CryptTalk 1.0 User Guide

1 Introduction

CryptTalk lets you talk with your friends securely by encrypting with the AES cypher each message you write in Google Talk before sending it.
The encrypted message will be received by your destinator and decrypted if this one uses CryptTalk and has the correct password. The main purpose is that the messages are sent in the network after being encrypted. This ensures you to chat without the risk of being spied.
The Advanced Encryption Standard (AES) algorithm is a symmetric-key algorithm which has been selected among others to be the most suitable and relatively secure one.
Thank you to Chris Veness, the author of the JavaScript implementation of the AES algorithm used in CryptTalk.

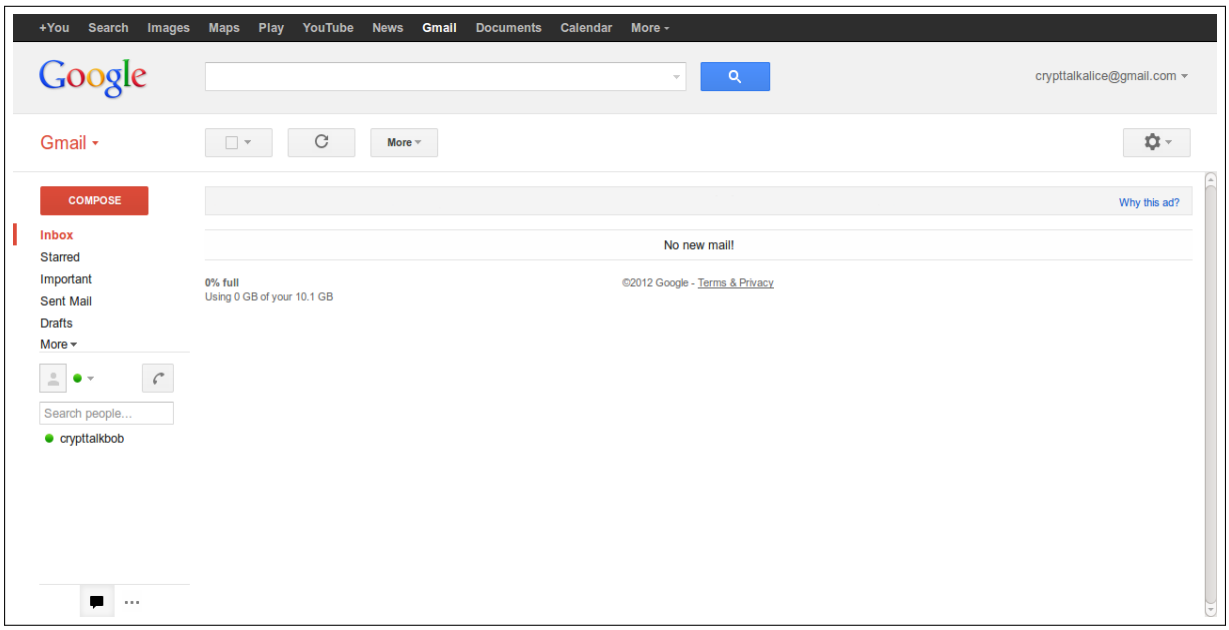
2 Requirements

The version 1.0 of CryptTalk has been tested on Mozilla Firefox 16.0.2. An Opera 12.02 version is also available on the repository.
The user needs to get the latest version of Greasemonkey on
`https://addons.mozilla.org/fr/firefox/addon/greasemonkey/`.
A version for other web browsers does not exist.

