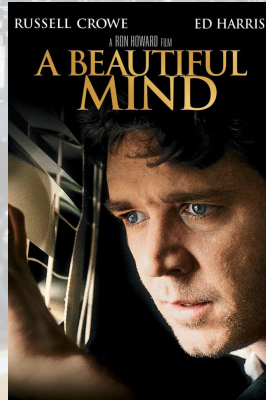
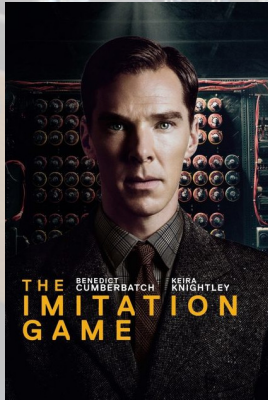


# A PANORAMA ON CLASSICAL CRYPTOGRAPHY

*Benoît Viguiier*

December 13<sup>th</sup>, 2021

# WHAT IS CRYPTOGRAPHY?



# WHAT IS CRYPTOGRAPHY?

A Pomeranian dog with light brown and white fur is wearing dark-rimmed glasses. The dog is looking down at a silver tablet computer that is propped up in front of it. The background is a soft, out-of-focus indoor setting with light-colored walls and a wooden surface.

***Cryptography is about communication in the presence of adversaries.***

**Ron Rivest**

# WHAT DO WE WANT TO PROTECT?

- **Confidentiality**
- Data Integrity
- Data origin authentication
- Entity authentication



# WHAT DO WE WANT TO PROTECT?

## ERROR

- Confidentiality

[25] BattlEye: Corrupted Data - please perform a clean game reinstall

- **Data Integrity**

OK

- Data origin authentication
- Entity authentication

# WHAT DO WE WANT TO PROTECT?

- Confidentiality
- Data Integrity
- **Data origin authentication**
- Entity authentication

# WHAT DO WE WANT TO PROTECT?

- Confidentiality
- Data Integrity
- Data origin authentication
- **Entity authentication**

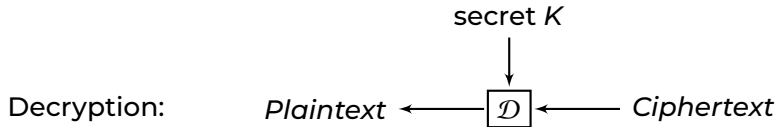
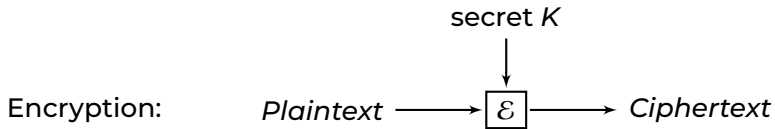


# CRYPTO IN OUR EVERYDAY LIFE.



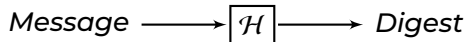
# CRYPTO 101.

## Symmetric encryption scheme

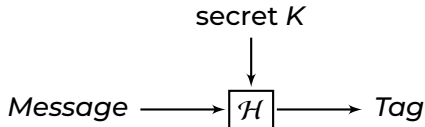


# CRYPTO 101.

## Hashing function

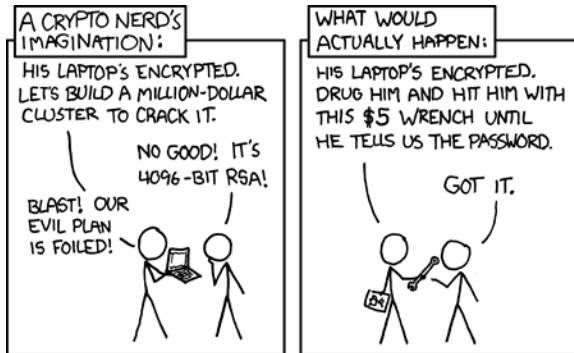


## Message Authentication Code (MAC)





# WHAT MY THESIS IS ABOUT.



<https://xkcd.com/538/>

- Designing
  - Implementing
  - Breaking
  - Verifying
  - Standardizing
- ... cryptography.



# DESIGNING.

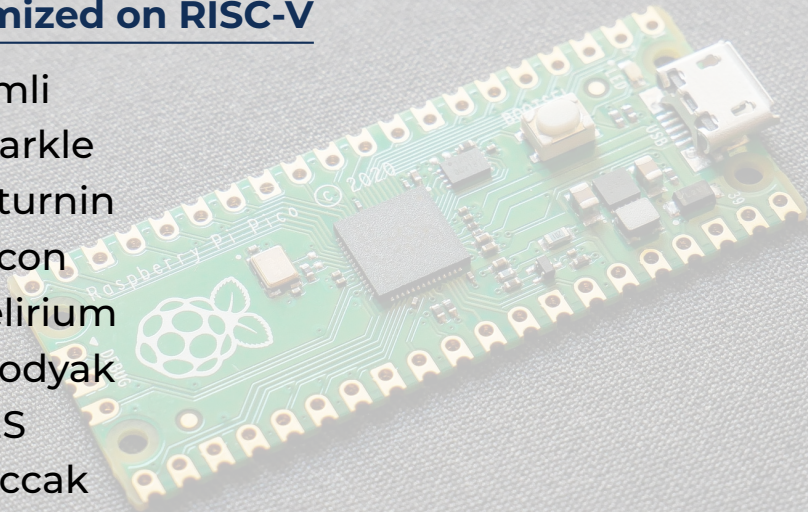
## Gimli

- Authenticated-Encryption scheme (AE)
- Cross-platform and Lightweight
- High performances & secure

# IMPLEMENTING.

## Optimized on RISC-V

- Gimli
- Sparkle
- Saturnin
- Ascon
- Delirium
- Xoodyak
- AES
- Keccak



# BREAKING.

## Cryptanalysis of Morus

- Morus is a high-performances AE scheme.

	complexity claim	our result
Morus-640	$2^{128}$	$2^{146}$
Morus-1280	$2^{256}$	$2^{152}$



# VERIFYING.

## Proof of correctness of X25519 in TweetNaCl

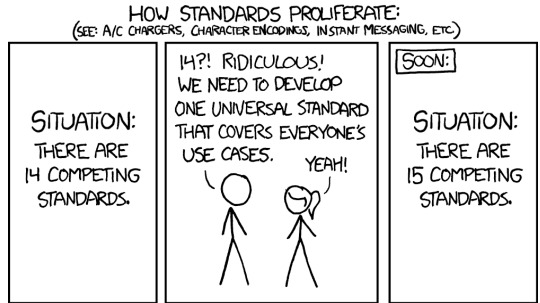
Using the Coq theorem prover, we verify:

- the correctness of the C implementation,
- that it matches RFC 7748,
- and we link with X25519 maths definition.

First complete proof from C to the maths definition.

# STANDARDIZING.

- KangarooTwelve  
(SHA-3 *on steroids*)
- 1<sup>st</sup> Draft in January 2017,
- Still not accepted...
- CFRG is very slow.



<https://xkcd.com/927/>



# Thank you for your attention.



THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

<https://xkcd.com/1403/>