v02enc:
What I learned while rolling my own crypto.

Introduction

Introduction

Introduction

Kenny aka. Yahe

Introduction

Kenny aka. Yahe

Senior Application Security Engineer @ Staffbase

DPO & CISO @ Inter.link

Introduction

Kenny aka. Yahe

Senior Application Security Engineer @ Staffbase

DPO & CISO @ Inter.link

Maintainer of ~~https://github.com/SysEleven/shared-secrets~~
https://github.com/yahesh/shared-secrets

Introduction

Kenny aka. Yahe

Senior Application Security Engineer @ Staffbase

DPO & CISO @ Inter.link

Maintainer of ~~https://github.com/SysEleven/shared-secrets~~
https://github.com/yahesh/shared-secrets

Maintainer of **https://github.com/calcpw/calcpw.ios**
https://github.com/calcpw/calcpw.php

Introduction

Kenny aka. Yahe

Senior Application Security Engineer @ Staffbase

DPO & CISO @ Inter.link

Maintainer of ~~https://github.com/SysEleven/shared-secrets~~
https://github.com/yahesh/shared-secrets

Maintainer of **https://github.com/calcpw/calcpw.ios**
https://github.com/calcpw/calcpw.php

Maintainer of **https://github.com/nextcloud/encryption-recovery-tools**

History

History

History

Shared-Secrets

→ encryption format **v00** to **symmetrically** encrypt content for a **single** recipient

→ encryption format **v01** to **hybridly** encrypt content for **multiple** recipients

History

Shared-Secrets

→ encryption format **v00** to **symmetrically** encrypt content for a **single** recipient

→ encryption format **v01** to **hybridly** encrypt content for **multiple** recipients

Challenge:

→ store configuration files with credentials and other secrets in Git / Mercurial repositories

→ update existing configuration files without access to key material of all previous recipients

History

Shared-Secrets

→ encryption format **v00** to **symmetrically** encrypt content for a **single** recipient

→ encryption format **v01** to **hybridly** encrypt content for **multiple** recipients

Challenge:

→ store configuration files with credentials and other secrets in Git / Mercurial repositories

→ update existing configuration files without access to key material of all previous recipients

Solution:

→ encryption format **v02** to **symmetrically** encrypt content for **multiple** recipients

→ introduce update method while keeping most of the file header untouched

Learnings

Learnings

Learnings

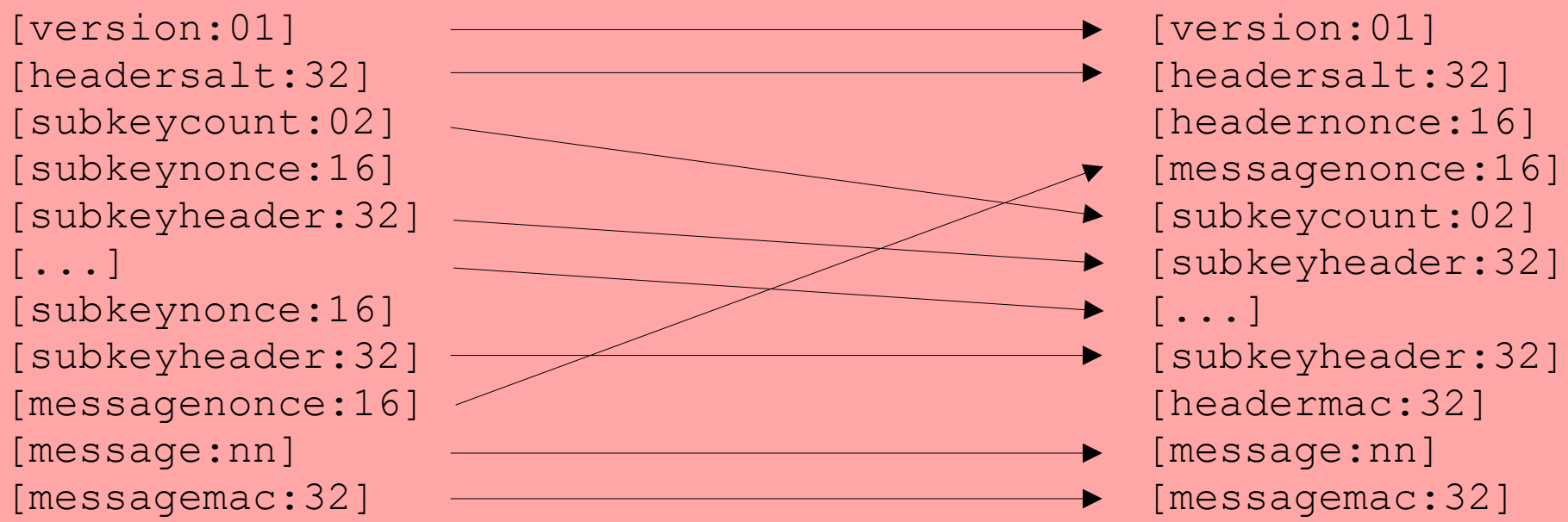
```
[version:01]
[headersalt:32]
[subkeycount:02]
[subkeynonce:16]
[subkeyheader:32]
[...]
[subkeynonce:16]
[subkeyheader:32]
[messagenonce:16]
[message:nn]
[messagemac:32]
```

