



Technical Challenges in Implementing Cryptography for Accessible Mediums

Nadim Kobeissi

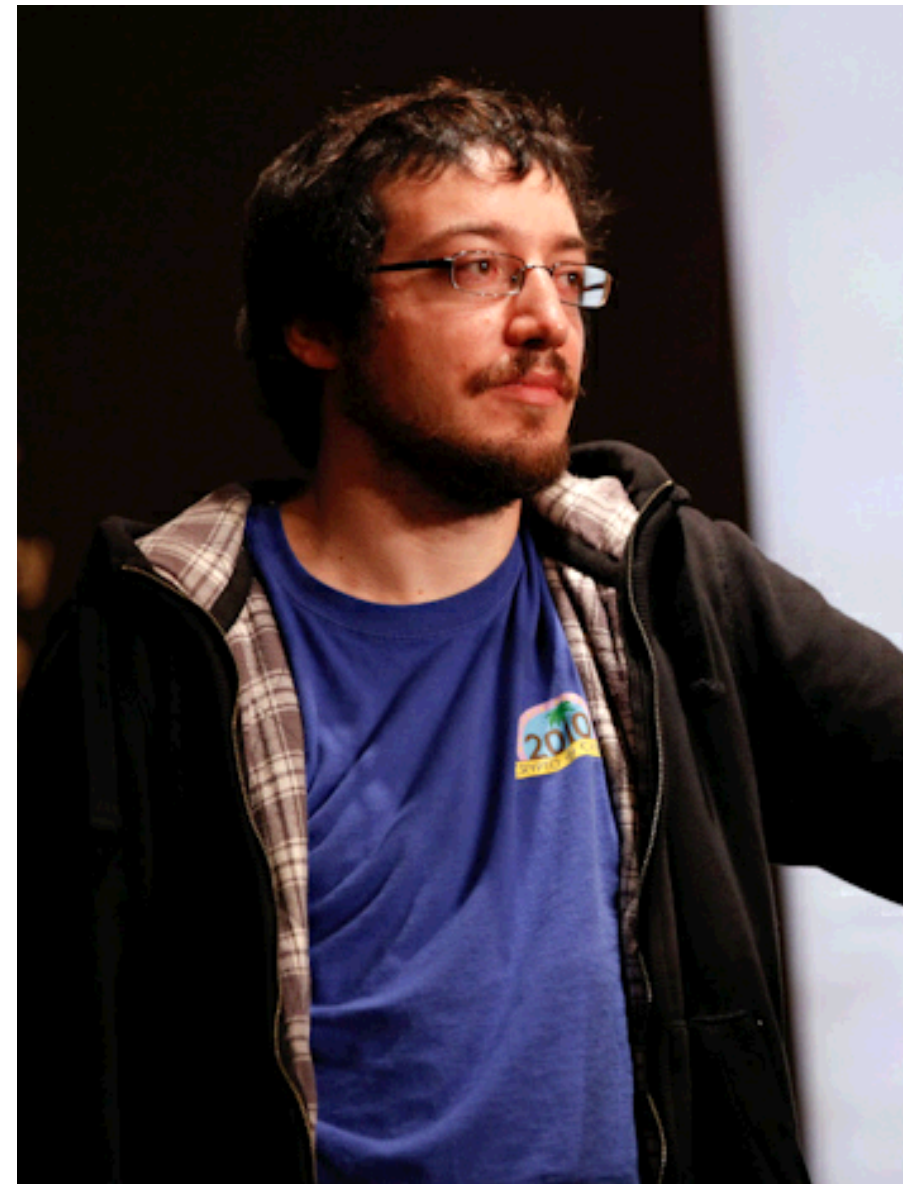
Application Security Forum 2013 – Yverdon, Switzerland



Thanks, J.P.!

Aumasson? More like
AWESOMEASSON.

...also Mr. Sylvain Maret
and other AppSec
organizers :3





Encryption tools

We can be optimistic about:

- Research.
- Availability.
- Variety.

```
mein-key - WordPad
Datei Bearbeiten Ansicht Einfügen Format ?

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.3-cvs (MingW32)

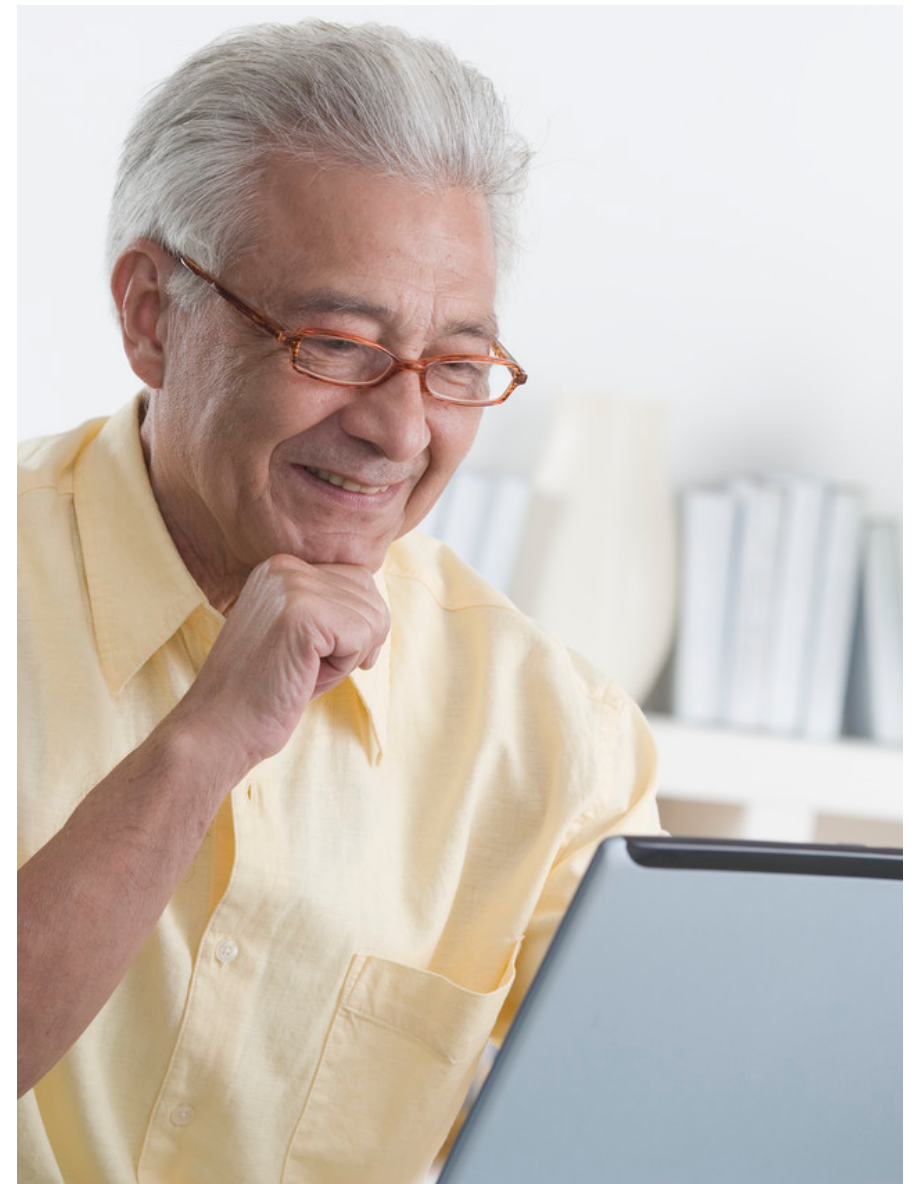
mQGIBEPe01ARBADP1bT8KfDjMjuOdLQrggk04zZb44sSEv
UnvQSnqP2L4bzHjPsIV1WiWY1gers5vzPUkvCOB6SOx6QW
KgcsAbMIwkAyVJbbxYPq/MbXavtANqbKZQ7MuFxn2WEZM3
w8czwZLTi1LKrvNTIF9Lg5kEAI+nzPfkUg7YUDXCabJAIn
rDWqF2jDiaHZ102bGW1M5bmnyhApjIfssFdnrcq4X/HqOR
3+oeny2xpiWSRarEP29OmXVLVqsSX+MAavaVBgfXJ4mgT
Sd/SBACRrxGsCUAJ29x4y/mZFicEenBeju2R9TINNQ1w33
D78kHwDuuJqKJh8+e4bUddEKdNVU00mkZaHA/SfJmI9oku
g6iLAfc2mAbRovV3dy4c1KZkGOK7h7GMJRLnaIsHasogGE
SGVpbmUgPGhlaW5yaWNoaEBkdWVzc2VsZG9yZi5kZT6IYA
IwYLCQgHAwIEFQIIAwQWAgMBAh4BAheAAAJECqKerJJXJ
QNe6vZmt4SGNPYkuAJ4ik20hE2iUr8wf53fycE+MbIkubb
8s1FOi7GfRAo4lJLuZttgl5cffKbNCBnXQJXREwnlhFtYb
5USzzcZRR3i3Ieikn2OXNdUsIFKg2Ywj21/2Cecq23MnOe
vyFujFVQNn1Y4JFGRgOarWVWOf7aSfR7rK+iTw8AAwUEAI
mnSGPgka/L6yWwrMn3l5SA8U+FqBohkgIzN8BCguqgcysE
8jzOR6QY7OXV5R/GcPE+O6UORLRzJBadoyEmD/G29VhHyg
+bJPMgtB+JnmX2apIYbGFAQDiEkEGBECAAkFAkPEO3ICGw
pACfUyuODaNmaLsOROGGCUE1mV+e8hAAmgK+xvYjsezXzJ
=J4dH
-----END PGP PUBLIC KEY BLOCK-----

Drücken Sie F1, um die Hilfe aufzurufen.
```




