Tetris-based Cryptography: a gateway to serious Crypto

Léo Ducas[1]

INVENTEURS DU MONDE NUMÉRIQUE

digitalcuisine

Crypto' 14, Rump Session

[1] ENS Paris, Université Paris VII, UCSD

Cryptris, a gateway to serious Crypto

Cryptris : A **scientific mediation** video Game mimicking Tetris, on the foundation and usage of asymmetric cryptography.

- Coordination, Médiation, Funding : **INRIA**
- Scenario, développement : **digitalcuisine**
- Sponsoring : **Cap Math**

It is **Open-Source**[2] and runs fully on HTML5 !

[2] https://github.com/inriamecsci/cryptris/

A Crypto Game[3]? But why ?

January 2013 :
For the first time, a user actually tries to use crypto !

[3] From Dan, Tanja and Nadia http://toogl.es/#/view/HJB1mYEZPPA

A Crypto Game ‽ But why ?

January 2013 :
For the first time, a user actually tries to use crypto !

...and fails.[3]

[3] From Dan, Tanja and Nadia `http://toogl.es/#/view/HJB1mYEZPPA`

A Crypto Game‽ But why ?

January 2013 :
For the first time, a user actually tries to use crypto !

. . .and fails. [3]

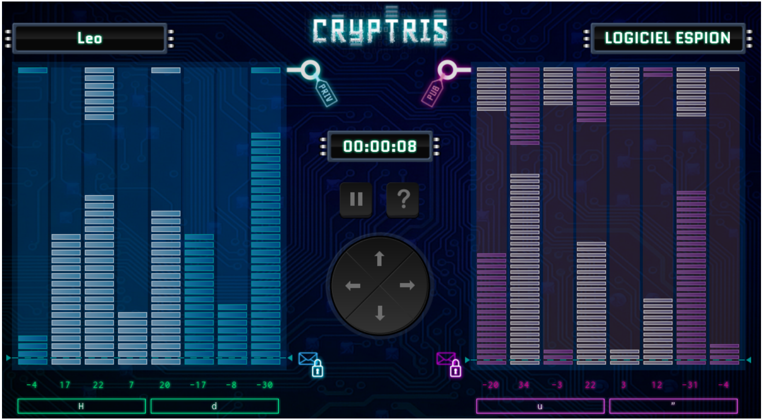
Go beyond the “IACR Copenhagen Resolution”, and act :

- Promote and Supervise the development of secure and easy to use crypto software
- Educate about cryptography : raise awareness, avoid misconceptions, fight the “**dark-art**” feeling, make it conceptually simple

[3] From Dan, Tanja and Nadia `http://toogl.es/#/view/HJB1mYEZPPA`

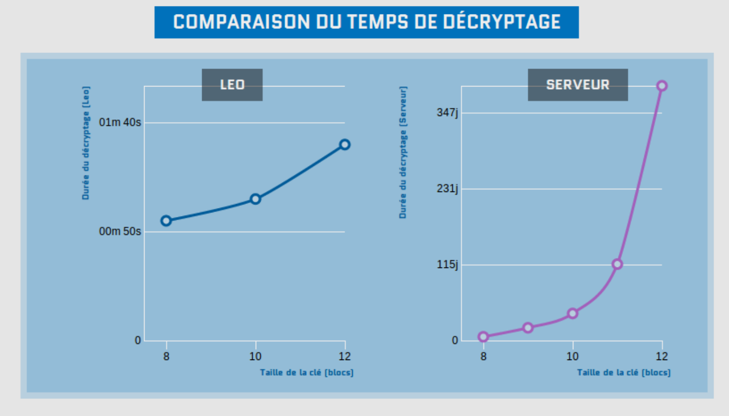
Playing against the Spy

On the left, the player (legitimate receiver) plays with the private key, making the game easy.



