

Cryptocat

Genma

1^{er} avril 2014



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.



A propos de moi

Où me trouver sur Internet ?

- Le Blog de Genma :
<http://genma.free.fr>
- Twitter :
<http://twitter.com/genma>

Mes centres d'intérêts ?

Plein de choses dont :

- La veille technologique
- Le chiffrement

Qu'est ce que Cryptocat

- Cryptocat est une application web open source destinée à permettre des communications sûres et chiffrées.
- Cryptocat chiffre les chat côté client ; la confiance au serveur se limite à des données déjà chiffrées.
- Cryptocat est une extension pour Mozilla Firefox, Google Chrome et Safari, ainsi qu'une application Mac OSX native.



ADD-ONS

EXTENSIONS | THEMES | COLLECTIONS | MORE...

search for add-ons

Welcome to Firefox Add-ons. Choose from thousands of extra features and styles to make Firefox your own.

Home » Extensions » Cryptocat



Cryptocat 2.1.21

by the Cryptocat Project

Cryptocat lets you instantly set up a safer chatting alternative. Cryptocat makes accessible communications to everyone.

+ Add to Firefox

This add-on has been preliminarily reviewed

Software Installation



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:



Cryptocat (Author not verified)

<https://addons.mozilla.org/firefox/downloads/file/248812/cryptocat-2.1.21-fx.xpi?s>

Install Now

Cancel

Cryptocat en extension Firefox

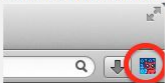
- Cryptocat s'installe donc comme une extension Firefox et au premier lancement, il est indiqué que l'on aura un icône dans la barre de menu.



Getting started with Cryptocat

Thanks for installing Cryptocat. Now, it's easier than ever to chat with friends without risking your privacy. Here's how you can open Cryptocat in **Firefox**:

1. Click the **Cryptocat** icon in your Firefox toolbar to launch Cryptocat:



2. Start chatting by typing in a **name for your conversation** and a **nickname for yourself**!

Please remember that Cryptocat is not a magic bullet. While we are trying our best to make encrypted chat easy to use and accessible, remember to never trust any software with your life. Cryptocat is still under continuous research and improvement.

We hope you enjoy safe, private chats with Cryptocat! 🐱

Cryptocat - lancement d'une conversation

Une fois que l'on clique sur l'icone de Cryptocat, on a la fenêtre suivante :

- On saisit le nom d'une conversation (que l'on veut créer ou rejoindre).
- On saisit un pseudonyme.
- On clique sur connexion.



CRYPTOCAT

nom de la conversation

pseudonyme

connexion

Saisissez le nom d'une conversation à rejoindre.

Conversations privées pour tout le monde.

Bienvenue chez Cryptocat. Voici quelques conseils utiles:



Cryptocat n'est pas une solution miracle. Vous ne devriez jamais faire confiance à n'importe quel logiciel avec votre vie privée.



Cryptocat ne peut pas vous protéger contre les personnes malhonnêtes ou les enregistreurs de frappe, et ne rend pas votre connexion anonyme.



CRYPTOCAT

demogenma

genma

connexion

Connexion...

Conversations privées pour tout le monde.

Bienvenue chez Cryptocat. Voici quelques conseils utiles:



Cryptocat n'est pas une solution miracle. Vous ne devriez jamais faire confiance à n'importe quel logiciel avec votre vie privée.



Cryptocat ne peut pas vous protéger contre les personnes malhonnêtes ou les enregistreurs de frappe, et ne rend pas votre connexion anonyme.



CRYPTOCAT



Generating encryption keys...

Here is an interesting fact while you wait:



Private Co

Welcome to Cryptocat. Here are some helpful tips:



Cryptocat is not a magic bullet. You should never trust any piece of software with your life.



Cryptocat can't protect you against untrustworthy people or key loggers, and does not anonymize your connection.

Cryptocat - début d'une conversation

- La communication est alors établie de façon chiffrée.
- Dans l'exemple, Genma voit que Ryoga est connecté.
- Ryoga lui a envoyé un message, auquel Genma réponds.




genma@demogenma

Group conversation. Click on a user for private chat.



08:32 + ryoga

Conversation 

ryoga

genma Salut ryoga, c'est Genma

|





genma@demogenma

Group conversation. Click on a user for private chat.



08:32 + ryoga

genma Salut ryoga, c'est Genma

ryoga Salut Genma! How are U?

Conversation

ryoga ▾



Cryptocat - conversation en cours

- Quand un participant est en train de rédiger un texte, un icône l'indique sur l'écran des autres participants.



ryoga@demogenma

Group conversation. Click on a user for private chat.



08:32 + genma

genma Salut ryoga, c'est Genma

ryoga Salut Genma! How are U?

ryoga We are using cryptocat, fun isn't it?

ryoga Let's test the notification!

genma 

Conversation



genma



Cryptocat - validation des participants

Dans la barre de menu

- Quand on clique sur l'icône myInfo, on a différentes informations.
- En particulier le "group conversation fingerprints".
- Et le OTR fingerprint.



genma@demogenma

Group conversation. Click on a user for private chat.



08:32 + ryoga

genma Salu

ryoga Salu

ryoga We

ryoga Let'

genma

Group conversation fingerprint:

47CDC344 91CB247 E9A4B70C 0A1CFFAD CF20D643

OTR fingerprint (for private conversations):

14E78400 3740CFCD 12B2E8FE 4E0100B8 5372D1F4

My Info ation

ryoga



Cryptocat - validation des participants

Quand on clique sur le nom d'un participant

- On retrouve les mêmes informations.
- Il est possible de saisir une question secrète
- Et la réponse à cette question.

On transemtra la réponse au participant via un autre canal de communication.



genma@demogenma

Group conversation. Click on a user for private chat.



08:32 + ryoga

genma Salu

ryoga

ryoga Salu

ryoga We

ryoga Let'

Group conversation fingerprint:

59159D30 795AE4B4 850200FA 8389DDA4 0A686B50

Authenticate

OTI fingerprint (for private conversations):

01277434 731BDE21 83A9D784 52BC2522 8004E2D1

Verify this user's identity by asking a secret question. Answers must match exactly!

Secret question

Secret answer

Ask

Conversation



ryoga

Display Info

Ignore



Cryptocat - validation des participants

Sur l'écran de l'autre participant (Ryoga)

- Celui-ci se voit demander la réponse à la question secrète.
- Il saisit la réponse qu'il connaît.



ryoga@demogenma

Group conversation. Click on a user for private chat.



08:32 + genma

08:32:16

Salu

Authenticate

ryoga

Salu

ryoga

We s

ryoga

Let'

genma

genma wants to verify your identity. Please answer the below secret question to authenticate yourself:

What's ur favorite anim?

Answer

Your answer must exactly match the one given by genma.

Conversation



genma



Cryptocat - validation des participants

Sur l'écran de Genma

- Il y a un message qui indique Ryoga a bien saisi la bonne réponse.
- On a une validation que la personne qui utilise le pseudonyme de Ryoga est bien celle qu'elle prétend être.



genma@demogenma

Group conversation. Click on a user for private chat.



08:32 + ryoga

genma Salu

ryoga

ryoga Salu

ryoga We

ryoga Let'

Group conversation fingerprint:

59159D30 795AE4B4 850200FA 8389DDA4 0A686B50

OTR fingerprint (for private conversations):

01277434 731BDE21 83A9D784 52BC2522 8004E2D1

Identity verified.

Conversation

ryoga

Display Info

Ignore

Cryptocat - validation des participants

- Ryoga posera à son tour une question secrète si besoin, pour valider l'identité de Genma.