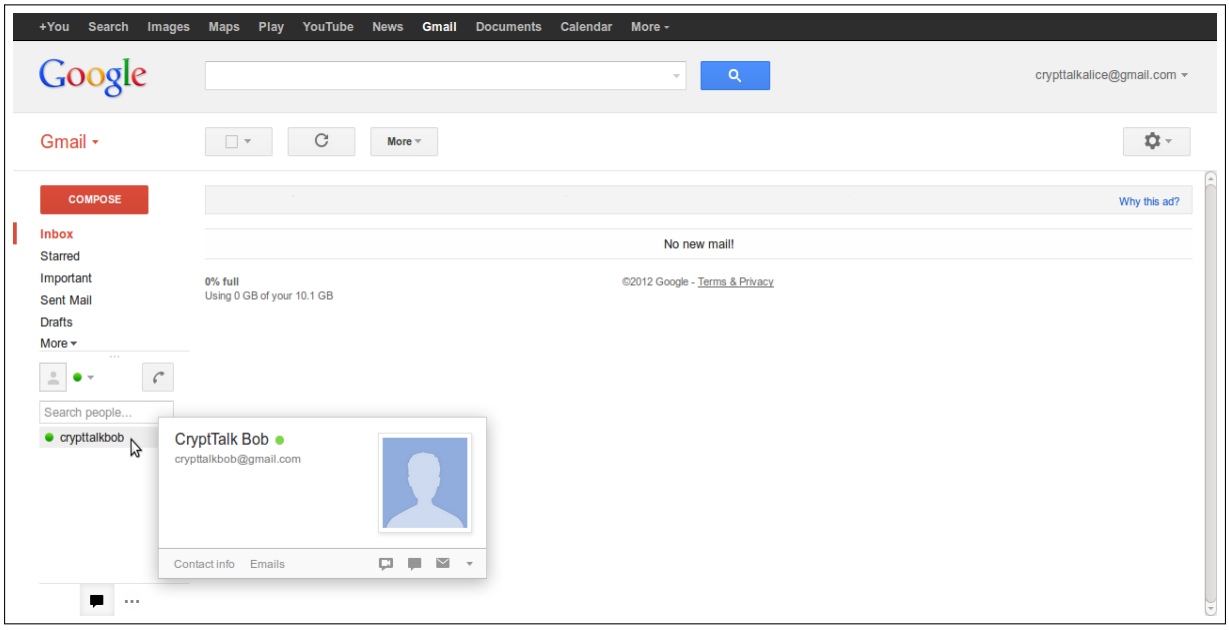
3 Installation

You first have to add CryptTalk to the list of your Greasemonkey scripts in Firefox. After downloading *CryptTalk.user.js*, you can use the Firefox menu bar *File/Open File* and just open the file.
Depending on the version of Firefox, you can also drag and drop the file on the window. You will have to activate the script in the Greasemonkey menu.

