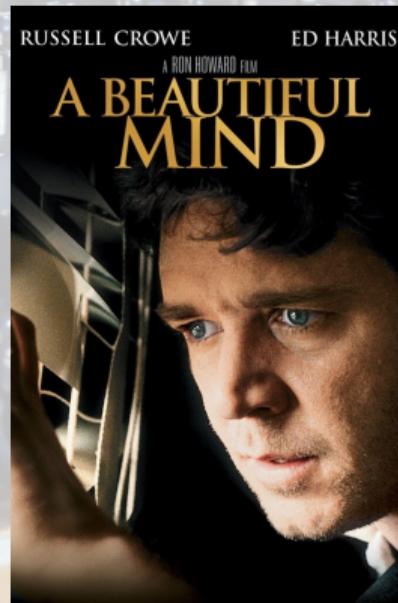
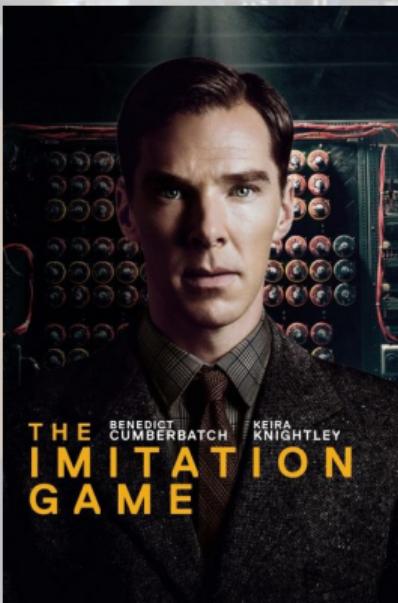




A PANORAMA ON CLASSICAL CRYPTOGRAPHY

Benoît Viguier

WHAT IS CRYPTOGRAPHY?



WHAT IS CRYPTOGRAPHY?



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

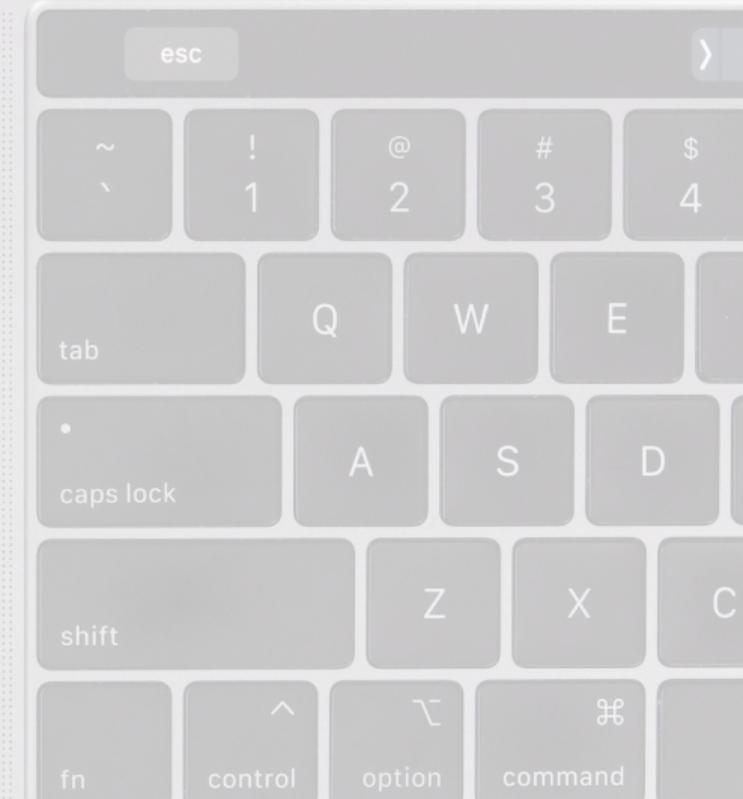
WHAT DO WE WANT TO PROTECT?

The image shows a screenshot of an Amazon website. At the top, there's a navigation bar with icons for Apple, Safari, File, Edit, View, History, Bookmarks, Window, and Help. Below the bar, there are three colored dots (red, yellow, green) and standard browser navigation buttons (back, forward, search). The main header features the Amazon logo and a "Deliver to Australia" button. A search bar with the word "All" is positioned next to it. Below the header, there's a menu bar with links like "Customer Service", "Registry", "Gift Cards", and "Sell". The main content area has a large blue background with white text. On the left, there's a bulleted list: "Confidentiality", "Data Integrity", "Data origin authentication", and "Entity authentication". To the right, there are sections for "Shipping" and "Visit amazon to shop for m...".

