User_42657830

Tu ne crois pas si bien dire mon ami, elle est surtout chiffrée de façon innovante et solide. Et en plus, elle ne conserve aucune donnée et elle a été créée par un groupe français.

User_42657830

C'est super !

User_42657830


Si tu veux rencontrer l'équipe qui l'a créée, rends toi sur le lien <https://www.orion-hub.fr/w/c7d2df35-5189-4620-9931-5da432640d2a>

User_42657830

Ce projet m'a l'air très bien...

Ecrivez un message...

Antoine75



TransCrypt 2

Public

Privé

Vous ID était: 78945652

Id d'un utilisateur à c... +

User_78459625

Merci beaucoup, à bientôt

User_96542578

Quand veux-tu que nous nous ren...

User_42657830

Ce projet m'a l'air très bien...

User_42657830

Ça va très bien, merci

User_42657830

Quelle belle messagerie

User_42657830

Tu ne crois pas si bien dire mon ami, elle est surtout chiffrée de façon innovante et solide. Et en plus, elle ne conserve aucune donnée et elle a été créée par un groupe français.

User_42657830

C'est super !

User_42657830

Si tu veux rencontrer l'équipe qui l'a créée, rends toi sur le lien <https://www.orion-hub.fr/w/c7d2df35-5189-4620-9931-5da432640d2a>

User_42657830

Ce projet m'a l'air très bien...

Ecrivez un message...

Antoine75



TransCrypt ?

Public

Privé

User_42657830

Votre ID était: 78945652

Id d'un utilisateur à...



User_78459625

Merci beaucoup, à bientôt

User_96542578

Quand veux-tu que nous nous r...

User_42657830

Ce projet m'a l'air très bien...

Ça va très bien, merci

Quelle belle messagerie

Tu ne crois pas si bien dire mon ami, elle est surtout chiffrée de façon innovante et solide. Et en plus, elle ne conserve aucune donnée et elle a été créée par un groupe français.

C'est super !

Si tu veux rencontrer l'équipe qui l'a créée, rends toi sur le lien <https://www.orion-hub.fr/w/c7d2df35-5189-4620-9931-5da432640d2a>

Ce projet m'a l'air très bien...

Ecrivez un message...



TransCrypt

La Frontend

Responsive design

Antoine75

TransCrypt ?

Public

Privé

Votre ID était: 78945652

Id d'un utilisateur à contacter



User_78459625

Merci beaucoup, à bientôt

User_96542578

Quand veux-tu que nous nous rencontrions ?

User_42657830

Ce projet m'a l'air très bien...

User_85475698

Non merci

User_84562315874

Antoine75

TransCrypt ?



User_42657830

Ça va très bien, merci

Quelle belle messagerie

Tu ne crois pas si bien dire mon ami, elle est surtout chiffrée de façon innovante et solide. Et en plus, elle ne conserve aucune donnée et elle a été créée par un groupe français.

C'est super !