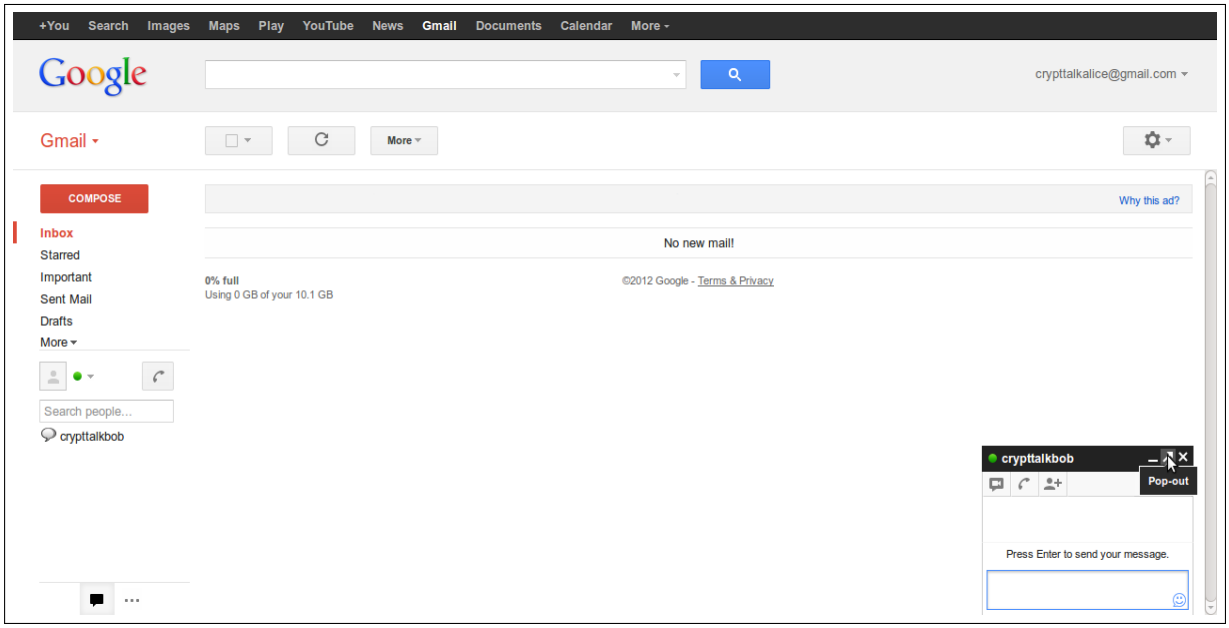
4 How to use it



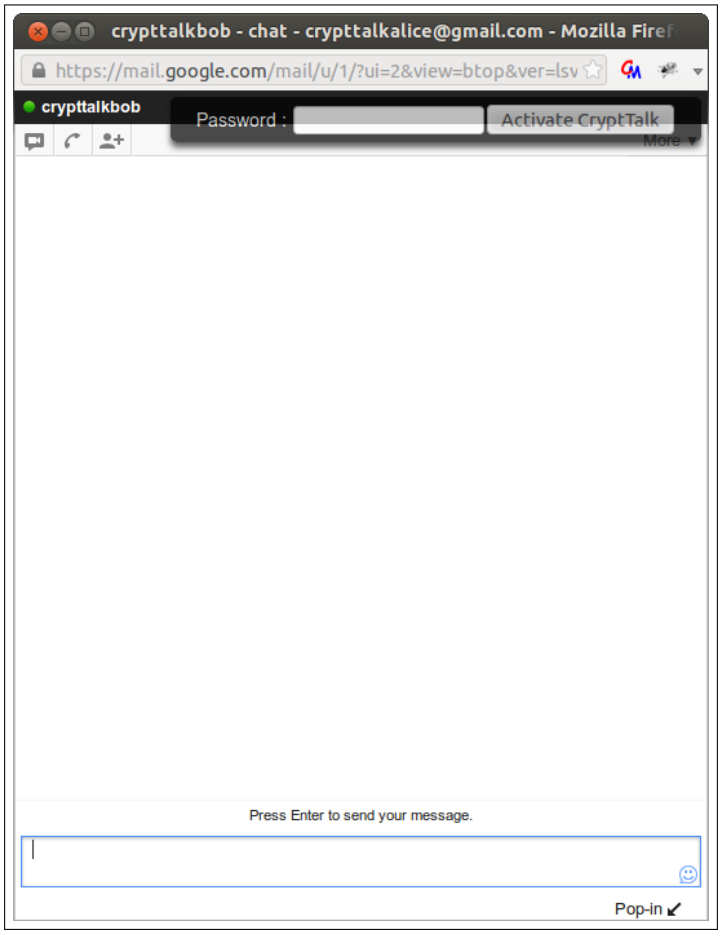
1. First, Alice connects to her Gmail account



