



CryptPad

Editeur collaboratif en temps réel
Zero-Knowledge

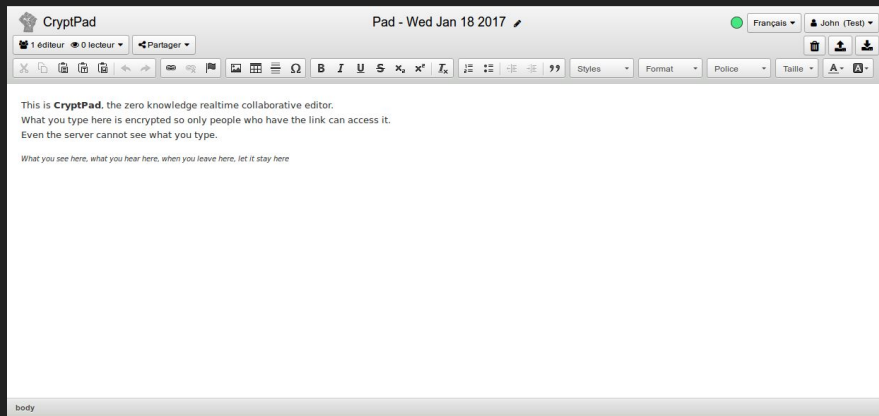
<https://cryptpad.fr/>
@pbondoer



Photo: **Paxson Woelber**
CC BY-SA 3.0

CryptPad

- Un outil collaboratif
- Un espace de stockage éthique
- Open-source, sous license libre



Un peu de contexte...

- L'internet d'aujourd'hui est devenu mobile
- Nous voulons nos données **n'importe-où** et **n'importe-quand**
 - ◆ Sur notre ordinateur
 - ◆ Sur nos téléphones
- Bienvenue sur *le cloud*

Le cloud

- Qu'est-ce-que c'est?
 - ◆ Le cloud est un **réseau d'ordinateurs** connectés entre eux, qui vont garder une copie des données à tout moment pour les rendre plus accessible et les servir à la demande.
- Le plus simple, c'est d'utiliser un gros fournisseur

Les fournisseurs de cloud

- Le fournisseur devient l'intermédiaire pour nos données
- Il faut lui faire confiance
- Les conditions d'utilisations sont un labyrinthe de termes légaux
 - ◆ À tel point que seulement 7% d'entre nous les lisent...
<https://theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems>
 - ◆ En général, elles donnent des droits d'utilisation aux fournisseurs
 - *Problème...*

Problème...

- Le fournisseur est, souvent, une entreprise
- Le but d'une entreprise est de **faire un profit**
 - ◆ Services: de l'espace disque contre de l'argent
 - ◆ Revente de données
 - ◆ Utilisation des données pour **mieux cibler les publicités**

Mais, mais... ils n'ont pas le droit de faire ça! 🤖

Bah... si



J'ai lu et j'accepte les conditions

Bah... si



Vous avez signé!

- Vous êtes devenu un produit
- Le modèle économique est de vendre les données au plus offrant
- Est-ce moral?
 - ◆ Je vous invite à formuler votre propre opinion là-dessus
- ...lucratif?
 - ◆ Très certainement ;)

Supposons que...

- Même quand ce n'est pas le cas, il reste un autre problème
- Si des pirates viennent à voler les données, elles sont en clair
 - ◆ <http://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Comment faire?

- Chiffrer ses données avant de les mettre en ligne
 - ◆ Efficace, mais **peu pratique**
 - ◆ Compliqué pour une personne quelconque
- Mettre en place son propre serveur
 - ◆ Encore une fois, requiert des **connaissances techniques** avancées
 - ◆ Demande un **investissement** de temps et d'argent conséquent
 - ◆ Peut potentiellement représenter un **risque de sécurité**
 - Mauvaise configuration, etc.

Comment faire?

- Utiliser un service chiffré
 - ◆ **Attention!** Certains services se disent « chiffrés » mais bien souvent ne le font qu'à *froid*, ou *en transit*
 - Si le fournisseur a les **clés de chiffrements**, ce n'est pas vraiment chiffré
 - ◆ Pour chiffrer dans le navigateur, le JavaScript est obligatoire
 - Encore une fois, il faut faire confiance au fournisseur

Bien choisir son service

- Le code est-il **open source**? Sous **license libre**?
- A-t-il eu des **failles de sécurité** dans le passé?
- Quelle est le niveau de **transparence** du fournisseur?
- Le code source est-il **audité** par un organisme indépendant?
- Le service est-il **payant**?

Zero Knowledge... quoi?