But what about...


- Accessibility?
- Usability?





Cryptocat's goal

Web chat client that's just
as **fun, easy, accessible** as
Facebook chat. 

But with **strong, reliable,**
useful, open source
encryption. 



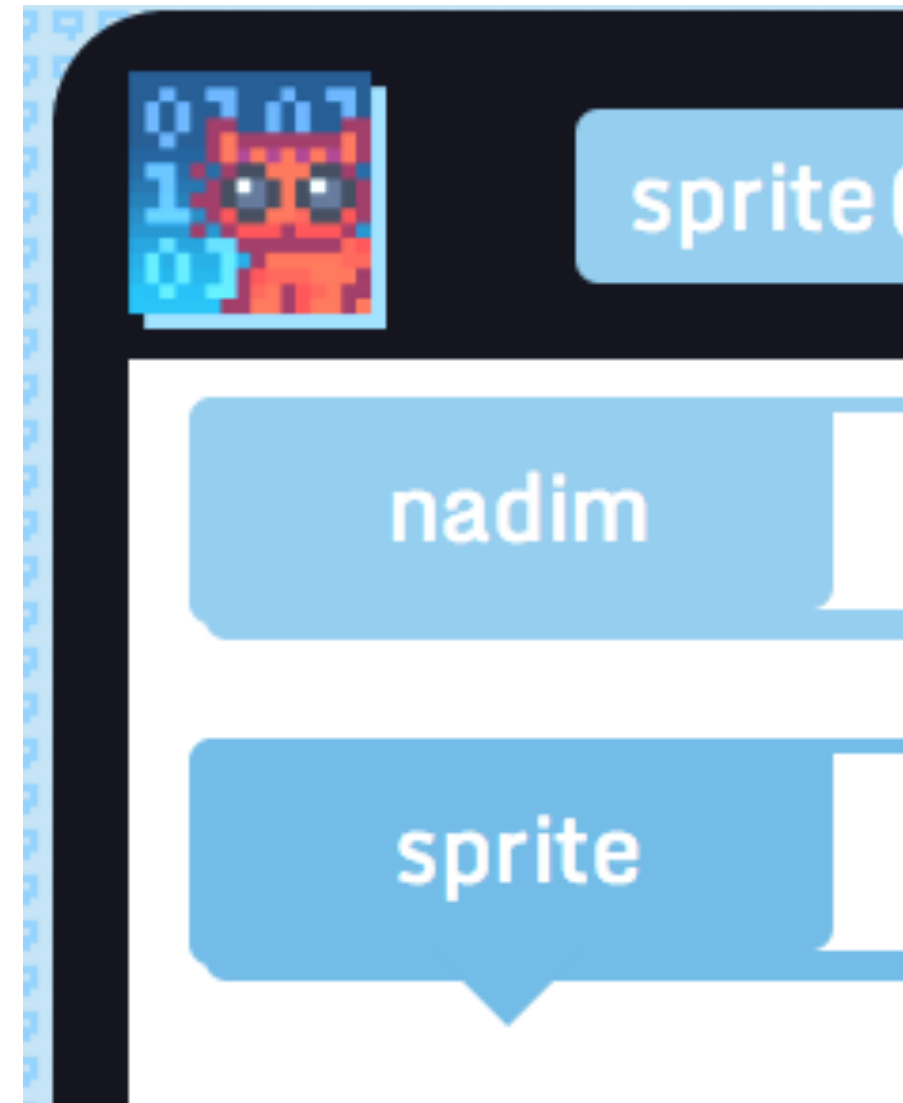


How does it work?

Download a browser app...

...install it and join a chat!

And that's it.



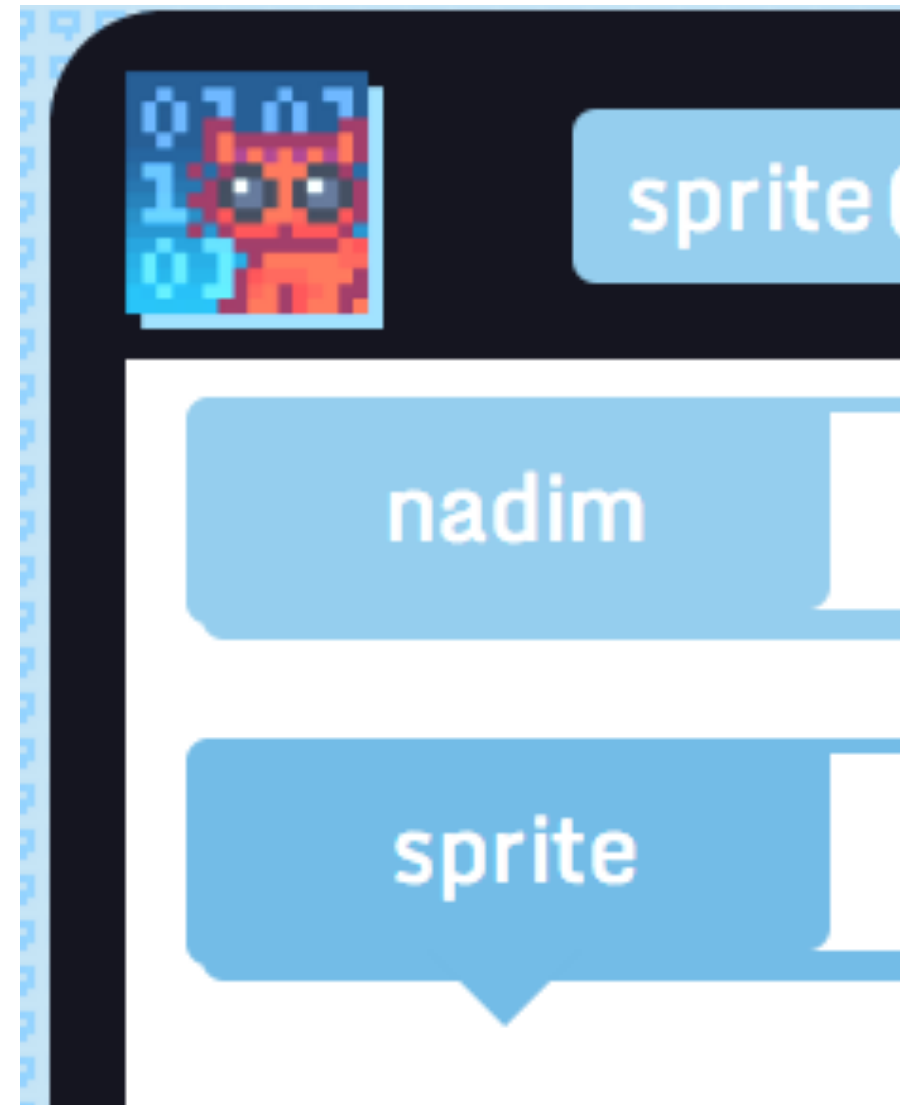


Usability matters

A colorful, familiar,
appealing interface...