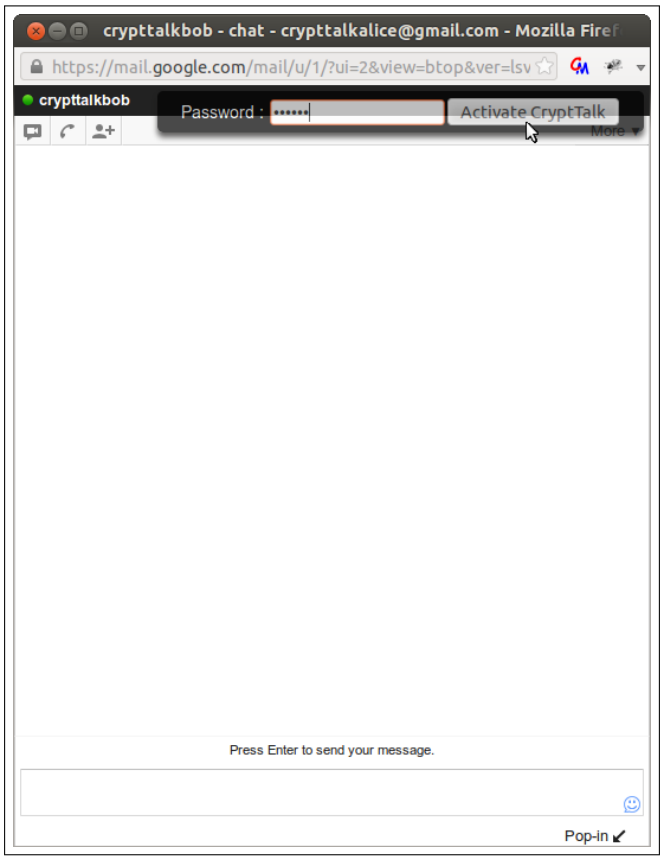
2. She then clicks on the contact she wants to chat with: Bob



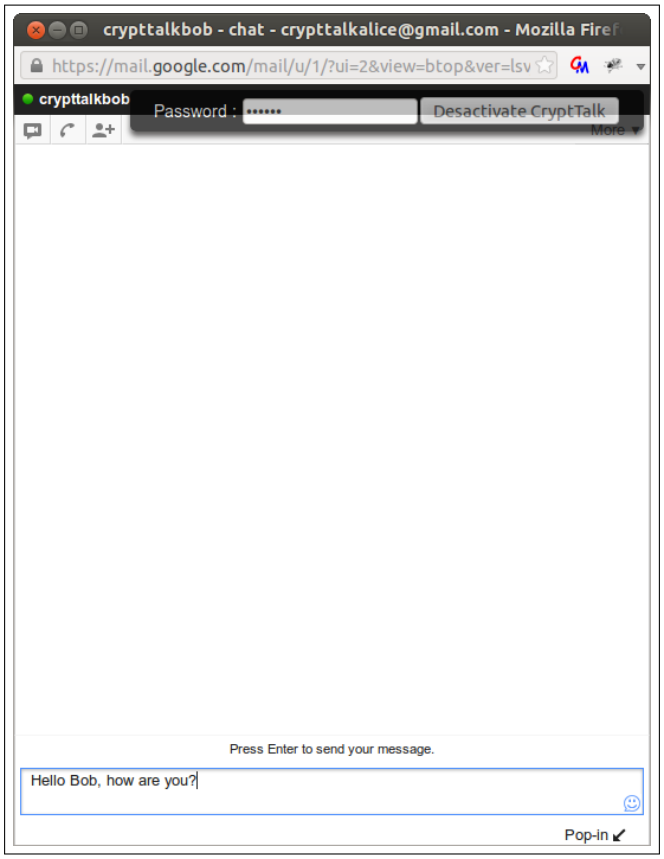
3. She pops the dialog box out to activate CryptTalk



