Filesystem encryption

Pascal Engélibert

University of Bordeaux

8 April 2024

Summary

Summary

- Why to encrypt
- How to encrypt
- Attacks
- Defences
- Implementations

Why to encrypt

You have something to hide

If your drive or computer is stolen, you want to protect :

- Passwords, private keys
- Sensitive, personal data
- Evidence
- Root-me solutions

How to encrypt

What properties are needed ?

- Confidentiality
- Fast random access
- Small space waste

How to encrypt

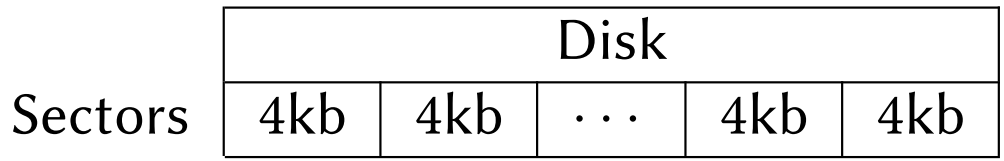
What properties are needed ?

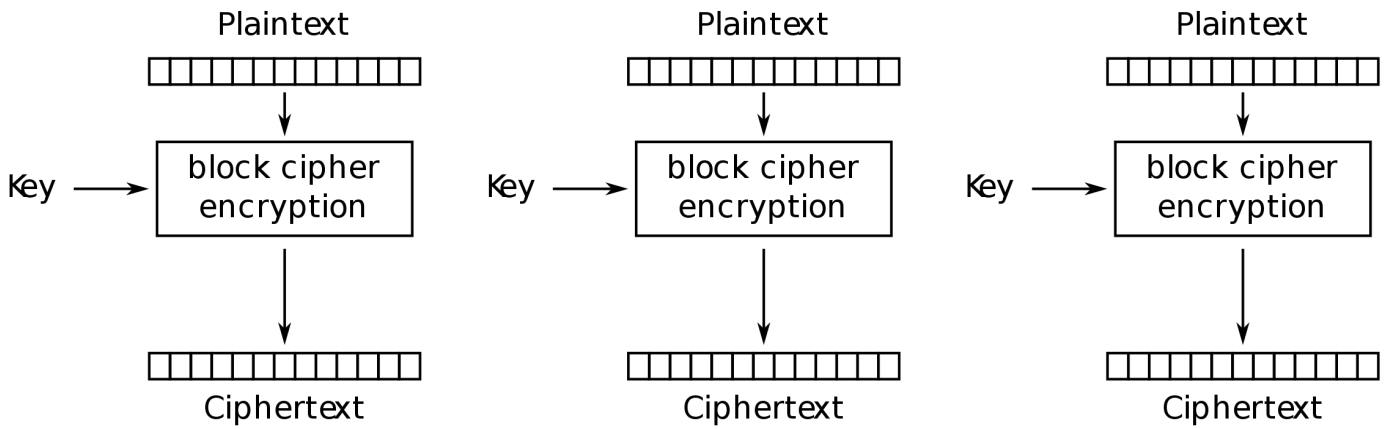
- ➢ Confidentiality
- ➢ Fast random access
  $\Longrightarrow$ use small blocks ! (physical sectors : 4kb)
- ➢ Small space waste
  $\Longrightarrow$ do not store additional metadata for sectors

	Disk				
Sectors	4kb	4kb	$\cdots$	4kb	4kb

How to encrypt

What about ECB ?



