File Edit View History Bookmarks Tools Help

Max Cryptoblog

https://johnfkraus.pythonanywhere.com

Search

Most Visited | http://localhost:5000/ | file:///C:/dev/home/D... | Flask-RESTful — Flask-... | Getting Started | CACI apps | Google | http://api.usatoday.co...

MAX CRYPTOBLOG ALPHA

Read more on the About Page.

Join or Log In

localhost:5000

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Max Cryptoblog intends that your unpublished blog posts are private to you. Unless you share your unpublished blog posts (for example, via email), Max Cryptoblog allows only you to see your own unpublished blog posts. Otherwise, Max Cryptoblog allows only you to see, edit, encrypt or decrypt your own draft (unpublished) blog posts.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

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

Version 0.04 © 2015

Contact

What Happened in Vegas

author: John published: Nov. 13, 2015, 11:38 a.m.

Ciphertext:

gAAAAABWRhH2sw-0oAQnC-3msPuu6TJJZEq0egjhhtFNZpB9tyK2BWuOb-
OHVqcTUw9Xuoi7hsjrtzbTLJFpHS8EDQs0SkVTlQAcxT4f5HCv_YD0tCtCR6e2ehkQHZ9S0wLDxba5EslaD0xm2S-nPEjnwyZXCjhGUlHmk0kalz7yYKUt-
UNngWaXU95B33MlgMNsHXniCfVP46NzqbbJWjUJgttkbAlwjsA7Kt2zKc_Y1e8liN6yNGAFxHqRZm5bmrtqA1blMio7lHFnZ6ipOxl2pxMlEBxpXj3llZPMKxp5-
Uf02Dyh1nTlUWxc2-V8XJKx4n8lqcD17dkl5N8QgL5MWoqOqixcpZ6nOpAl-
l2y2fAJXxqrQzwwnzlFyqsFvWWo4LupDUZ_AZwDGm8SjVn0URcz90Ghtq18XCtAE3SVu9J9PXPEwMU4vqN0qdNa4Wwi4BPx5rZPXnc3pA3TdFikU9lxWr
HfFVxOGsUTcXl1ubETFVzjblxdorTj7WtSZxl6hygXUD9tQQ3M12R5OkvLOZ0hDRlN0GEGQ6il5nCG7VBbndDNXw1iLO3ArVJm7ViZd9nwBbH8kipQhGsw
4HON6qEswejN3NfVly6eaU4GXfiqSvtkNjyxN-
QlO0WMzqZWxkj6WYfxWyx2tQVYyiHlDzgfTc8s7xtKfHhO7Ea0ldT93nPBDaDSPL9mbbOgP0yn3Ym7kqEiL0XVJly7-
LD1MxYi1JNX06uWmphiQq9yPod1S9bZhb4gnPZQriBqavS4ySnDDBDD377K5ajVvrsT1SrEFDek-L9P7qSzRcSqdP6mB4dU7doLTsPYwbz31Ng-
uj0OxPc2s3m_VMOymMZ6irRlp2s_6_QY0ygB8wk7aNrc32jDcZQZJ-lJD_01t8e97Ul5W6n_S4uViMGJ9th3kZW1MMl8hUoZ3ixmfkuuhVBSpL-
xqnWlLEYg8qM6-pFVj2V9jFl9moSnhlKN1lrKyE-58lsXWjbJjHOUYPEkub0ztpucZKFlmCY4PURyWEUl-cwQnmMT6ndcPO7dFK46_xXCHL1ED1Wojoy7r-
vSw73gqdfASsHqL4Dhq0NwjlQmcyE6rZYVAPwmZ5HwsEOP91AkU9l0xbD_4LH9LJ9PtgNOghmwgAF835Z7mMzyFgheEnuWESwNSN6JSs8CoEJVUSw
Cxe2cB1rQqgiJU1l0-
sElY2oJcE29GLGjVq2J8kx9lMlUdcDBHg0SQzHdky25B5trNZDmFiT8JFlLZO4f0x7YvR9EguzbWFSsyS8jlyNHH5iRs7nfy_luEonCY780D6dskJbc7epYqMt
Lo9ikoKmclyvySPXr0qZD46pV8ATy8ORK-e2dDK4DqPGJKm3cknF2F8pdc5h5-Fy4R7NxgRYLJcRj0Gfceoze2Hteg38FlvdSrzPBX-
pxbYnm03OoHspn5XTVnlQ6_cw9XVhohyYw6TKxFoi6wSaMpOkM4-
_xB1l0CwhBTy9LSY4ZRoUUpTl_pzhJ2Kd0U8NzKdee489fatZ3_SV8sKBfg5sDr3O2rZBT-BEpar8udt88CJ5PDMwdYDfl4MRD-
dALlnf5DWqykXoDPNZ0l2-
rtlyhTZygBmH1LBCgUldRmPAHLMbOlYb6lRjkmbECz9q3gDBLuJsjx0_1JTNVl6MQJz9QBm3Qv1lsGA3jc_5gTJdhQHteEPcCCuky4lVpG7n6V0z8lLxMcq
LKlWdDo2q3LlM8i5fqOC4hTFCVgrj_dRi5CFD7a7aRidD3UfuPo-
4Q7MQOc9otrCbVa1SGnfUCG3ZcUMy4VLLPO7LlGAL3V69SztSw1Tvq1p0TwGL_dfhudqepgFqro9l7twOnU9TBZW9PE_69TP6n7qQO1svSloZSG97O
Ggsv8V-hLeVA2eNFNxGu6ZDuhbGWi6hitPC_8_bV-lnLRH5g8A_pw25HjrRV1D74hdpzirMcaaf15gyryhJ08gYuYwm62lk5F9WbD-nOMyJ3eXY_Y8R_c-
0Zj7HLQr7cw10FzL247MojTwBhFY6wYHhkVW16msdgjJVWMTvhHBEQnZESCT8W2dX8dEX2B5GrGLdqY1l8K4bYiygUhvB3NUlvTdJy1zdahEo2PsTclk
YmEFDgnJOLmbmxmBvjU4GW-
wUO9QkdvtXc6VRlw7nrF5cks0Vl0NC_AE4Y_aYhabCEszbZoGBZ1jOYkOntbw5kkm58WLbR2v0e70x6-9wG3mlg1V1y9dF7rmwweywthdhgSLed_uhRK
F6Rqo-
_rYOzG1w3hB0nEaqK3FPcMsUeF778pETHmdPEfSgqepez4M9Pr9fgD0CRdWxiyM3Wn6ucUfDCOPu47K42GDgcAMrvzewzG_E8uYb87rgLSWgOqVS
klnn7fVMRK0cBCefJp1WSDnD6gWlwf_VeUDDvonqru88AwM0htrsAEe7TuyamV6yftilDHxMFyOjuxYFEpkRFhv0wdW0LZg==

