ELCA for

BLACK ALPS

2018.05.29

Chiffrement des données

Un exemple de compromis entre sécurité et utilisabilité

Jean-Luc Beuchat

Why we Encrypt?

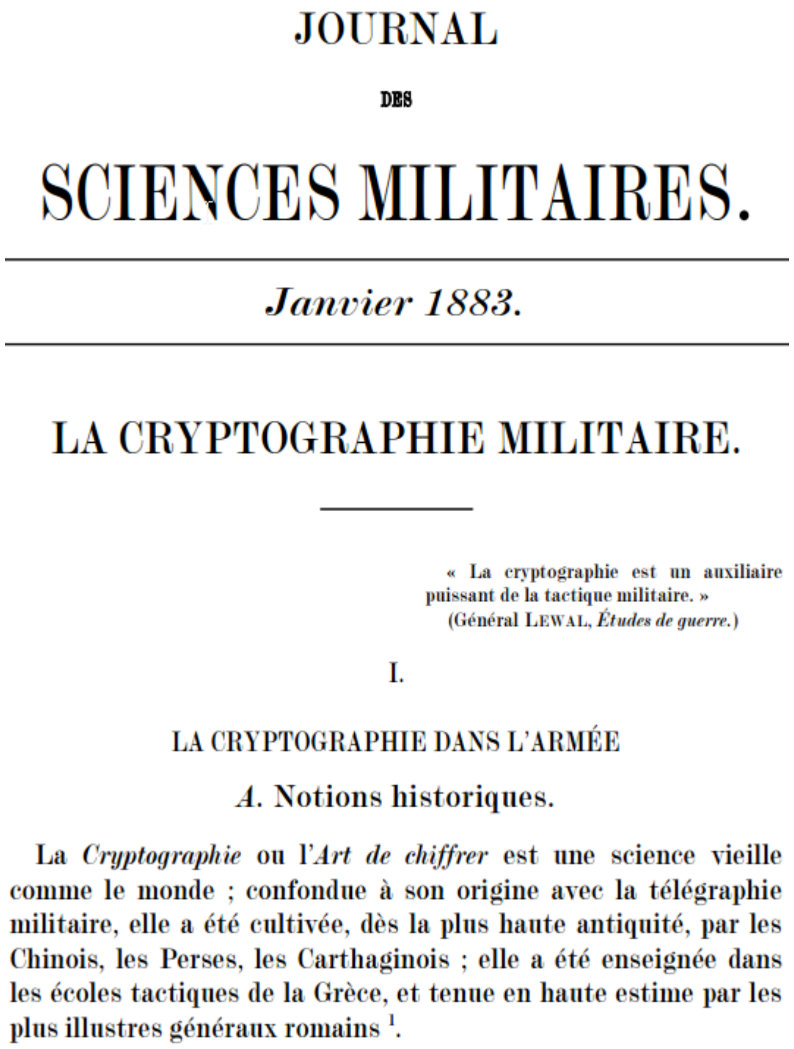
The Telegraph (August 22, 2008) – **Data on 130,000 criminals lost**

«The loss of the details, which were stored on an unencypted computer memory stick, has raised fears that the taxpayer may now face a multi-million pound compensation bill from criminals whose safety may have been compromised and police informants who could be at risk of reprisals. »

The Guardian (February 8, 2015) – **HSBC Files**

«HSBC files show how Swiss bank helped clients dodge taxes and hide millions. Data in massive cache of leaked secret bank account files lifts lid on questionable practices at subsidiary of one of world's biggest financial institutions.»

How Does Encryption Work?



JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

> « La cryptographie est un auxiliaire puissant de la tactique militaire. »
> (Général LEWAL, *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains[1].

- Done by scrambling your data
- Kerckhoffs's principle
  - The system must not require secrecy…
  - …and can be stolen by the enemy without causing trouble

Caveats

- Only as strong as your key
- Programmers are human (e.g. E-Fail, Heartbleed, etc.)
- Standardized back door (Dual_EC_DRBG)