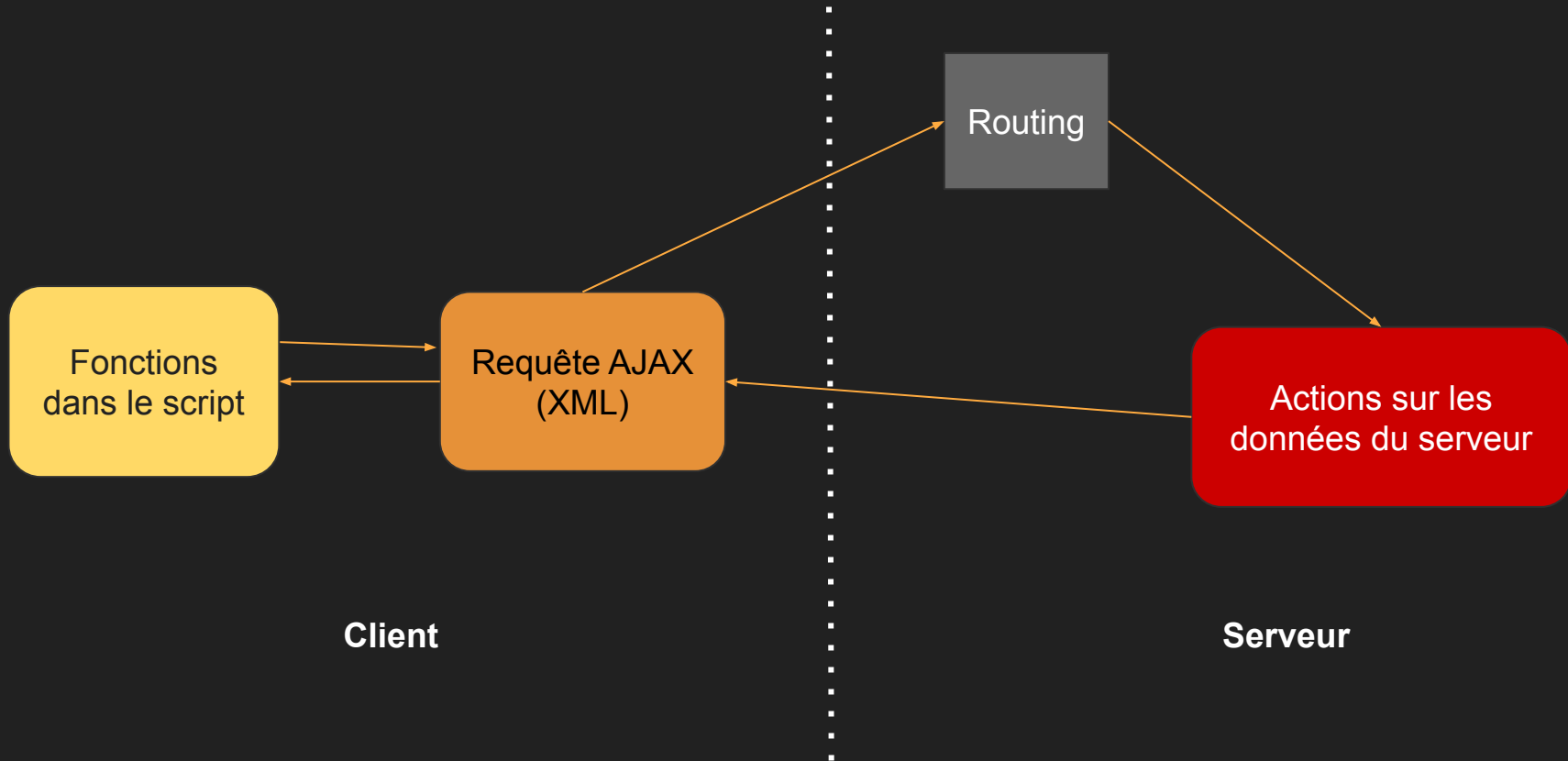
Si tu veux rencontrer l'équipe qui l'a créée, rends toi sur le lien

Ecrivez un message...



Démonstration

La backend : schéma échanges des données



La backend : Groupe, un exemple de POO

Paradigme Programmation Orientée Objet :

Avantages :

- Intuitive, lisible
- Fonctionnalités extensibles
- Application flexible

Inconvénients :

- Plus lente en python
- Traduction impossible en langage purement fonctionnel

TransOwl: Difficultés rencontrées

- Documentation incomplète de la bibliothèque flask en python
- Documentation non mise à jour de la bibliothèque jQuery en javascript
- Lenteur du chiffrement pour des clefs trop grandes
- Requêtes synchrones et asynchrones
- IdentError d'un ordi à l'autre
- Trouver une architecture admettant aisément des extensions
- Problème avec la configuration du pare-feu pour la machine hébergeant le serveur
- Traitement des codes d'erreur : couverture de tous les cas possibles d'erreur
- Bugs venant de la bibliothèque venv en python
- Adaptation du format de la page à diverse tailles d'écran
- Taille finale du code augmentant la difficulté de maintenance
- Adapter la taille de la barre de saisie au message entré

Versions de TransOwl (1)

V.03 : Envoyée aux Trophées NSI : envoi et réception de messages, responsive design.



Versions de TransOwl (2)

V.04 : Profils publics et privés, possibilité de se renommer;

V.05 : Version actuelle : Intégration de thèmes, envoi du pseudo d'un utilisateur à son correspondant, aide et informations diverses (FAQ);

V.06 : (en préparation)

- Chiffrement & envoi d'images, d'audios;
- Améliorer l'efficacité et la rapidité de TransOwl : l'implémenter dans d'autres langages;

Répartition des tâches

- Alex-Pauline : Algorithme TransCrypt + son implémentation en Python;
- Clémence : Coordination de l'équipe, implémentation de TransCrypt en JavaScript, présentation, documentation, FAQ;
- Daniel : Frontend, responsive design + interface graphique (dont les thèmes), logo et schéma de l'architecture de TransOwl;
- Gabriel : Backend + Ajax.

Commun : vidéo, débogage, brainstormings.

Conclusion

Merci de nous avoir écoutés !