...accessibility features,
audio and visual
notifications...

..and more.





Challenges in making crypto accessible

- Code delivery,
- PRNG,
- Implementation,
- ...and more.





General browser issues (not Cryptocat-specific)

- PRNG (now fixed.)
- Code delivery (now fixed.)
- Shaky sandboxing
(probably good in Chrome.)
- Bigger attack surface.
- More research needed.





Code delivery (2011)

- Reported by: the entire Internet (probably Jacob Appelbaum deserves more credit.)
- Cryptocat was a website, not a browser extension.
- Code was sent from scratch for every use.
- MITM, malicious server potential.

 **CRYPTOCAT**

In order to maximize conversation privacy for users, Cryptocat uses a browser-plugin only model. To access Cryptocat conversations, download the Cryptocat for Google Chrome. It's easy and takes

New to Cryptocat? Check out this



Cryptocat lets you instantly set up private conversations with an open source encrypted alternative to other services.



Messages are encrypted inside your own browser using AES-256 and are wiped after one hour of inactivity.



Cryptocat also runs as a [Tor](http://xdtfje3c46) hidden service (<http://xdtfje3c46>) for your iPhone, Android and BlackBerry.

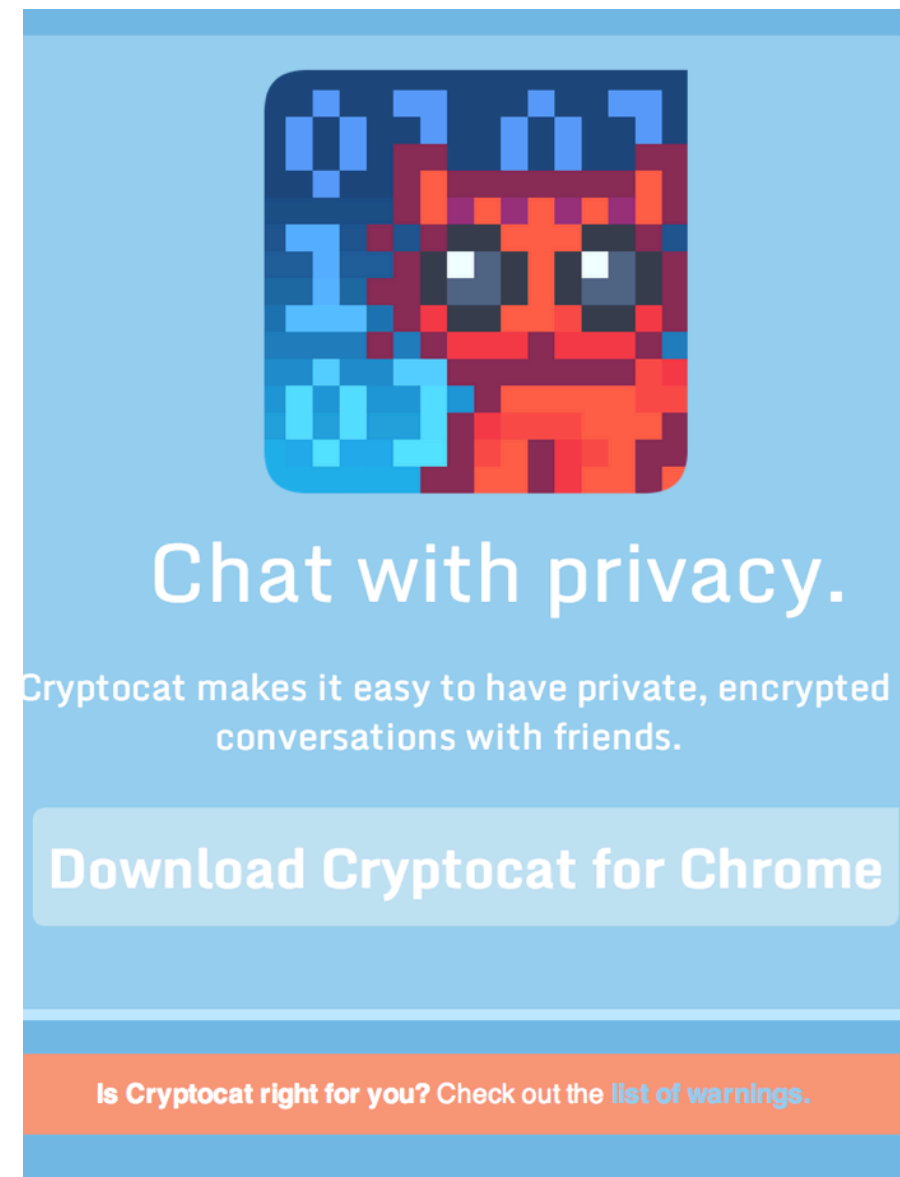
ca de eu fr it pt ru sv uk



Code delivery (2011)

- Cryptocat now signed browser extension only (since August 2012.)

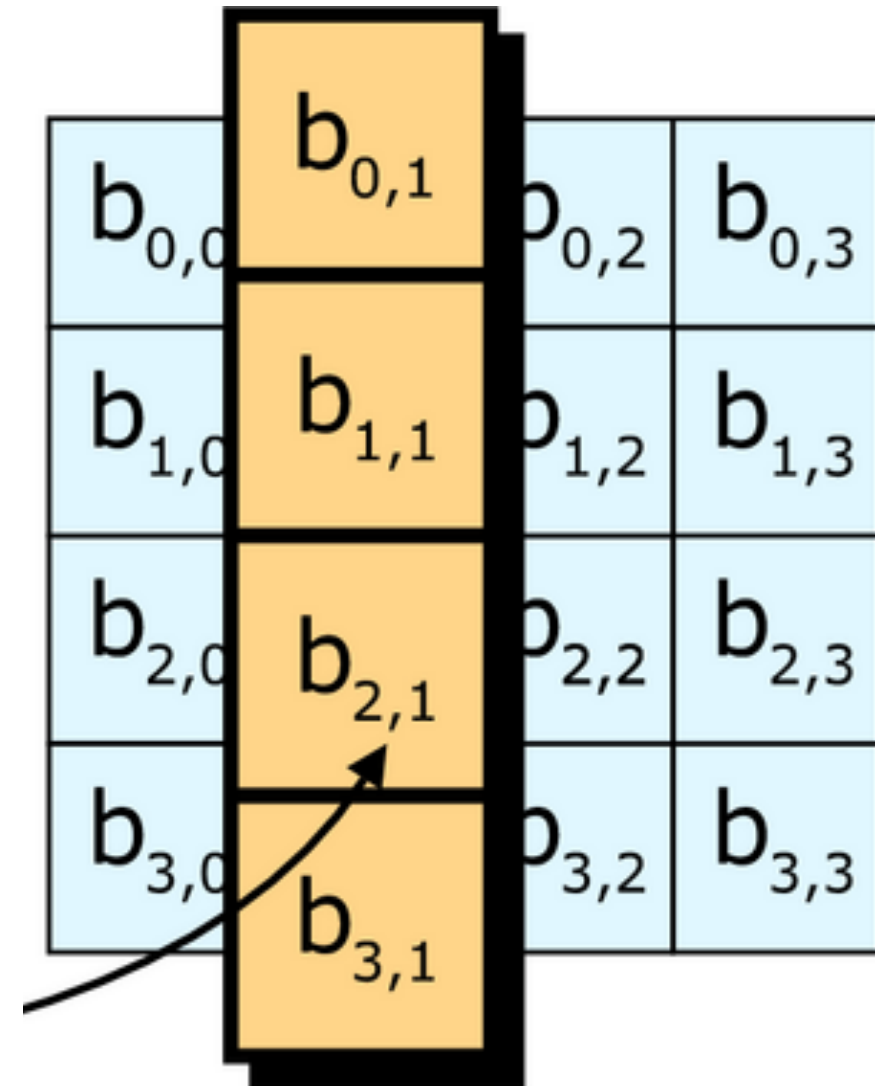
Chrome, Firefox, Safari
(soon Opera.)