Learnings

```
[version:01]
[headersalt:32]
[subkeycount:02]
[subkeynonce:16]
[subkeyheader:32]
[...]
[subkeynonce:16]
[subkeyheader:32]
[messagenonce:16]
[message:nn]
[messagemac:32]
```

```
[version:01]
[headersalt:32]
[headernonce:16]
[messagenonce:16]
[subkeycount:02]
[subkeyheader:32]
[...]
[subkeyheader:32]
[headermac:32]
[message:nn]
[messagemac:32]
```

Learnings


[version:01]
[headersalt:32]
[subkeycount:02]
[subkeynonce:16]
[subkeyheader:32]
[...]
[subkeynonce:16]
[subkeyheader:32]
[messagenonce:16]
[message:nn]
[messagemac:32]
[version:01]
[headersalt:32]
[headernonce:16]
[messagenonce:16]
[subkeycount:02]
[subkeyheader:32]
[...]
[subkeyheader:32]
[headermac:32]
[message:nn]
[messagemac:32]

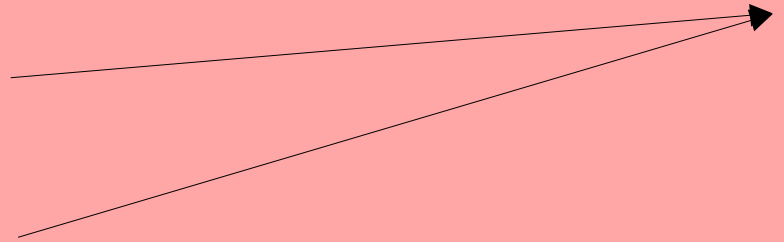
Learnings

```
[version:01]
[headersalt:32]
[subkeycount:02]
[subkeynonce:16]
[subkeyheader:32]
[...]
[subkeynonce:16]
[subkeyheader:32]
[messagenonce:16]
[message:nn]
[messagemac:32]
```

```
[version:01]
[headersalt:32]
[headernonce:16]
[messagenonce:16]
[subkeycount:02]
[subkeyheader:32]
[...]
[subkeyheader:32]
[headermac:32]
[message:nn]
[messagemac:32]
```

Learnings

```
[version:01]
[headersalt:32]
[subkeycount:02]
[subkeynonce:16]
[subkeyheader:32]
[...]
[subkeynonce:16]
[subkeyheader:32]
[messagenonce:16]
[message:nn]
[messagemac:32]
```



```
[version:01]
[headersalt:32]
[headernonce:16]
[messagenonce:16]
[subkeycount:02]
[subkeyheader:32]
[...]
[subkeyheader:32]
[headermac:32]
[message:nn]
[messagemac:32]
```

Learnings

```
[version:01]
[headersalt:32]
[subkeycount:02]
[subkeynonce:16]
[subkeyheader:32]
[...]
[subkeynonce:16]
[subkeyheader:32]
[messagenonce:16]
[message:nn]
[messagemac:32]
```

```
[version:01]
[headersalt:32]
[headernonce:16]
[messagenonce:16]
[subkeycount:02]
[subkeyheader:32]
[...]
[subkeyheader:32]
[headermac:32]
[message:nn]
[messagemac:32]
```