- 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.

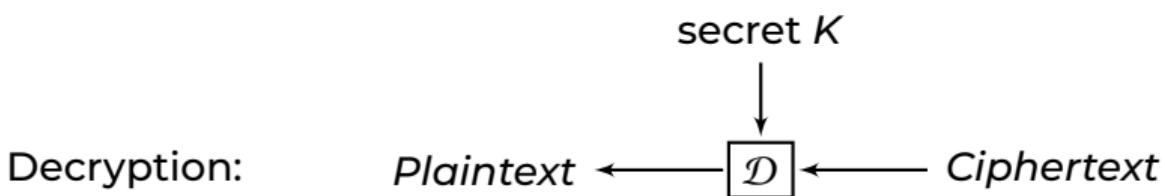
A word cloud visualization centered around WhatsApp, showing related concepts like encryption, WiFi, banking, security, and various digital identities and payment methods.

The most prominent words are:

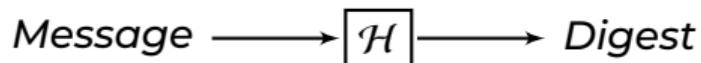
- WhatsApp
- encryption
- WiFi
- banking
- mailskey
- security
- WhatsApp
- DigiD
- internet
- AES
- banking
- 2FA
- Signal
- DigiD
- Certificate
- Signature
- Yubikey
- GPG
- bluetooth
- TLS1.3
- payment
- internet
- Paypal
- End-to-end
- WPA
- Faceld
- WiFi
- AES
- blueetooth
- messages
- CoronaCheck
- bitcoins

CRYPTO 101.

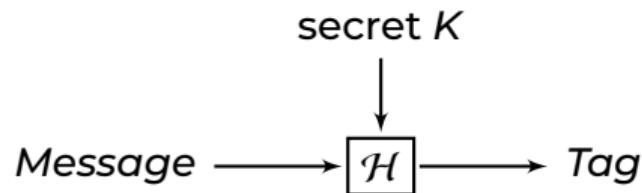
Symmetric encryption scheme



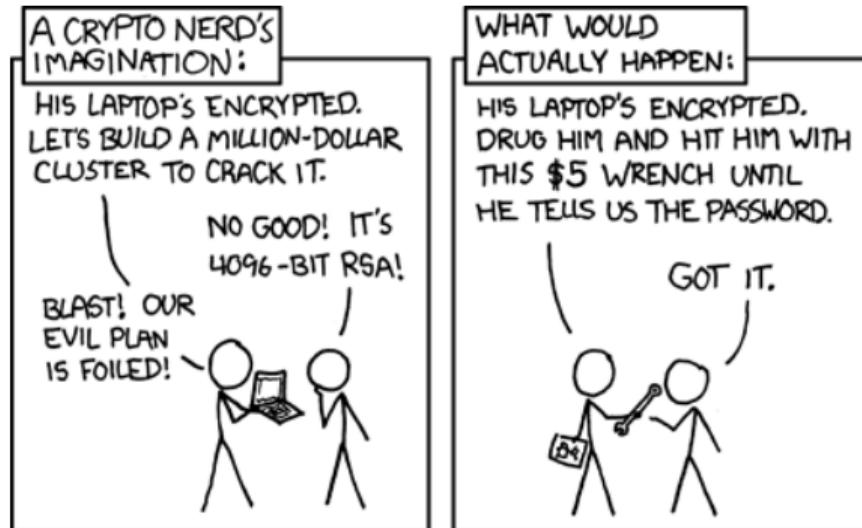
Hashing function



Message Authentication Code (MAC)



WHAT MY THESIS IS ABOUT.



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

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

The background of the slide features a photograph of Gimli the Dwarf from the Lord of the Rings movies. He is shown from the chest up, wearing his characteristic dark armor with gold accents and a tall black helmet. He has a long, bushy brown beard and is looking slightly to the left. A large two-handed axe is strapped to his back, with its head visible on the right side of the frame. The setting appears to be a rocky, mountainous landscape with trees in the background.

DESIGNING.