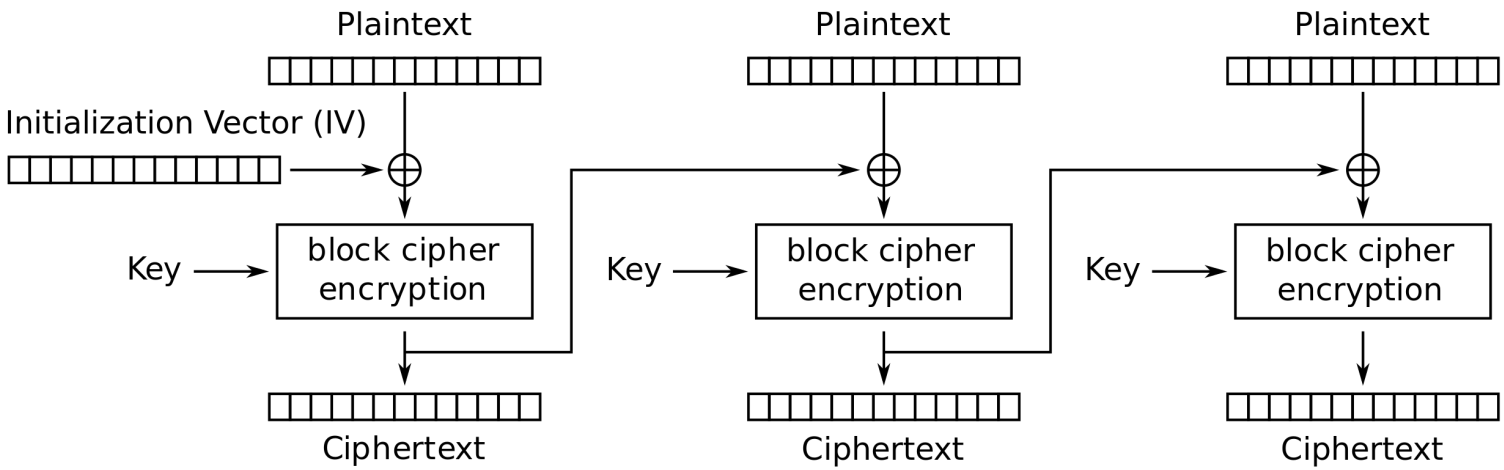


Electronic Codebook (ECB) mode encryption

How to encrypt

We need Initialization Vectors!

	Disk					
Sectors	4kb			4kb		4kb
Blocks	128b	$\cdots$	128b	$\cdots$	$\cdots$	$\cdots$
IVs	$IV(0)$			$IV(1)$		$IV(N-1)$



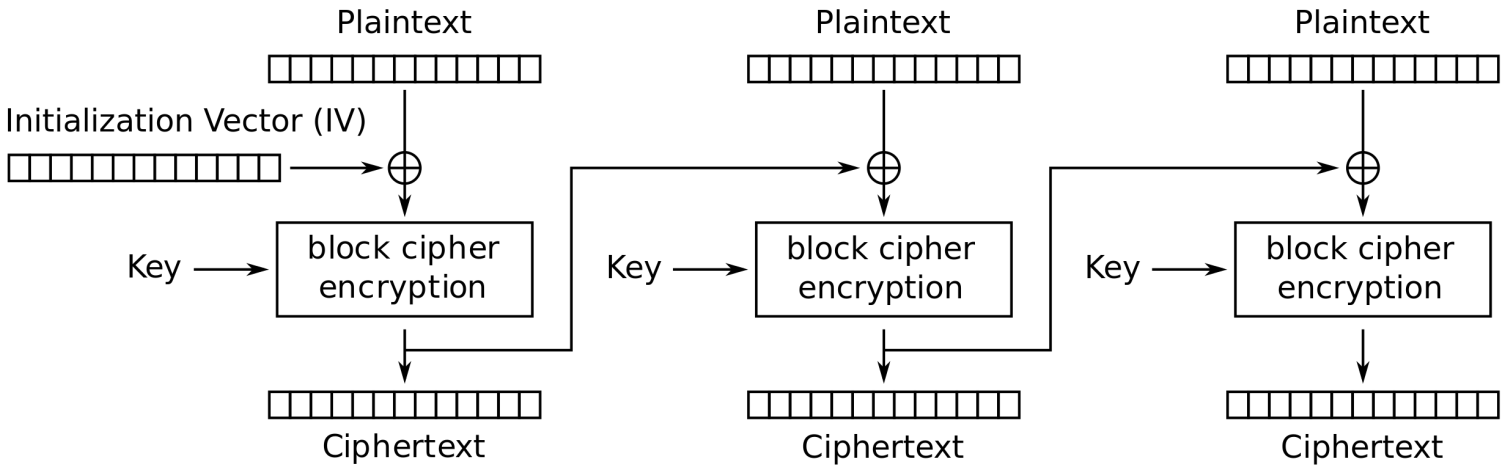
Cipher Block Chaining (CBC) mode encryption

How to encrypt

We need Initialization Vectors!

	Disk						
Sectors	4kb			4kb			4kb
Blocks	128b	$\cdots$	128b	$\cdots$	$\cdots$		$\cdots$
IVs	$IV(0)$			$IV(1)$			$IV(N-1)$