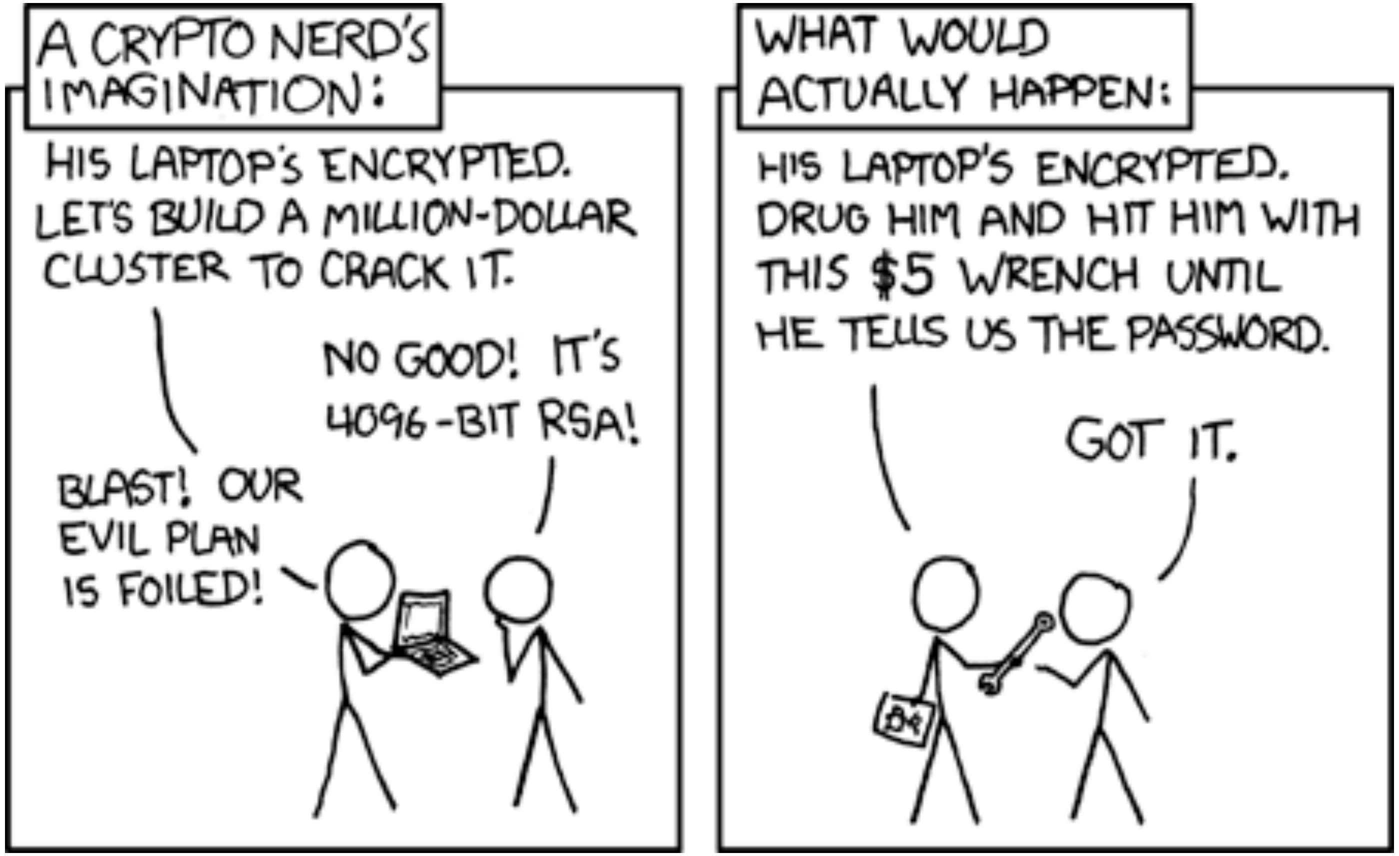

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Image retrieved from https://xkcd.com/538/

Use Case #1 – Disk Encryption

Pre-boot authentication

Protects data at rest

Pre-boot authentication

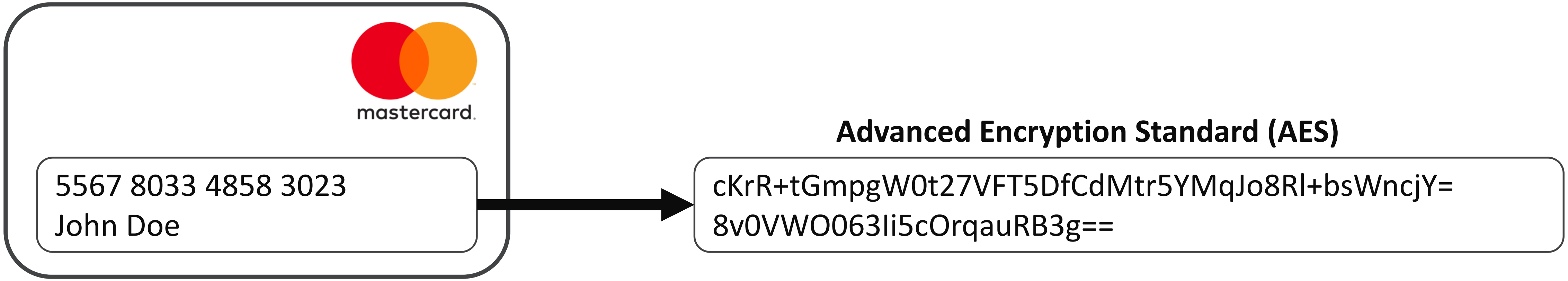
Only as strong as your password

Management

Evil maid attack

Image retrieved from https://mintzit.com/present-data-theft-with-full-disk-encryption/