AES-CTR nonce re-use (Nov. 2012)

- Reported by: Daniel Faucon (now a Cryptocat developer.)
- Parties use shared secret key, and...
- Nonce for both conversation parties started at 0 and incremented for each message.





AES-CTR nonce re- use (Nov. 2012)

$$C = P \oplus F(\text{Key}, IV)$$

where P is the plaintext, C is the ciphertext, and F is a complex function of its two inputs.

The problem with this is if you encrypt two different plaintexts with the same Key , IV values, then the attacker gets two pairs:

$$C_1 = P_1 \oplus F(\text{Key}, IV)$$

$$C_2 = P_2 \oplus F(\text{Key}, IV)$$

Where he can see the values C_1 , C_2 . With those, he can then compute:

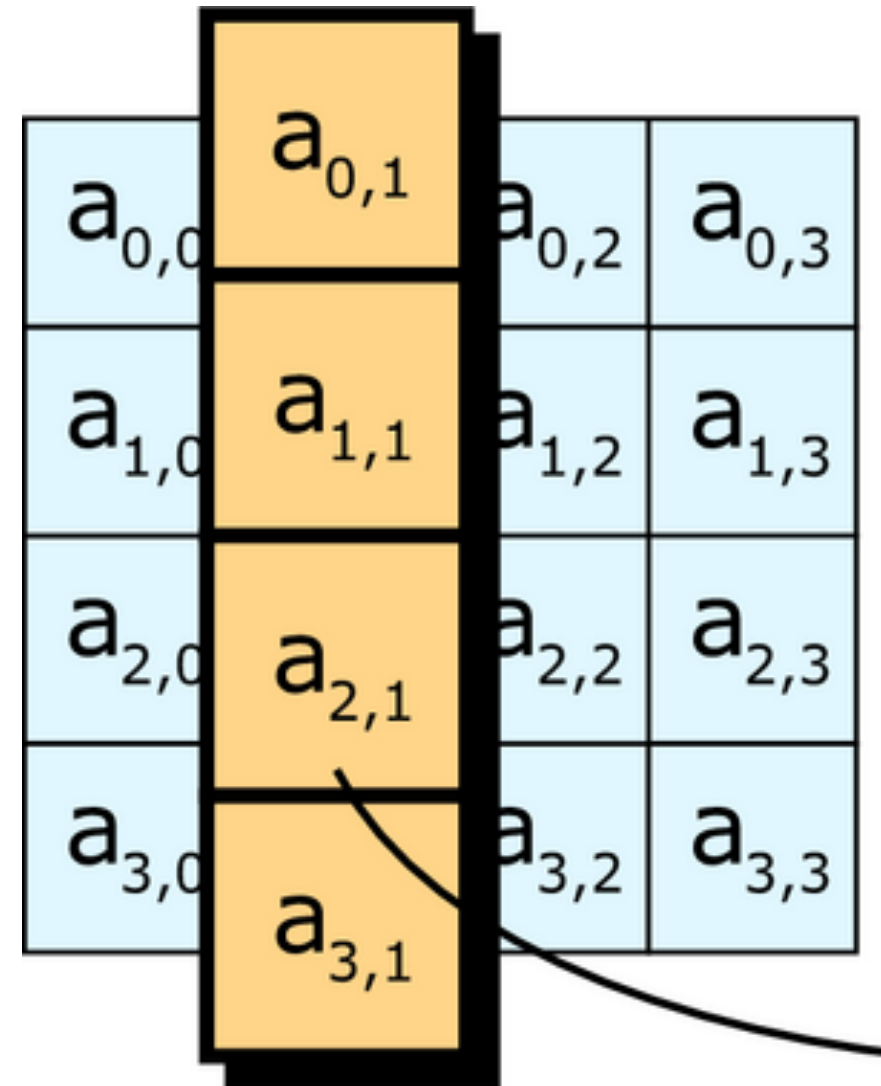
$$C_1 \oplus C_2 = P_1 \oplus P_2$$

and thus deriving the value of the two plaintexts exclusive-or'ed together.



AES-CTR nonce re-use (Nov. 2012)

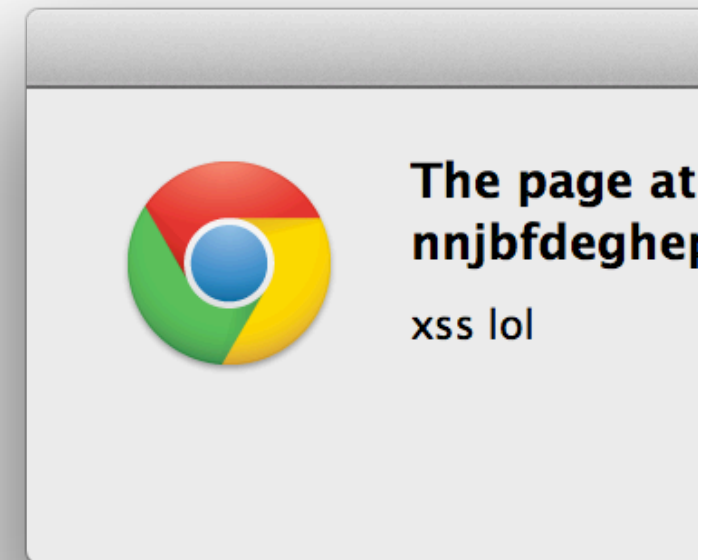
- Fixed by generating random nonces.
- Cryptocat client stores each nonce, discards messages with repeat nonces and warns user.





Code execution via nickname (Nov. 2012)

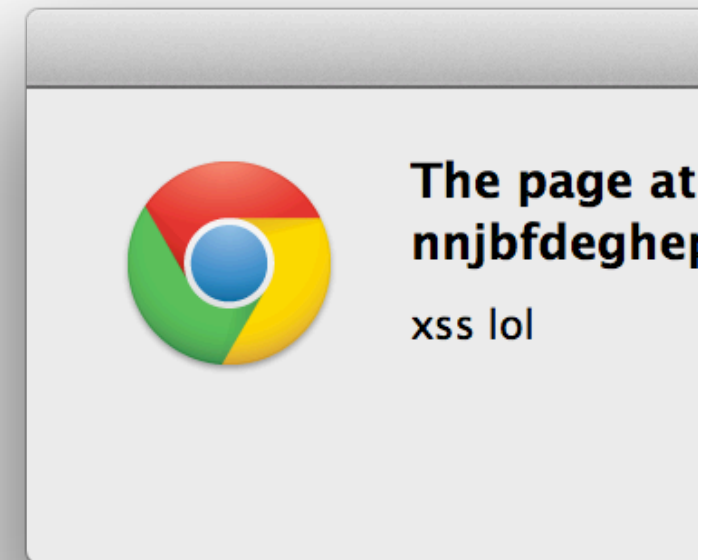
- Reported by Mario Heiderich & team (as part of a paid audit.)
- With Cryptocat, now you can have XSS bugs in your crypto!
- Important lesson: always watch out for the weakest link in a crypto app (might be the UI code.)





Code execution via nickname (Nov. 2012)

- Chrome now has impressive security restrictions for browser apps/extensions.
- Severely limits code injection/XSS attack surface.