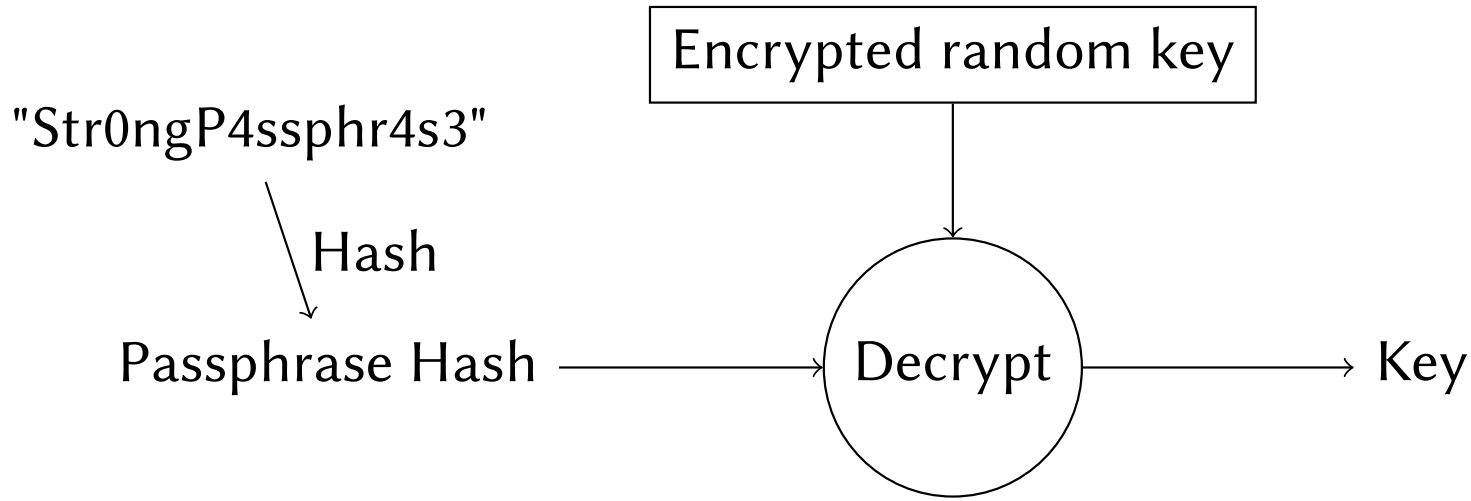
ESSIV (Encrypted Sector Salt IV) : $IV(n) = E(H(K), n)$



Cipher Block Chaining (CBC) mode encryption

How to encrypt

Key management

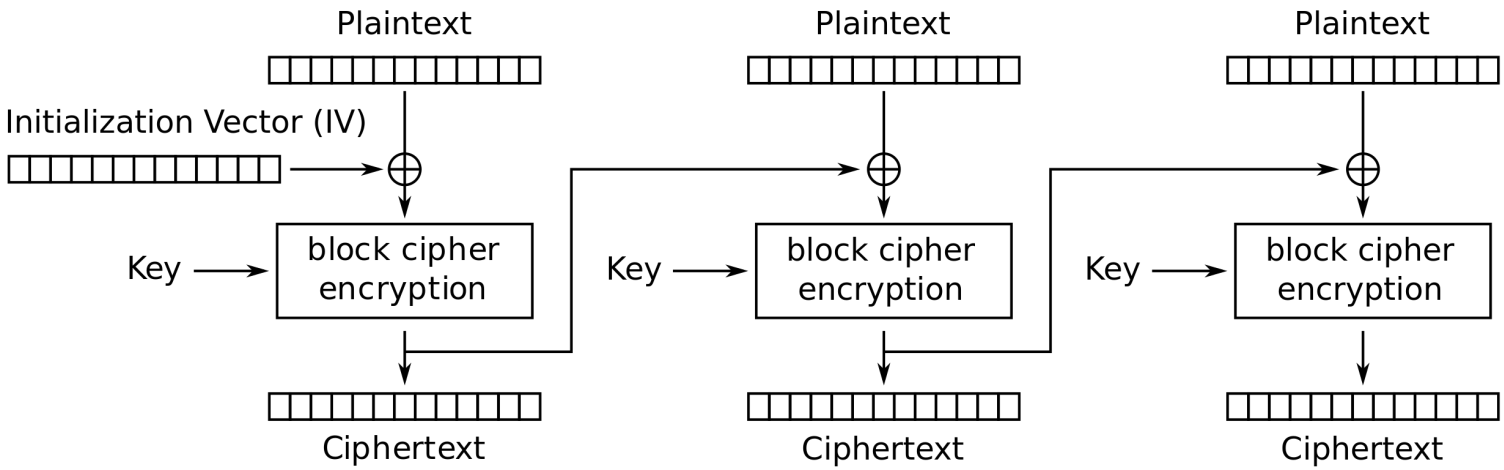


- Multiple key slots
- Key derivation algorithm (Argon2)
- You can change your passphrase without changing the key (changing the key means re-encrypting all the filesystem)

Attacks

Malleability

CBC does not ensure integrity nor authenticity!
If you know a block's plaintext, you can control subsequent blocks.



Cipher Block Chaining (CBC) mode encryption

Attacks

Back to the Past

An attacker can restore a previous state of an entire sector.

Attacks

The Evil Maid Attack

Oops, the maid installed a keylogger!

- ➢ Rootkit
- ➢ Hardware keylogger
- ➢ Firmware replacement

Attacks

Force

The encryption metadata are in clear!
Hence an attacker knows you are using encryption.