Use Case #2 – Database Encryption



5567 8033 4858 3023
John Doe

Advanced Encryption Standard (AES)

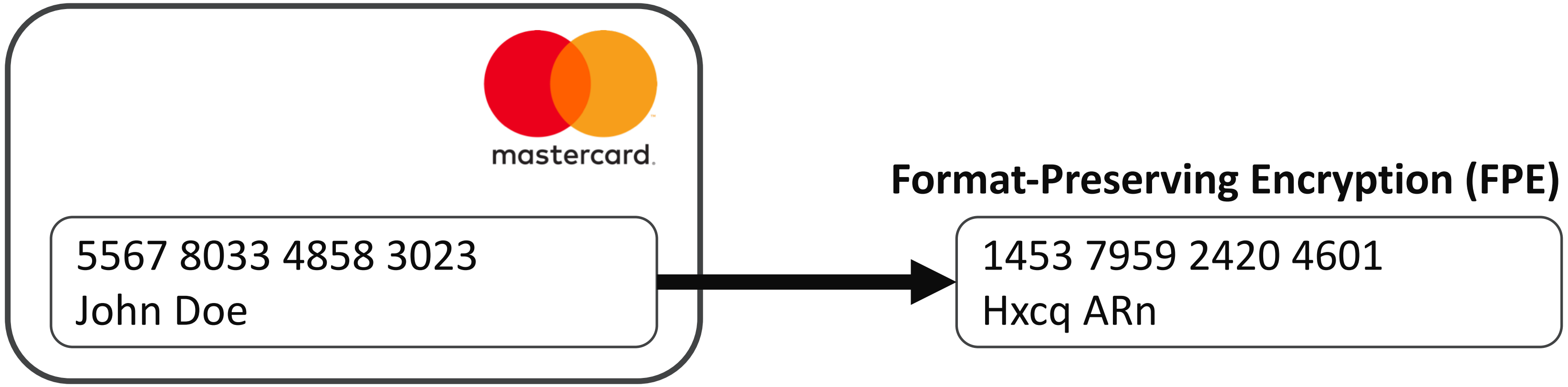
cKrR+tGmpgW0t27VFT5DfCdMtr5YMqJo8Rl+bsWncjY=
8v0VWO063Ii5cOrqauRB3g==

Standard

AES-NI

In-place encryption

Use Case #2 – Database Encryption



mastercard

5567 8033 4858 3023
John Doe

Format-Preserving Encryption (FPE)

1453 7959 2420 4601
Hxcq ARn

In-place encryption

Standard

Security

Implementation

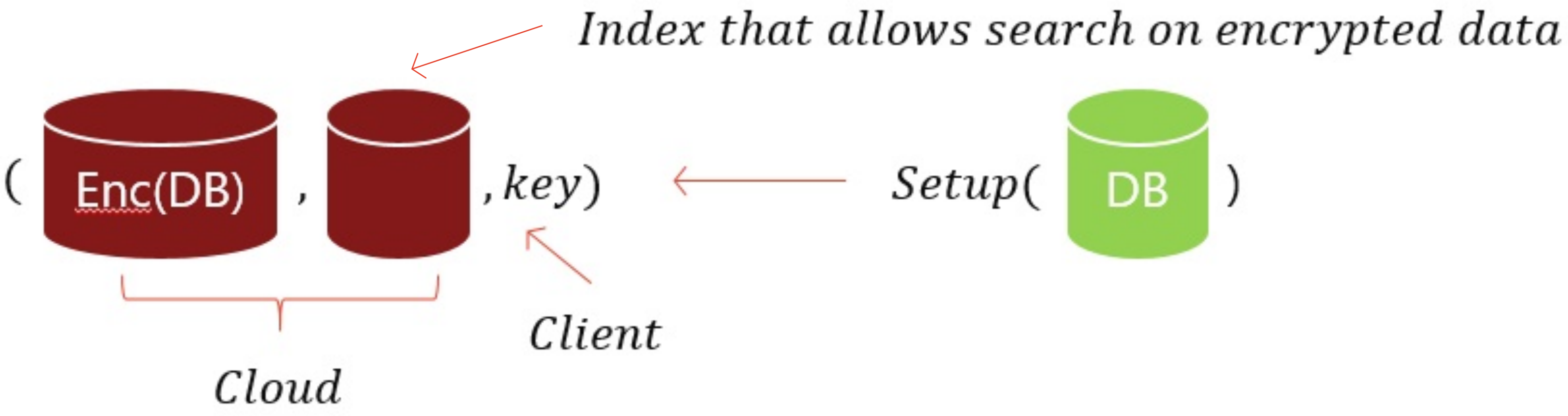
Use Case #3 – Searchable Encryption

Who is playing chess?