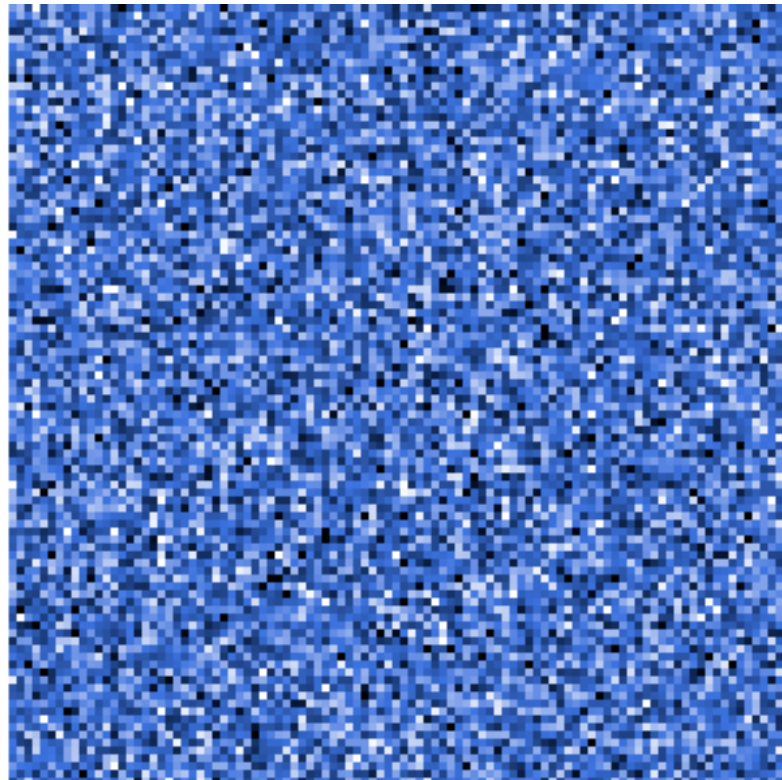
PRNG Bug (July 2013)

- Reported by: Steve Thomas, further researched and documented by Paul Ducklin of Sophos Security.
- Shows how a tiny typo can have a big effect.
- Strong CSPRNG (Salsa20) with strong seed!
- But when converting output to decimals, mistake produced bias towards 0.

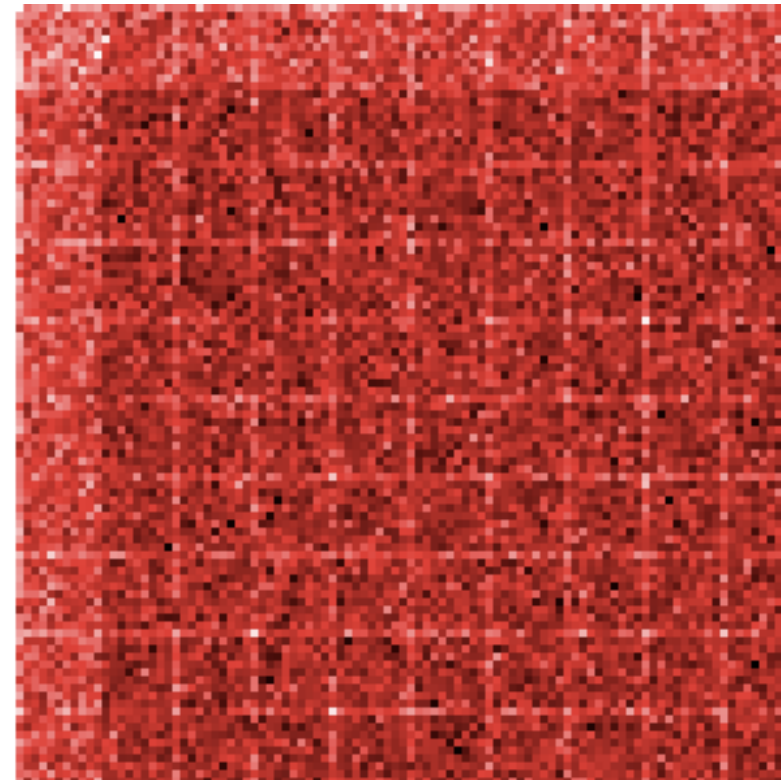
```
ore/js/etc/cryptocatRandom.j  
50,7 +60,7 @@ else {  
    var x, o = '';  
    while (o.length < 16) {  
        x = state.getBytes(1);  
        if (x[0] <= 250) {  
            if (x[0] < 250) {  
                o += x[0] % 10;  
            }  
        }  
    }  
}
```



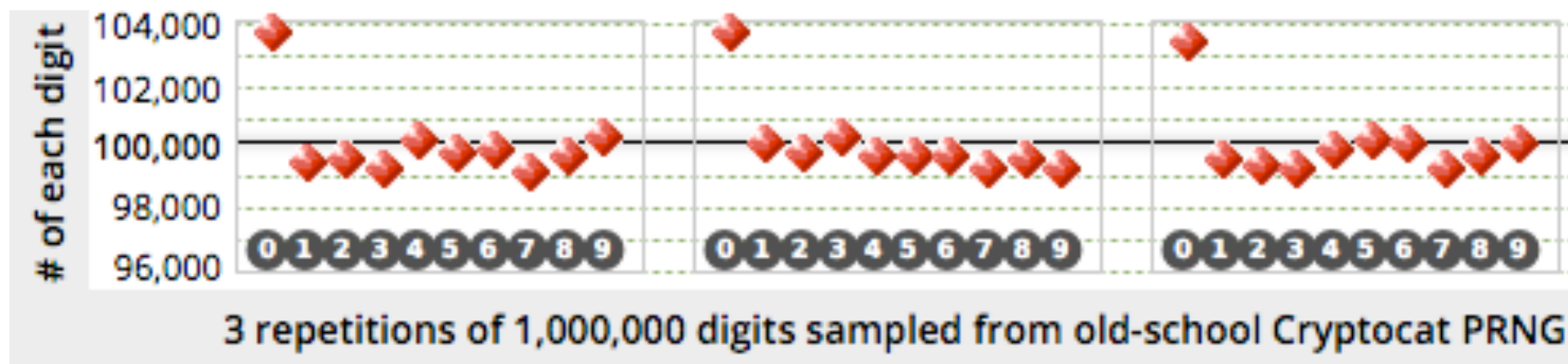
PRNG Bug (July 2013)



Colourmap of 20,000,000 Cryptocat floats (derived from /dev/urandom values 0..249)



Colourmap of 20,000,000 old-school Cryptocat floats (derived from PRNG values 0..250)



Credit for graphics: Paul Ducklin, Sophos Security (thanks!)



Wrong data typing

bug (July 2013)

- Reported by Steve Thomas (published as “Decryptocat”)
- Disastrous bug, reputation of project still recovering.
- For ECDH private key, we generated 32 **decimals** instead of 32 **bytes**.
- Security went from $\sim 2^{250}$ to $\sim 2^{54}$.

90	90	multiParty.genPrivateKey = function() {
91		- rand = Cryptocat.randomString(32, 0, 0, 1);
92		- myPrivateKey = BigInt.str2bigInt(rand, 10);
	91	+ var rand = Cryptocat.randomString(64, 0, 0, 0, 1);
	92	+ myPrivateKey = BigInt.str2bigInt(rand, 16);
93	93	return myPrivateKey;



Wrong data typing

bug (July 2013)

- This bug was **missed by two audits by leading code security and auditing firms.**
- Possible reason: it's hard/impossible to unit test for this kind of thing.

90	90	multiParty.genPrivateKey = function() {
91		- rand = Cryptocat.randomString(32, 0, 0, 1);
92		- myPrivateKey = BigInt.str2bigInt(rand, 10);
	91	+ var rand = Cryptocat.randomString(64, 0, 0, 0, 1);
	92	+ myPrivateKey = BigInt.str2bigInt(rand, 16);
93	93	return myPrivateKey;



It's not all bad

- These bugs happen in any good encryption project, early in its life.
- We got some good feedback and dealt with the bugs transparently.

What Cryptocat Doesn't Do

Cryptocat aims to offer strongly encrypted, private I...
ng, it's important to note what Cryptocat does *not* prote

Cryptocat does not anonymize you: While your communications are encrypted, you
still be traced since Cryptocat does not mask your IP address. For anonymiz
y recommend using [Tor](#).

Cryptocat does not protect against key loggers: Your messages are encrypted a
gh the wire, but that doesn't mean that your keyboard is necessarily safe. Crypt
protect against hardware or software key loggers which might be snooping
oard strokes and sending them to an undesired third party.

Cryptocat does not protect against untrustworthy people: Parties you're conver
still leak your messages without your knowledge. Cryptocat aims to make sure
parties you're talking to get your messages, but that doesn't mean these p
ssarily trustworthy.



Tips for disclosure

- Be honest and transparent.
- Take full responsibility.
- Fix quickly.
- Be truly open source.
- Encourage further audits.
- Learn from mistakes.
- Perfect your practice.

What Cryptocat Doesn't Do

Cryptocat aims to offer strongly encrypted, private I. ng, it's important to note what Cryptocat does *not* prote

Cryptocat does not anonymize you: While your communications are encrypted, you still be traced since Cryptocat does not mask your IP address. For anonymiz y recommend using [Tor](#).