- ➢ It can be illegal to refuse to disclose a password.
- ➢ An attacker can torture you to obtain the password.

Kill switch

They are coming to take your drives!

- Remove the key stored on the drive
- Remove it from the RAM
- What about the drive's cache?
- What about key backups?
- You may be accused of evidence destruction.

Kill switch

They already took your drives!

If the wrong passphrase is entered, the key is removed.

- ➢ They can make a cold backup.
- ➢ They can detect the trap.
- ➢ They can use their own decryption software.

Plausible denialability

Pretend there is nothing

Yes, my hard disk is empty, and so what ?

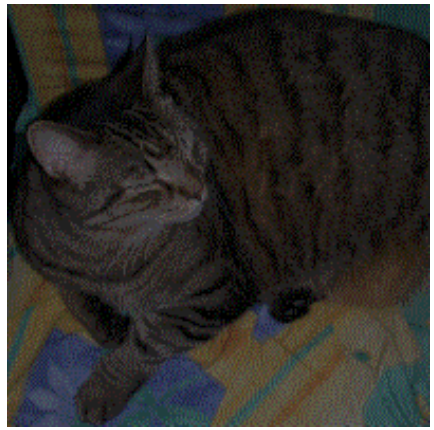
- ➢ Where do you store the key and metadata ?
- ➢ No metadata means weaker security.
- ➢ They may not believe you.
- ➢ What if they notice you write "random" bytes in "empty" regions ?

Plausible denialability

Pretend there is something else (steganography)

Yes, I have a hard disk full of random pictures, and so what ?

(a) Original



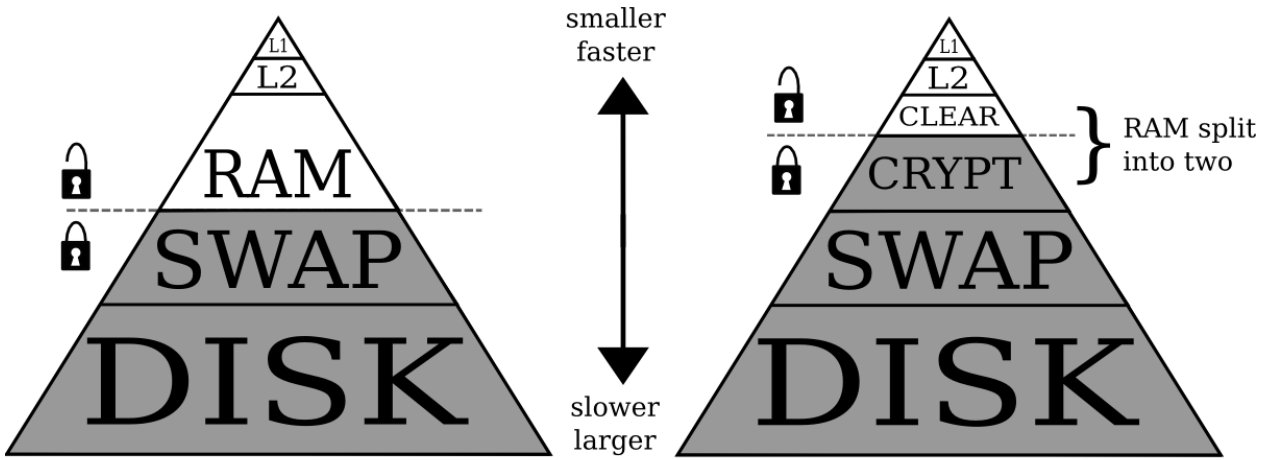
(b) Extracted

- ➢ Poor capacity and performance.
- ➢ How do you hide the steganography software ?
- ➢ Where do you store the key and metadata ?
- ➢ They may not believe you.

RAM encryption

CryptKeeper

Experimental : keep most of the RAM encrypted
(mitigates Cold Boot Attacks)



Typical memory hierarchy with FDE.

Cryptkeeper memory hierarchy.

Drawback : up to 9× slower
still research

Implementations

On Linux

LUKS

Linux Unified Key Setup

Implementations

On Windows

BitLocker (Microsoft)

VeraCrypt (free software)

Sources & Credits

- Cryptsetup Documentation
- Can the NSA break BitLocker? (Schneier on Security)
- CryptKeeper, 2009
- Are cold boot attacks still feasible: a case study on Raspberry Pi with stacked memory, 2021
- Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors, 2017
- Hard Disk Drive : Hannes Grobe, CC BY-SA 4.0, [link]
- Steganography examples : Cyp, CC BY-SA 3.0, [cat] [tree]
- Evil Maid : The Handmaid's Tale (Hulu series)
- Font : Linux Libertine