CryptPad

Secure Online Collaboration

CryptPad

An *Experiment* in Secure* Online Collaboration

What is CryptPad?

- a suite of real-time collaborative editors
- employs clientside encryption
- server can't read your content

An Experiment...

- help you be more productive
- know as little as possible about you
- advance the state of the art

In other words...

- try new things
- focus on users' needs
- learn from mistakes
- improve the ecosystem

Security

- **PII** is a liability, not an asset
- *Zero-days* come out of nowhere
- defense-in-depth allows for graceful failure

Collaboration

- surveillance leads to **social cooling**
- *privacy vs freedom* is a false dichotomy
- people care more about *consent* than privacy

How does it work?

(*the technical part*)

Encrypted channels

- a **diff** algorithm calculates a **patch**
- **encrypt** the patch with a key shared via the URL **hash**
- communicate with a server via a **WebSocket**
- store all patches in an **append-only log**
- **forward patches** to clients in the *same channel*

Log-in

- **key derivation function**
- uses your *username and password*
- create your ***personal channel* and *secret key***
- store **encryption keys** and **channels** of your pads
- credentials are **never shared with the server**

In less technical terms

- **log in** to an *encrypted cloud*
- **documents are illegible** without the right secret keys
- **share links** to share access

What does it do?

Real-time editing

- **rich text**
- **code** (with highlighting)
- **presentations** (like this one)
- **polls** (scheduling dates)
- **illustration** (whiteboard)
- **file upload** and **embed**

Organization

- **CryptDrive** (folders, renaming)
- **tags** (not shared with other users)
- **search** (by title or tag)
- **thumbnails**

Social features

- **log in** for multi-device workflows
- **chat** with friends
- **profiles** to know who you're working with
- **read-only** links

Challenges

- browsers don't always agree
- inconsistent (or absent) API implementations
- data migrations and recovery are clientside
- we can't recover your password
- **we can't sell your data**

Open Source

Open Development

- Fully self-hostable
- **https://github.com/xwiki-labs/cryptpad**
- Freenode#cryptpad (Matrix or IRC)
- @cryptpad (twitter)
- research@xwiki.com *or* **sales@cryptpad.fr**

Free to try

https://cryptpad.fr