Cryptocat does not protect against key loggers: Your messages are encrypted a gh the wire, but that doesn't mean that your keyboard is necessarily safe. Cryptocat protect against hardware or software key loggers which might be snooping oard strokes and sending them to an undesired third party.

Cryptocat does not protect against untrustworthy people: Parties you're conver still leak your messages without your knowledge. Cryptocat aims to make sure parties you're talking to get your messages, but that doesn't mean these p ssarily trustworthy.



Tips in general

- Be honest and transparent.
- Be truly open source.
- Be inclusive but keep angry people away.
- Be clear about security claims/experimental status.
- Trust yourself and learn.

- Be a cat :3

What Cryptocat Doesn't Do



Cryptocat aims to offer strongly encrypted, private I...
ng, it's important to note what Cryptocat does *not* prote

Cryptocat does not anonymize you: While your communications are encrypted, you
still be traced since Cryptocat does not mask your IP address. For anonymiz
y recommend using [Tor](#).

Cryptocat does not protect against key loggers: Your messages are encrypted a
gh the wire, but that doesn't mean that your keyboard is necessarily safe. Crypt
protect against hardware or software key loggers which might be snooping
oard strokes and sending them to an undesired third party.

Cryptocat does not protect against untrustworthy people: Parties you're conver
still leak your messages without your knowledge. Cryptocat aims to make sure
parties you're talking to get your messages, but that doesn't mean these pa
ssarily trustworthy.



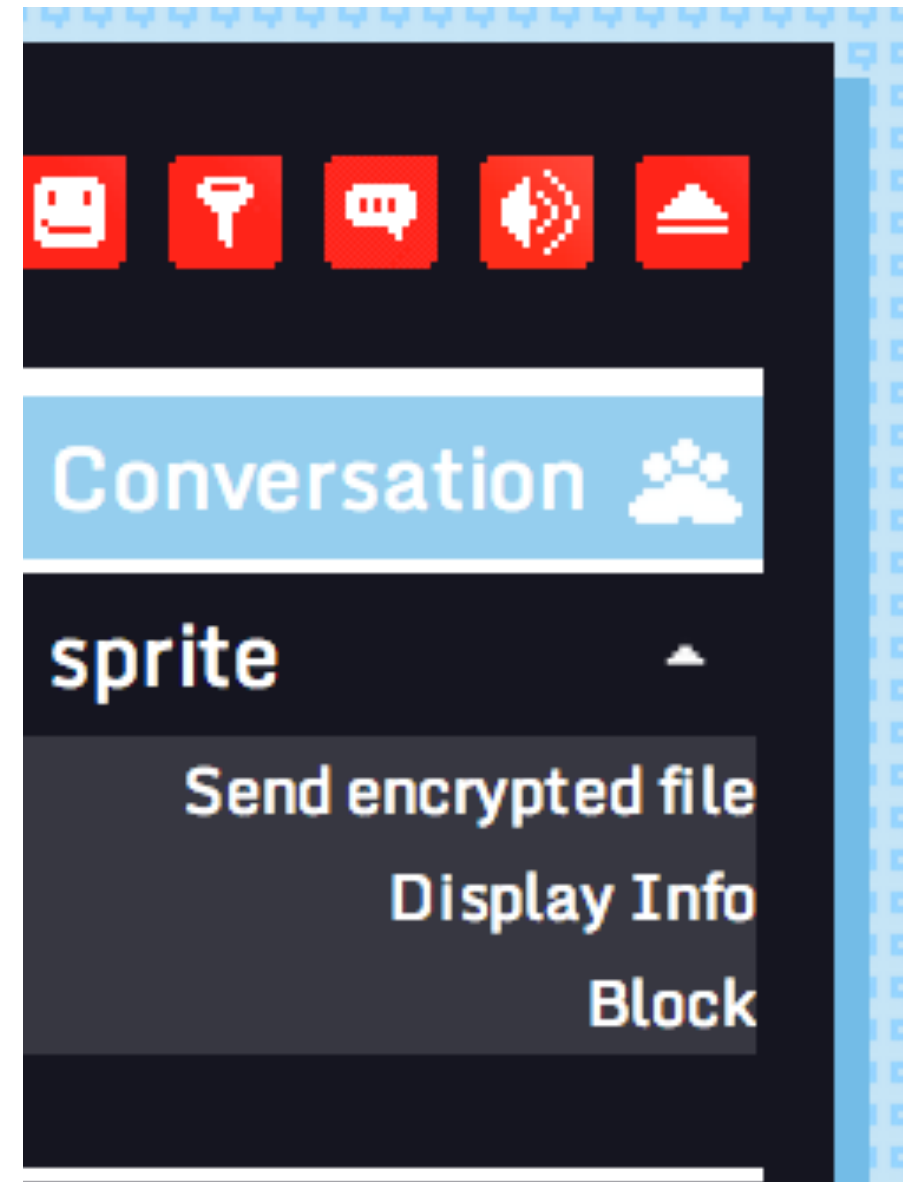
Who has your metadata when you use Cryptocat?	 Cryptocat Server	 Your ISP
Conversation name	Yes	No
Your nickname	Yes	No
Can see that you are connecting to Cryptocat	Yes (Sees a connecting IP)	Yes (Except if using Tor)
Time messages were sent	Yes	Yes
Which nicknames you are messaging privately/ having file transfers with	Yes	No
Your IP address	Yes (Except if using Tor)	Yes
Contents of conversation	No	No
Contents of file transfers	No	No
Names of files transferred	No	No
Sizes of files transferred	Yes (Approximately)	Possibly
Types of files transferred	Yes	No
Public keys and fingerprints	Yes	No
Private keys	No	No



Is it worth it?

We started in 2011: State of browser crypto almost non-existent.

Is it worth it? Are there any real accessibility results?

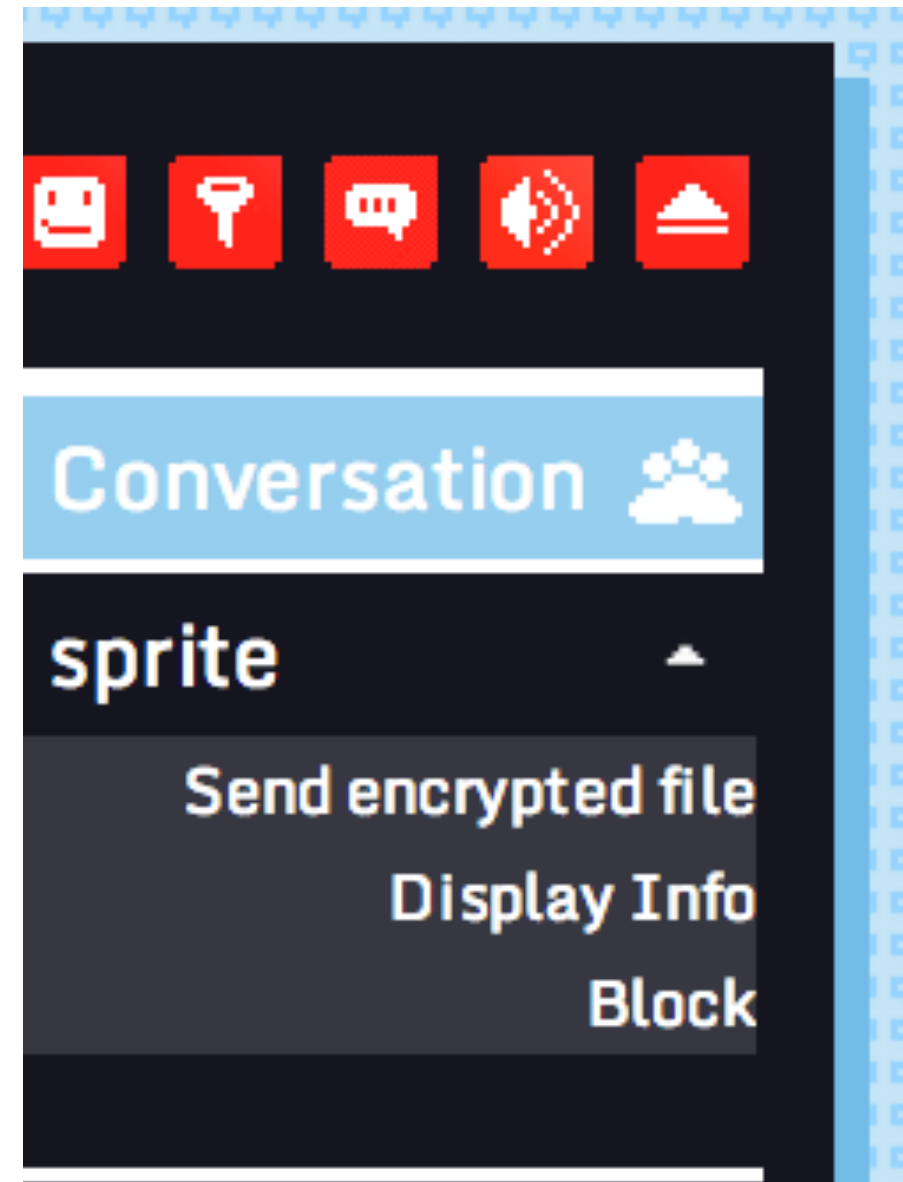




So much progress!