4. The CryptTalk interface appears in the top right of the window

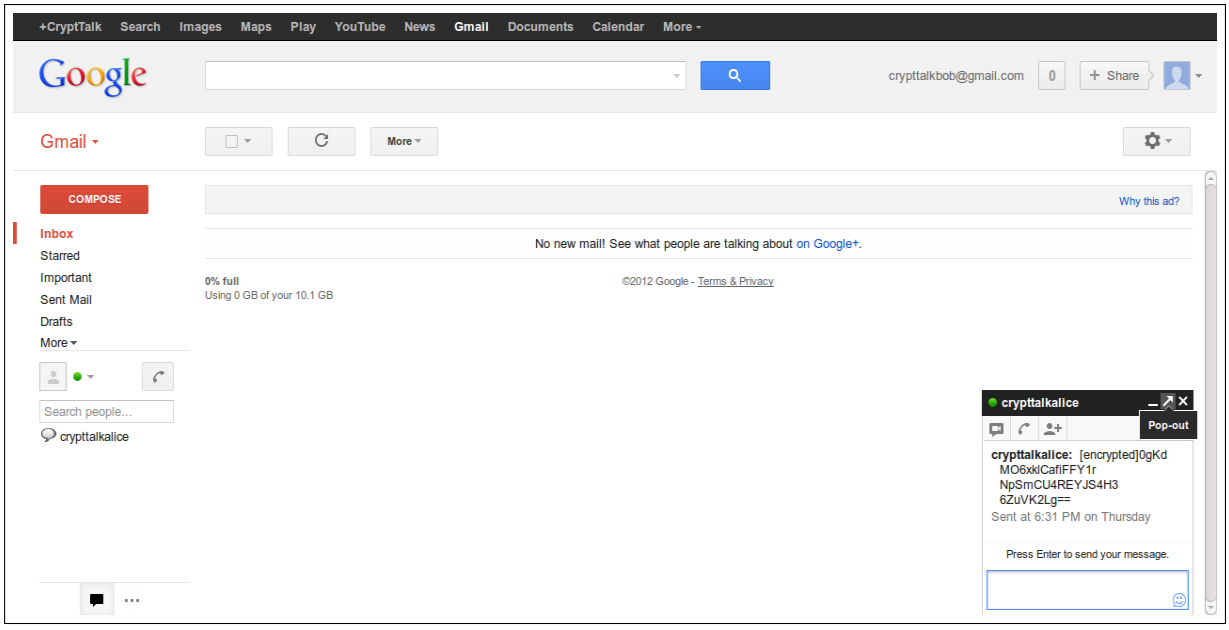


5. She enters the password and then presses “Activate CryptTalk”



6. CryptTalk is now activated and she can write messages as usual

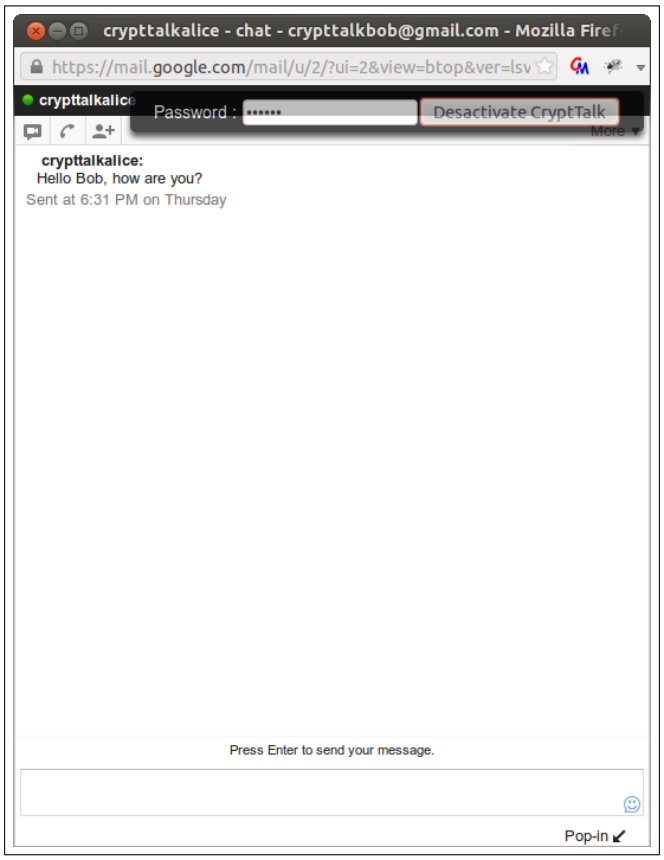
7. The encrypted message will appear clearly after a short time in the dialog box