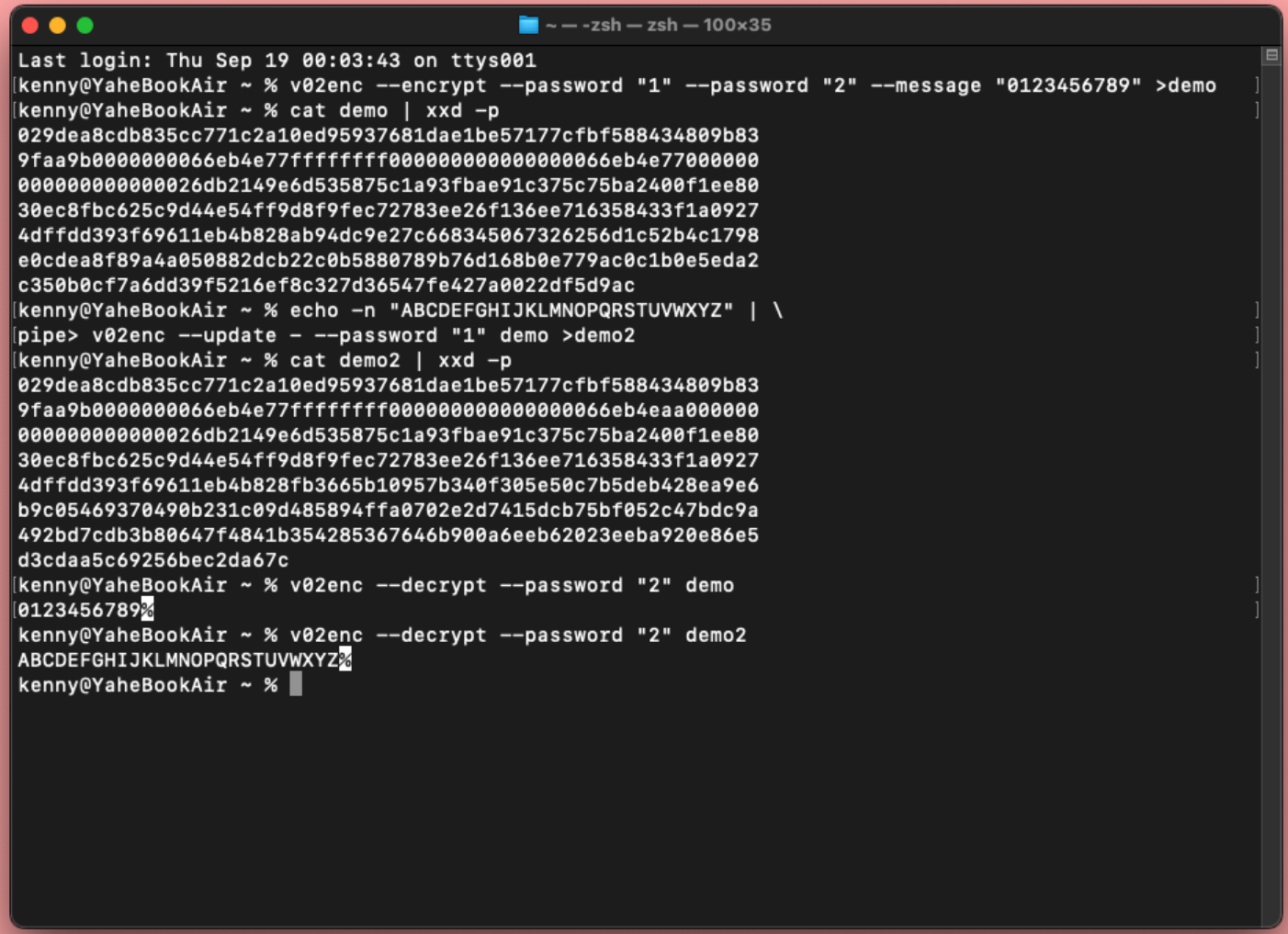
Learnings

```
[version:01]
[headersalt:32]
[subkeycount:02]
[subkeynonce:16]
[subkeyheader:32]
[...]
[subkeynonce:16]
[subkeyheader:32]
[messagenonce:16]
[message:nn]
[messagemac:32]
```

```
[version:01]
[headersalt:32]
[headernonce:16]
[messagenonce:16]
[subkeycount:02]
[subkeyheader:32]
[...]
[subkeyheader:32]
[headermac:32]
[message:nn]
[messagemac:32]
```