Teachers, counsellors,
Journalists,
Friends and family,
Businesspeople,
...have found a use for
accessible privacy.
~80,000 regular users.

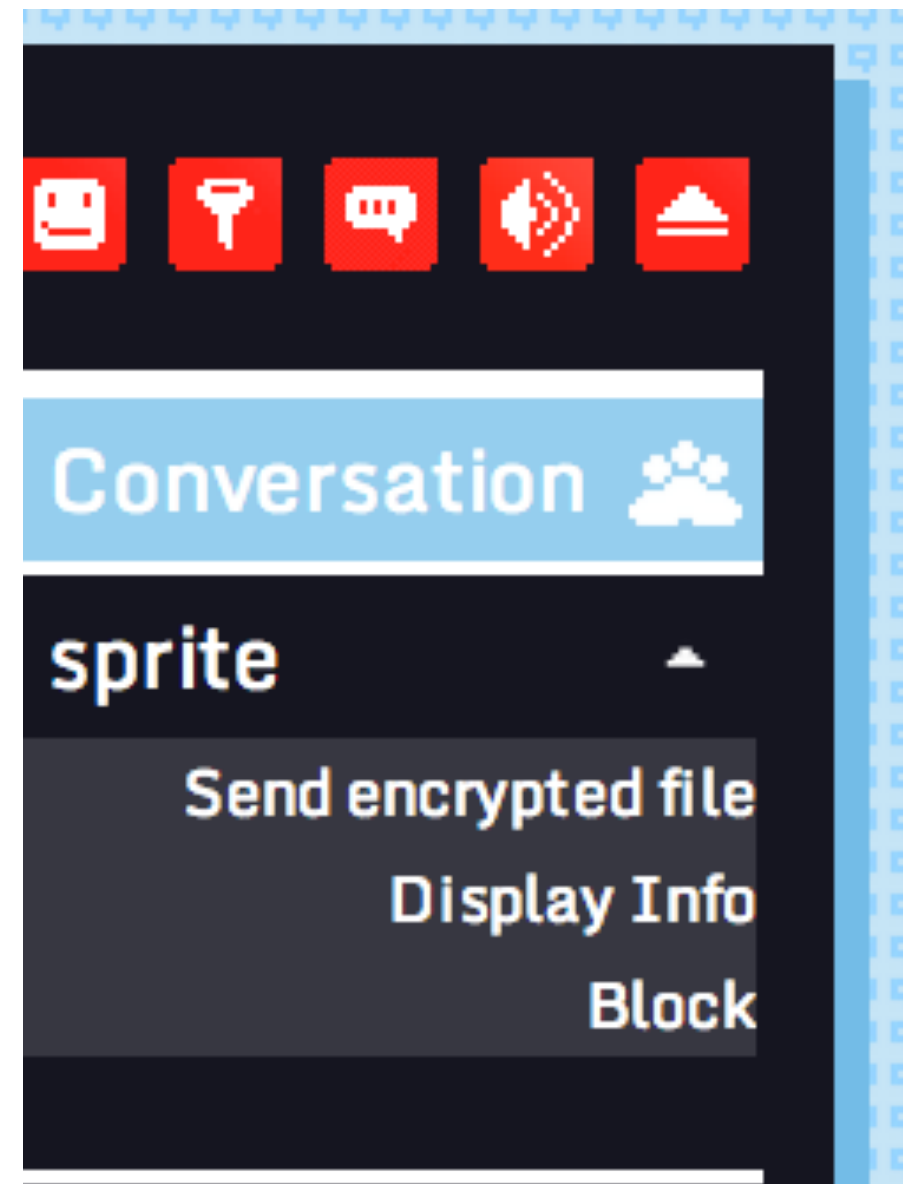
Plus, we have overcome
many technical challenges.





Big achievements

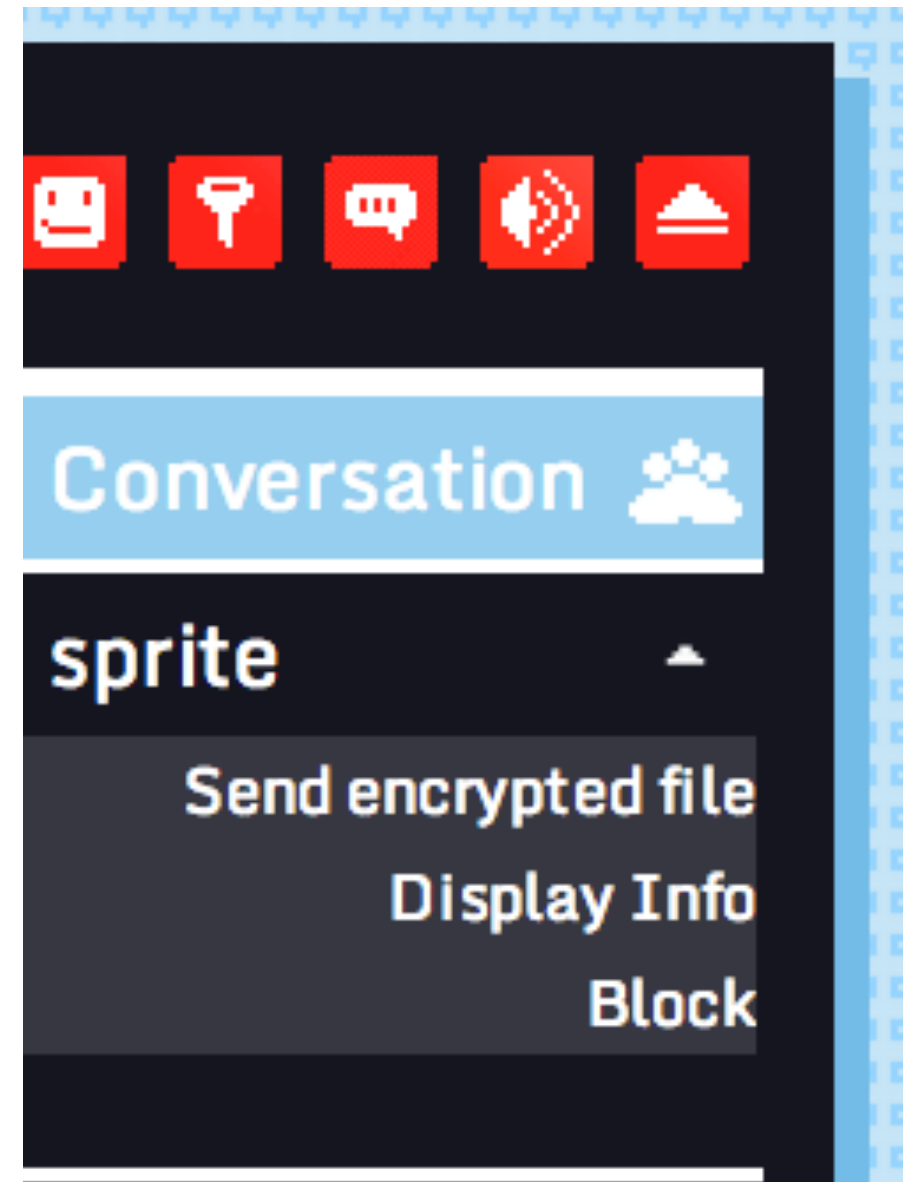
- Success story in making crypto usable!
- Great study of group chat encryption.
- OTR in the browser.
- Use-case for W3C Crypto API.