Add comment

comment author: John

Nov. 13, 2015, 11:43 a.m.

Unbelievable!!

File Edit View History Bookmarks Tools Help

Max Cryptoblog

https://johnfkraus.pythonanywhere.com/member/action

Search

Most Visited http://localhost:5000/ file:///C:/dev/home/D... Flask-RESTful — Flask-... Getting Started CACI apps Google http://api.usatoday.co...

MAX CRYPTOBLOG ALPHA

Join Log In Hello Guest

Published Posts (3)

From Cupcake Ipsum (http://www.cupcakeipsum.com)

author: John published: Nov. 19, 2015, 10 a.m.

Ciphertext (truncated) :

gAAAAABWTgmCUtu0XedgCwaC2-us1AivrK0kmnyGs8xNtwc7aSXToYlnm5AGa1b9mZtU_bDdX_FaCB7V8-
jZzNpuGie8EfbijHpIjeP2JSyZtCXkMrA2wr_7RFSB6rPokmL8wj_xjqqHP7epkL79Jhub-
p4bHaBmHFzuYyjlDkROz1mZnQFXXjY05B4xTy7vN77bsjcwhlVq0iSLeu2wB7VqSpaXWfHfH3BmOlYRDXCRpBpQGsm0HeCDN7OT_Xhm4GulJtfQRk29
JdViGlm8uCN7yRNc9gN5zNilUFfF6nz4qKBokKqvxupa3ulqqqAN6zgpTz_0l4ipoxPjLB90ZDc1N0...

Comments: 0

The Ambassadors by Henry James

author: John published: Nov. 13, 2015, 11:42 a.m.

Plaintext (truncated) :

New York Edition (1909). Volume I Preface Nothing is more easy than to state the subject of "The Ambassadors," which first appeared in twelve numbers of _The North American Review_ (1903) and was published as a whole the same year. The situation involved is gathered up betimes, that is in the second chapter of Book Fifth, for the re...

Comments: 0

What Happened in Vegas

author: John published: Nov. 13, 2015, 11:38 a.m.

Ciphertext (truncated) :

gAAAAABWRhH2sw-0oAQnC-3msPuu6TJJZEq0egjhhtFNZpB9tyK2BWuOb-
OHVqcTUw9Xuoi7hsjrtzbTLJFpHS8EDQs0SkVTIQAcxT4f5HCv_YD0tCtCR6e2ehkQHZ9S0wLDxba5EsIaD0xm2S-nPEjnwyZXCjhGUlHmk0kalz7yYKUt-
UNngWaXU95B33MlgMNsHXniCfVP46NzqbbJWjUJgttkbAlwjsA7Kt2zKc_Y1e8liN6yNGAFxHqRZm5bmrtqA1blMio7lHFnZ6ipOxl2pxMlEBxpXj3llZPMKxp5-
Uf02Dyh1nTlUWxc2-V8XJKx4n8lqcD17dkl5N8QgL5MWoq...

Comments: 1

Version 0.04 © 2015

Contact

File Edit View History Bookmarks Tools Help

Max Cryptoblog

https://johnfkraus.pythonanywhere.com/accounts/password/reset/

Search

Most Visited http://localhost:5000/ file:///C:/dev/home/D... Flask-RESTful — Flask-... Getting Started CACI apps Google http://api.usatoday.co...

Password Reset

Forgotten your password? Enter your e-mail address below, and we'll send you an e-mail allowing you to reset it.

E-mail

johnkraus3@gmail.com

Reset My Password

Please contact us if you have any trouble resetting your password.