- En français: *aucune connaissance*
- Les données sont chiffrées *avant* d'être envoyées
- Le fournisseur ne connaît pas la clé de chiffrement
 - ◆ Il redevient un *simple intermédiaire*
- Seul les *destinataires* détiennent les clés

Zero Knowledge!

- CryptPad est un service Zero Knowledge
 - ◆ Votre **combinaison utilisateur / mot-de-passe** devient votre clé
- Complètement open-source
 - ◆ Nous acceptons les contributions sur GitHub!
- Un projet de recherche ambitieux
- Disponible en plusieurs langues!
 - ◆ Aidez-nous à traduire, venez me voir après la conférence ;)

Le lien

- La manière la plus simple de partager est un lien
- Voici à quoi ressemble un lien CryptPad:

```
https://cryptpad.fr/pad/#/1/edit  
/xnwMrJo81JAqppCpqqo9g1w  
/j+967yxA-SpQMrRBDm4SH3rk
```

Le lien

- La manière la plus simple de partager est un lien
- Voici à quoi ressemble un lien CryptPad:

```
https://cryptpad.fr/pad/#/1/edit  
/xnwMrJo81JAqppCpqqo9g1w  
/j+967yxA-SpQMrRBDm4SH3rk
```

Le lien

- La manière la plus simple de partager est un lien
- Voici à quoi ressemble un lien CryptPad:

```
https://cryptpad.fr/pad/#/1/edit  
/xnwMrJo81JAqppCpgo9g1w  
/j+967yxA-SpQMrRBDm4SH3rk
```

Le lien

- La manière la plus simple de partager est un lien
- Voici à quoi ressemble un lien CryptPad:

```
https://cryptpad.fr/pad/#/1/edit  
/xnwMrJo81JAqppCpqqo9g1w  
/j+967yxA-SpQMrRBDm4SH3rk
```

Le lien

- La manière la plus simple de partager est un lien
- Voici à quoi ressemble un lien CryptPad:

```
https://cryptpad.fr/pad/#/1/edit  
/xnwMrJo81JAqppCpqqo9g1w  
/j+967yxA-SpQMrRBDm4SH3rk
```

Les éditeurs

- Plusieurs façons sont possibles de créer du contenu:
 - ◆ Texte riche
 - ◆ Code source
 - ◆ Présentation
 - ◆ Sondage
 - ◆ Upload

CryptDrive

The screenshot displays the CryptPad web interface. At the top, the browser title is "CryptPad" and the address bar shows "CryptDrive - Firefox Developer Edition". The user's name "Pierre (pbondoer)" is visible in the top right corner. A storage indicator shows "28.5 / 50 MB" with an "Upgrade account" button. A search bar is located below the storage indicator. The interface is divided into a left sidebar and a main content area. The sidebar contains a "Documents" section with a tree view of folders: "42", "CryptPad" (containing "Releases"), "Freelance", "My stuff", "Slides" (containing "2017/05/02 - 42", "2017/05/20 - Ubuntu Party 17.04", and "2017/06/30 - Pas Sage En Seine 2017"), and "XWiki". Below "Documents" are "Templates" and "Trash" sections. The main content area, titled "Documents", shows a grid of document thumbnails. The first row contains six folder icons labeled "42", "CryptPad", "Freelance", "My stuff", "Slides", and "XWiki". The second row contains four document icons: "ALORS" (calendar icon), "Learning JavaScript - the ..." (code icon), "loading corgi" (document icon), and "Roadmap XWiki 9.6 + 9.7" (code icon).

Éditeur: texte riche

The screenshot shows the CryptPad web application interface. At the top, the browser title is "CryptPad" and the page title is "Bonsoir". The user is logged in as "Pierre (pbondoer)". The interface includes a toolbar with various editing tools such as bold, italic, underline, strikethrough, link, unlink, list, and indent. The main editing area contains the following text:

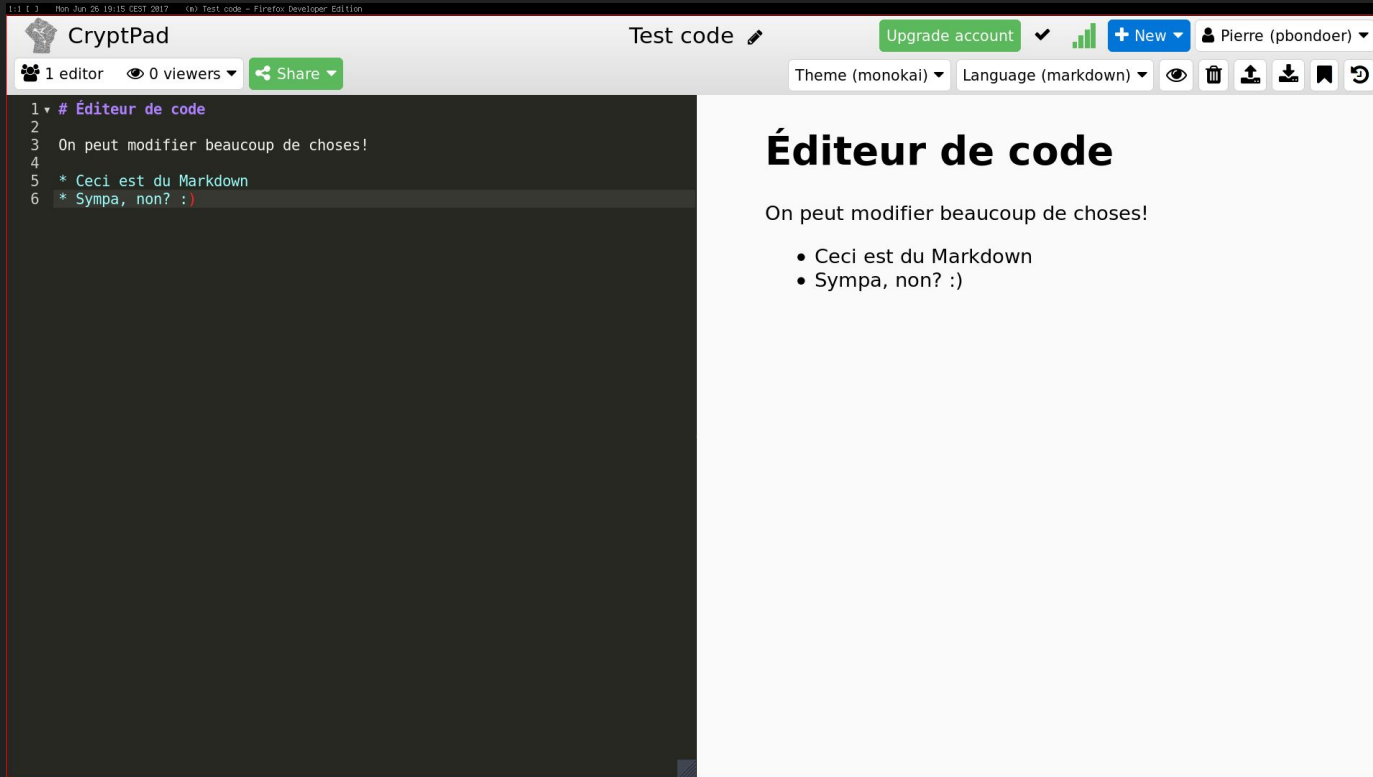
Bonjour, vous allez bien?

- J'aime faire des listes
- Je trouve que ça aide beaucoup

Ceci est un éditeur de texte... en temps réel!

body p

Éditeur: code source



The screenshot displays the CryptPad web interface. The top navigation bar includes the CryptPad logo, the title 'Test code', an 'Upgrade account' button, a '+ New' button, and a user profile for 'Pierre (pbondoer)'. Below the navigation bar, there are controls for '1 editor', '0 viewers', and a 'Share' button. The main editing area is split into two panels. The left panel, titled '1 editor', shows the source code in a dark theme with line numbers 1 through 6. The right panel shows the rendered output in a light theme.