Overall positive outlook

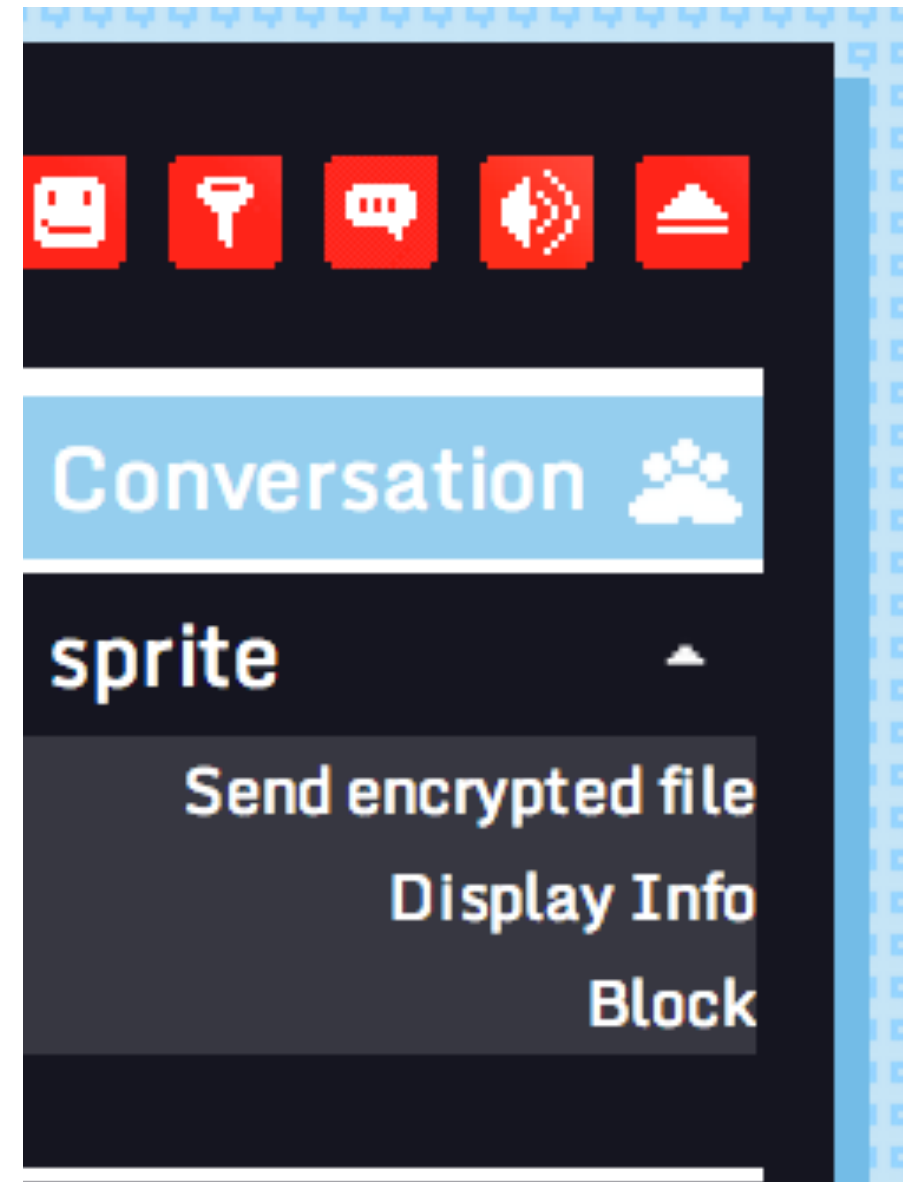
- More scrutiny than other projects = faster security improvements than other projects
- Third audit is underway right now (by Zooko Wilcox-O'Hearn, and team)





Yes, you can use Cryptocat!

- Obviously not as a replacement for PGP or something.
- But instead of Facebook chat or Skype, it's a great alternative with a lot of community review.



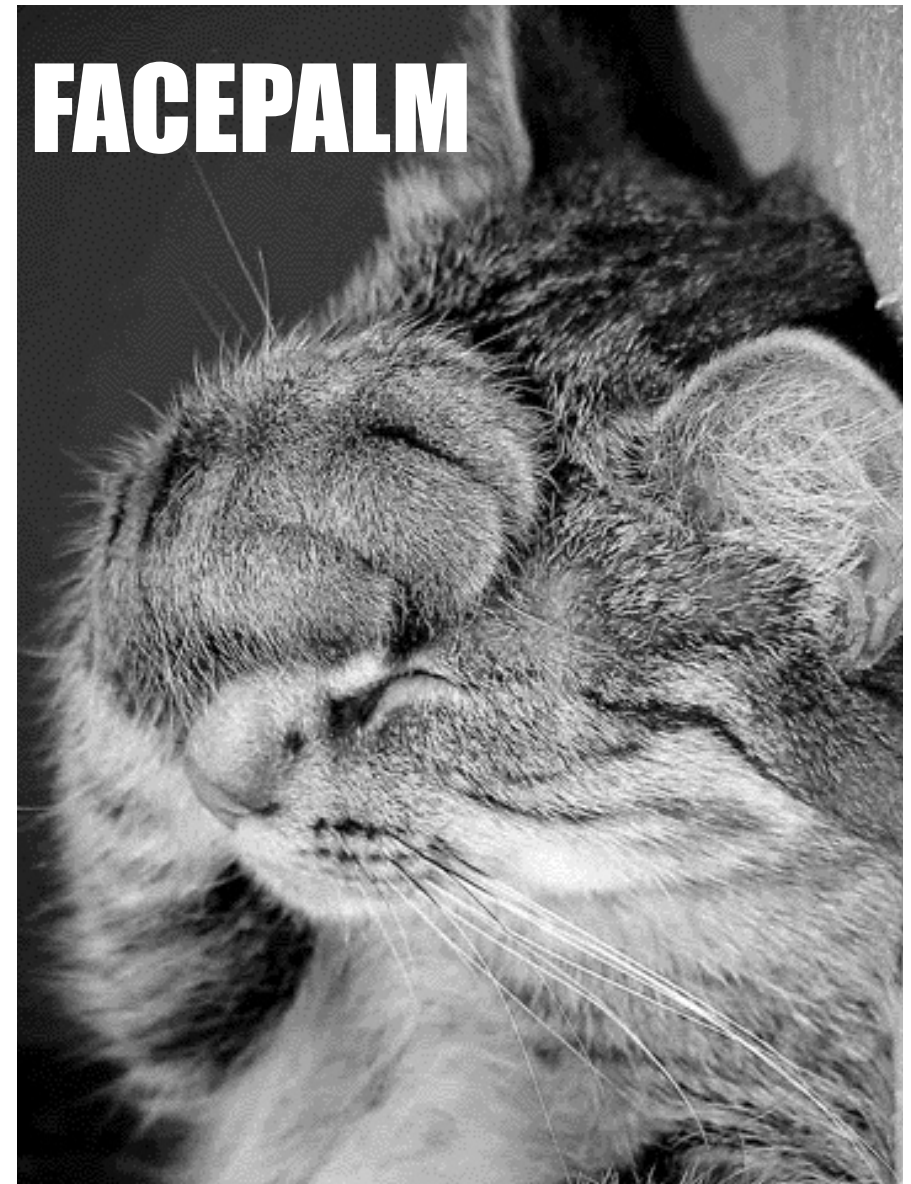


People today

“Let’s solve a global surveillance apparatus built thanks to strong shared realist foreign policy convictions doubled by domestic assurances...

WITH AN APP.”

FACEPALM





Localization matters

Over 35 languages covered.

Cryptocat automatically detects browser language, configures accordingly.





Get involved!

Website: www.crypto.cat

Twitter: @cryptocatapp

IRC: #cryptocat, irc.oftc.net

My email: nadim@crypto.cat