Name	Age	Hobby
sfR2Mpjut61/IrRhe++bNw==	S2331Qi4xbzU6IxI+Jtrqw==	HjhyqzzKgz7VhSqgq+DdLA==
9Z6b4vP7nVWAGKi3gAN0hg==	y1rvlToW+zvzgBzZ+HaJtw==	K5LCsBm2PzVu7LBsYXrHpQ==
aEo+liL64v6pialvLfUKIw==	43Mh1GoQ6aZFuogzptdhEQ==	fYViCqGjwd3CCi6y0wJVSQ==

Who is older than 20 and collecting stamps?

Use Case #3 – Searchable Encryption



Encrypted data in the cloud

Boolean queries

Wildcard search

Range search

Rewrite your search engine

Encrypted index (size, update, etc.)

Security

Conclusion

MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
To complete the log-in procedure, stare directly at the sun.
© Scott Adams, Inc./Dist. by UFS, Inc.

Use Case #3 – Searchable Encryption

The Albatross did follow

Document #1

But no sweet bird

Forged Document #1

But no sweet bird did follow

Document #2

sweet Bird did follow

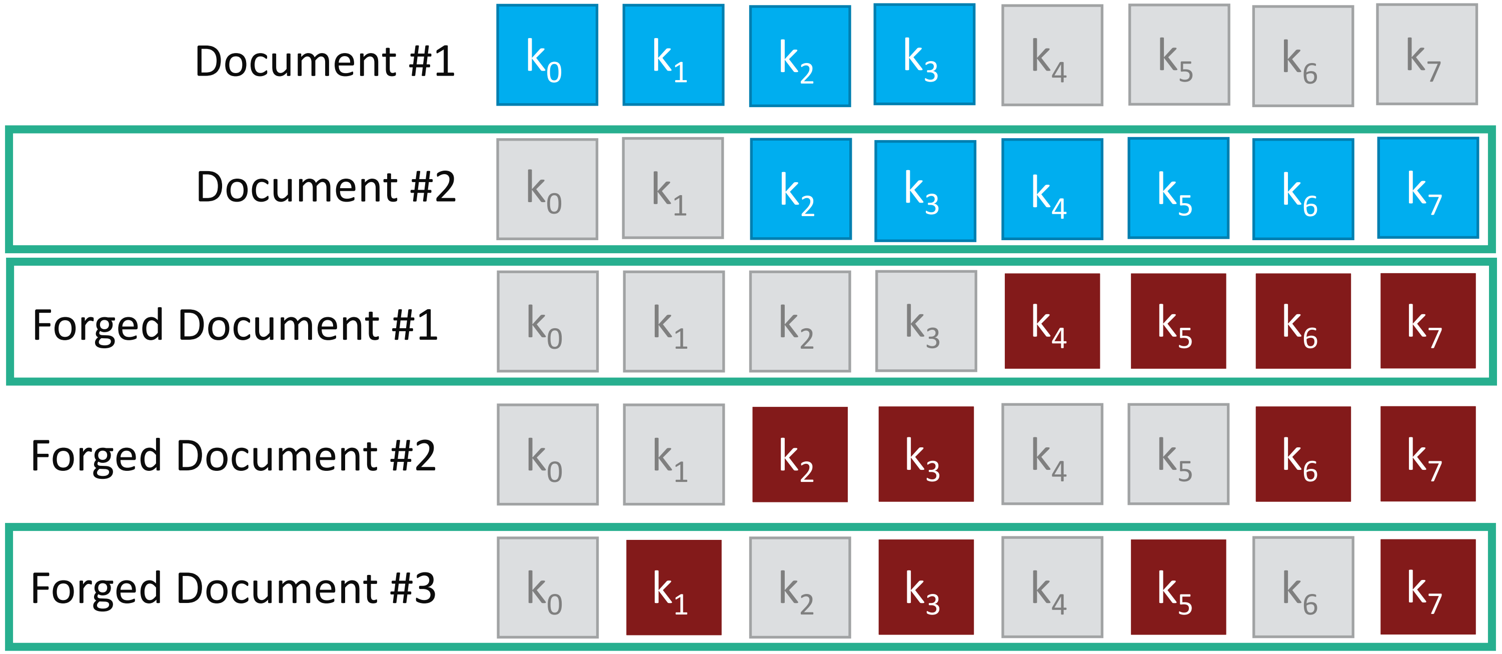
Forged Document #2

no Albatross bird follow

Forged Document #3

Use Case #3 – Searchable Encryption

Query: find all documents containing $\mathbf{k_5}$



Document #1	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7
Document #2	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7
Forged Document #1	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7
Forged Document #2	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7
Forged Document #3	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7

But no sweet bird

Forged Document #1

sweet Bird did follow

Forged Document #2

no Albatross bird follow

Forged Document #3