max cryptoblog alpha

- **Join**
- **Log In**
-
- max cryptoblog posts

- **Hello Guest**

About Max Cryptoblog

Features

Max Cryptoblog is a web application for blogging. Users may encrypt blog posts with a password. You can use a different password for each blog post. Max Cryptoblog was created using the Python Django web application framework.

Anyone can see any published blog posts on Max Cryptoblog. If a published blog post is encrypted, you can see the ciphertext. To create, encrypt and decrypt blog posts, you must sign in with a verified email address and password. Registrants will be sent a verification email.

Max Cryptoblog intends that your unpublished blog posts are private to you. Unless you share your unpublished blog posts (for example, via email), Max Cryptoblog allows only you to see your own unpublished blog posts. Otherwise, Max Cryptoblog allows only you to see, edit, encrypt or decrypt your own draft (unpublished) blog posts.

You can encrypt and decrypt your blog posts using a password. You can use a different password to encrypt and decrypt each blog post. You may opt to have Max Cryptoblog save the password, but this is not recommended.

Materials for blog post encryption might include, for example, "What Happened in Vegas", your Manifesto, or "What Really Happened During My 'Disassociative Fugure State'".

Additional features that might possible be added or enabled

- For users who, against our recommendation, recklessly opt to store blog post encryption passwords on the system, such passwords should at least be stored in encrypted form on our database.
- User One can allow authenticated User Two to read her encrypted posts User One you gives User Two the blog post password without User One having to let User Two log in as User One with User One's credentials.
- Users can email their encrypted posts using the Max Cryptoblog email facility.
- Users can can message other users.
- Allow unregistered recipients of encrypted emailed posts to decrypt encrypted posts using a password provided by the sender.
- Users can uploaded and encrypted documents and images, including documents in PDF format.
- Emailed posts can be in the form of email attachments.
- Emailing from the site should be subject to quantity limits. Limit the number of emails users can send from the app, with stricter limitations on non-paying users.

- Limit the length of emailed posts. Does anyone really need to email the entire text of Henry James' The Ambassadors?
- Add gratuitous features just for fun. For example, provide readability index measures for (unencrypted) blog post texts. Other possibilities: spelling and grammar checking. Automatic ipsum generation. Check for trigger words often found in badly-composed writing.

Cryptograpy

Max Cryptoblog uses symmetric ("secret key") authenticated cryptography, specifically the Fernet implementation in the Python Cryptography library. The Fernet implementation is said to guarantee that a message encrypted using Fernet cannot be manipulated or read without the key. The protection may be undermined, however it the user employs a weak encryption password.

The Fernet implementation is built on top of the following standard cryptographic primitives:

- AES in CBC mode with a 128-bit key for encryption; using PKCS7 padding.
- HMAC using SHA256 for authentication.
- Initialization vectors are generated using os.urandom().

Caution

This instance of Max Cryptoblog is in the early (alpha) development stage and is virtually untested. Max Cryptoblog is not ready for production usage. Use Max Cryptoblog for experimentation and entertainment only. At this time assurance of long-term maintenance of user accounts or content is impossible. The security and privacy of any information stored on the current version of Max Cryptoblog is uncertain. Account passwords are hashed, of course. Computer system administrators/developers and probably some hackers are capable of viewing your information. The system is designed such that (1) passwords that you use to encrypt your content are not stored on the system unless you choose, against our recommendation, to save such passwords; and (2) when you encrypt your content, the plaintext is discarded. The integrity of the system cannot be guaranteed, however. Your content is transmitted over the public Internet with the associated risk of interception. Your plaintext may be transmitted over the public Internet in unencrypted form (SSL/TLS may not be enabled). Employ additional layers of security as appropriate (example). Max Cryptoblog in its current state may be unsuitable for sensitive content. Trust no one. Enjoy!

Recommended web browsers

Where are the magical icons?

This website works best with Google Chrome or Mozilla Firefox. Internet Explorer? Not so much. Browsing at the office? Your organization may have enabled browser settings that degrade the user experience.

Max Cryptoblog is a Thing Made by John Kraus

- Contact