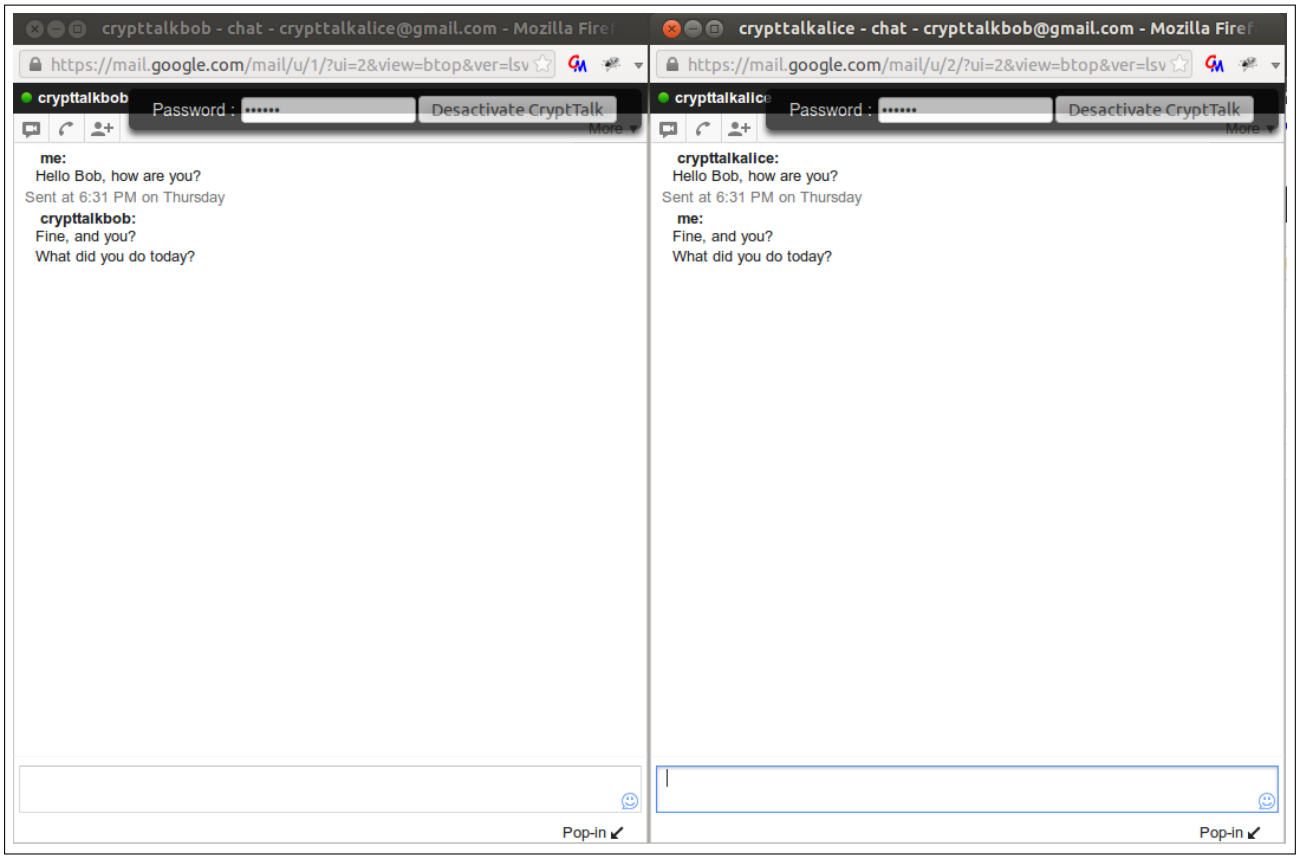
8. Now, let see what happens for Bob. He received the encrypted message from Alice

9. He pops the dialog box out. The message is still encrypted

10. He writes Alice's encryption key and activate CryptTalk



11. If the key is correct, the message will be decrypted



12. Alice and Bob can now write normally, CryptTalk will de/encrypt on-the-fly