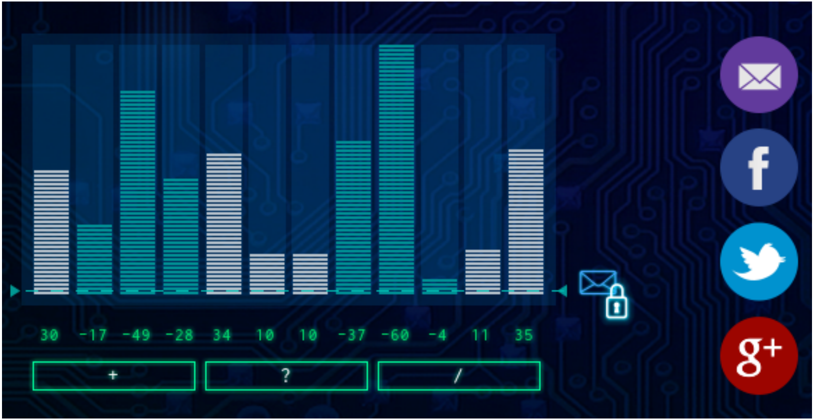
On the right, the adversary only has the public key : the game is much harder for him !

Exponential hardness



Soon it becomes impossible to decrypt for the adversary, but remains easy for the legitimate user. QEM !

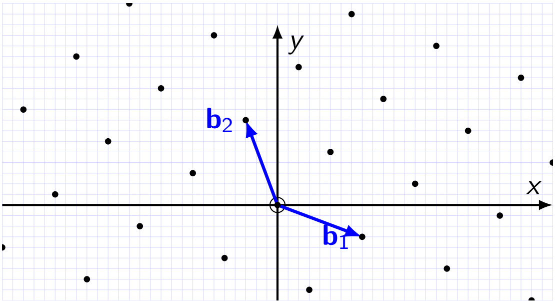
Share your Cryptopathy



The game is compatible with social networks :
challenge your contact with personalized “encrypted” messages.

Nah ! No prime numbers, can't be serious.

Its actually quite serious : Lattice based Cryptography.



It comes with 2 Popular Science articles[4] slowly switching from Tetris to serious math !

[4] published on CNRS's blog IMAGES DES MATHÉMATIQUES.

Bummer...

The game has been Obfuscated using an old algorithm

Bummer...

The game has been Obfuscated using an old algorithm

... called French.

Bummer...

The game has been Obfuscated using an old algorithm

... called French.

We are looking for $3k to $5k for internationalization of the source code and translation. Other contributions/publicity welcomed !

Figure: Non exhaustive list of logos I'd love to include

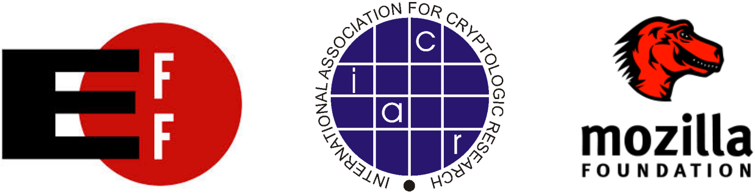
Bummer...

The game has been Obfuscated using an old algorithm

... called French.

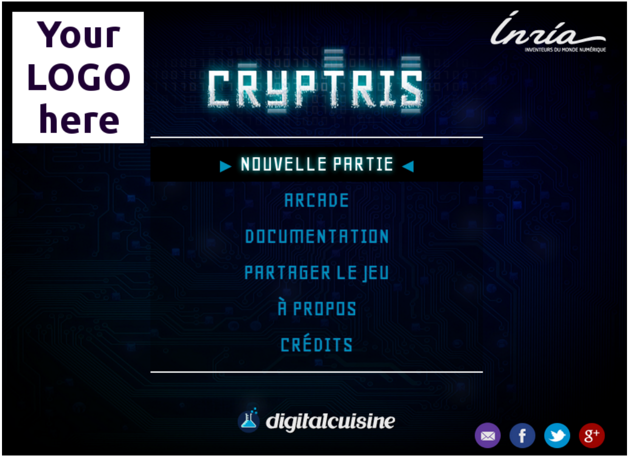
We are looking for \$3k to \$5k for internationalization of the source code and translation. Other contributions/publicity welcomed !

FIGURE: Non exhaustive list of logos I'd love to include



$\$2^{12} = o(\$2^{20})$

Be our sponsor !



And if you read French :

http://inriamecsci.github.io/cryptris/