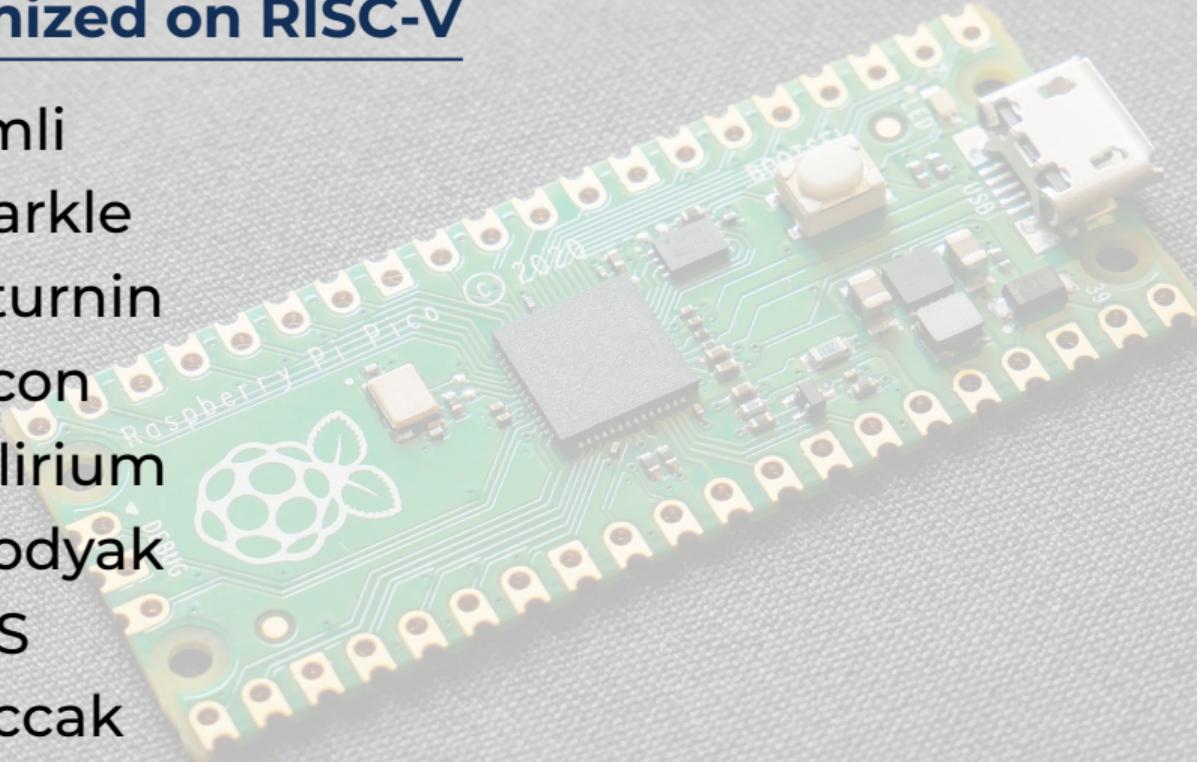
Gimli

- 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

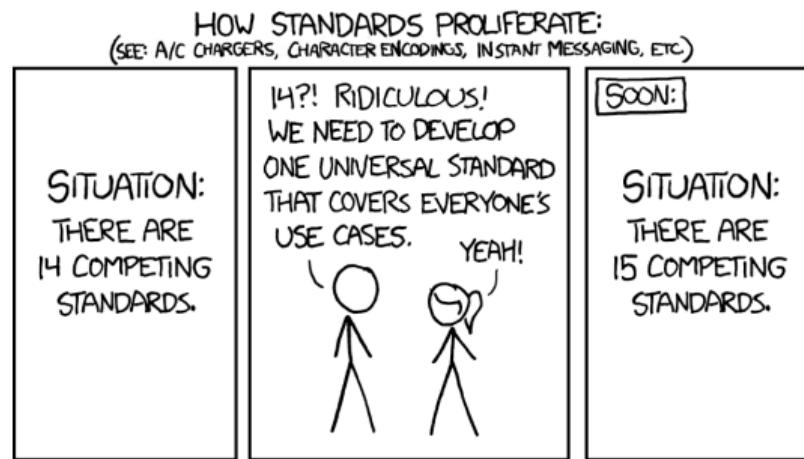
Using the Coq theorem prover, we verify:

- 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)
- 1st Draft in January 2017,
- Still not accepted...
- CFRG is very slow.



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

Thank you for your attention.