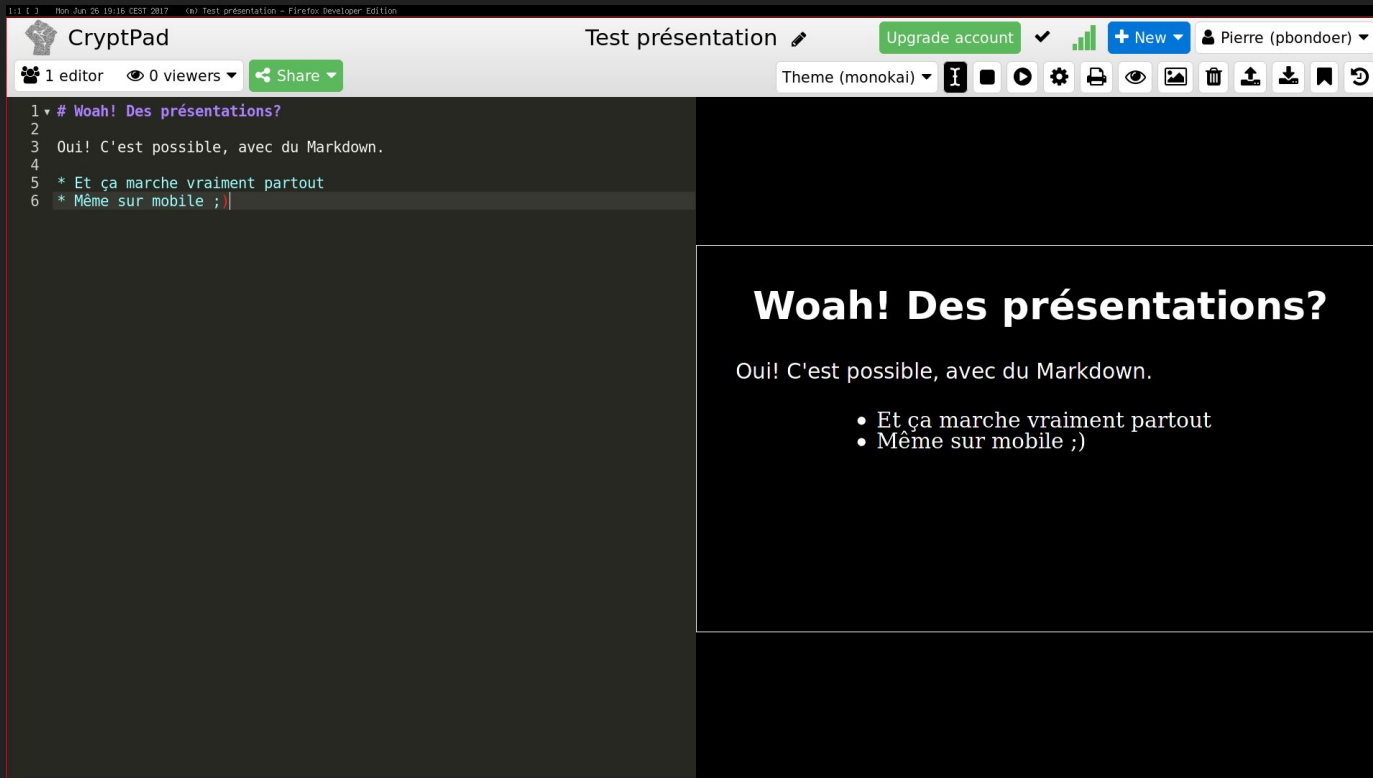
```
1 # Éditeur de code
2
3 On peut modifier beaucoup de choses!
4
5 * Ceci est du Markdown
6 * Sympa, non? ;)
```

Éditeur de code

On peut modifier beaucoup de choses!

- Ceci est du Markdown
- Sympa, non? ;)

Éditeur: présentations



The screenshot shows the CryptPad web editor interface. The top bar includes the CryptPad logo, the title "Test présentation", an "Upgrade account" button, a "+ New" button, and a user profile for "Pierre (pbondoer)". Below the top bar, there are controls for "1 editor" and "0 viewers", and a "Share" button. The main editor area on the left contains the following Markdown code:

```
1 # Woah! Des présentations?  
2  
3 Oui! C'est possible, avec du Markdown.  
4  
5 * Et ça marche vraiment partout  
6 * Même sur mobile ;)
```

The right side of the interface displays a rendered presentation slide with a black background and white text. The slide content is:

Woah! Des présentations?

Oui! C'est possible, avec du Markdown.

- Et ça marche vraiment partout
- Même sur mobile ;)

Éditeur: sondages

The screenshot shows the CryptPad interface for a poll titled "Test sondage". At the top, there is a navigation bar with the CryptPad logo, the poll title, an "Upgrade account" button, a "+ New" button, and the user name "Pierre (pbondoer)". Below this, there are buttons for "Admin" and "Show help". A large text box contains the message: "Ceci est un sondage. Vachement pratique pour s'organiser à plusieurs." Below the text box, there is a table of responses for three users: Pierre, John, and Marie. The table has four rows representing different food items: Pizza, Pasta, Salade, and Burger. Each cell in the table contains a colored background (yellow, green, or red) and a symbol (tilde, checkmark, or X).

	Pierre	John	Marie
Pizza	~	✓	~
Pasta	✓	✗	~
Salade	✓	~	~
Burger	✗	~	✓

Et après?

- Groupes de travail
 - Feuilles de calcul
 - Messagerie chiffrée
 - Le futur... et l'au-delà!
-
- N'hésitez pas à me faire part de vos suggestions <3

Merci!



<https://cryptpad.fr>

@pbondoer @cryptpad