Learnings

Learnings


~ — -zsh — zsh — 100×35
Last login: Thu Sep 19 00:03:43 on ttys001
kenny@YaheBookAir ~ % v02enc --encrypt --password "1" --password "2" --message "0123456789" >demo
kenny@YaheBookAir ~ % cat demo | xxd -p
029dea8cdb835cc771c2a10ed95937681dae1be57177cfbf588434809b83
9faa9b0000000066eb4e77ffffffff00000000000000066eb4e77000000
000000000000026db2149e6d535875c1a93fbae91c375c75ba2400f1ee80
30ec8fbc625c9d44e54ff9d8f9fec72783ee26f136ee716358433f1a0927
4dffdd393f69611eb4b828ab94dc9e27c668345067326256d1c52b4c1798
e0cdea8f89a4a050882dcb22c0b5880789b76d168b0e779ac0c1b0e5eda2
c350b0cf7a6dd39f5216ef8c327d36547fe427a0022df5d9ac
kenny@YaheBookAir ~ % echo -n "ABCDEFGHIJKLMNOPQRSTUVWXYZ" | \
pipe> v02enc --update - --password "1" demo >demo2
kenny@YaheBookAir ~ % cat demo2 | xxd -p
029dea8cdb835cc771c2a10ed95937681dae1be57177cfbf588434809b83
9faa9b0000000066eb4e77ffffffff00000000000000066eb4eaa000000
000000000000026db2149e6d535875c1a93fbae91c375c75ba2400f1ee80
30ec8fbc625c9d44e54ff9d8f9fec72783ee26f136ee716358433f1a0927
4dffdd393f69611eb4b828fb3665b10957b340f305e50c7b5deb428ea9e6
b9c05469370490b231c09d485894ffa0702e2d7415dcb75bf052c47bdc9a
492bd7cdb3b80647f4841b354285367646b900a6eeb62023eeba920e86e5
d3cdaa5c69256bec2da67c
kenny@YaheBookAir ~ % v02enc --decrypt --password "2" demo
0123456789%
kenny@YaheBookAir ~ % v02enc --decrypt --password "2" demo2
ABCDEFGHIJKLMNOPQRSTUVWXYZ%
kenny@YaheBookAir ~ %

Learnings

```
[version:01]
[headersalt:32]
[headernonce:16]
[messagenonce:16]
[subkeycount:02]
[subkeyheader:32]
[subkeyheader:32]
[headermac:32]
[message:nn]
[messagemac:32]
```

Learnings

```
[version:01]       02
[headersalt:32]    9dea8cdb835cc771c2a10ed95937681dae1be57177cfbf588434809b839faa9b
[headernonce:16]   0000000066eb4e77ffffffff00000000
[messagenonce:16]  0000000066eb4e7700000000000000000
[subkeycount:02]   0002
[subkeyheader:32]  6db2149e6d535875c1a93fbae91c375c75ba2400f1ee8030ec8fbc625c9d44e5
[subkeyheader:32]  4ff9d8f9fec72783ee26f136ee716358433f1a09274dffdd393f69611eb4b828
[headermac:32]     ab94dc9e27c668345067326256d1c52b4c1798e0cdea8f89a4a050882dcb22c0
[message:nn]       b5880789b76d168b0e77
[messagemac:32]    9ac0c1b0e5eda2c350b0cf7a6dd39f5216ef8c327d36547fe427a0022df5d9ac
```

Learnings

```
[version:01]       02
[headersalt:32]    9dea8cdb835cc771c2a10ed95937681dae1be57177cfbf588434809b839faa9b
[headernonce:16]   0000000066eb4e77ffffffff00000000
[messagenonce:16]  0000000066eb4eaa0000000000000000
[subkeycount:02]   0002
[subkeyheader:32]  6db2149e6d535875c1a93fbae91c375c75ba2400f1ee8030ec8fbc625c9d44e5
[subkeyheader:32]  4ff9d8f9fec72783ee26f136ee716358433f1a09274dffdd393f69611eb4b828
[headermac:32]     fb3665b10957b340f305e50c7b5deb428ea9e6b9c05469370490b231c09d4858
[message:nn]       94ffa0702e2d7415dcb75bf052c47bdc9a492bd7cdb3b80647f4
[messagemac:32]    841b354285367646b900a6eeb62023eeba920e86e5d3cdaa5c69256bec2da67c
```

Learnings

```
[version:01]       02
[headersalt:32]    9dea8cdb835cc771c2a10ed95937681dae1be57177cfbf588434809b839faa9b
[headernonce:16]   0000000066eb4e77ffffffff00000000
[messagenonce:16]  0000000066eb4eaa0000000000000000
[subkeycount:02]   0002
[subkeyheader:32]  6db2149e6d535875c1a93fbae91c375c75ba2400f1ee8030ec8fbc625c9d44e5
[subkeyheader:32]  4ff9d8f9fec72783ee26f136ee716358433f1a09274dffdd393f69611eb4b828
[headermac:32]     fb3665b10957b340f305e50c7b5deb428ea9e6b9c05469370490b231c09d4858
[message:nn]       94ffa0702e2d7415dcb75bf052c47bdc9a492bd7cdb3b80647f4
[messagemac:32]    841b354285367646b900a6eeb62023eeba920e86e5d3cdaa5c69256bec2da67c
```

Learnings

Learnings

~/github/v02enc — vi v02enc — zsh — 100×35

```
    # read the first byte to check if it contains the version byte
    $byte = fread($__INPUTS[$name][STREAM], strlen(VERSION_BYTE));
    if (false !== $byte) {
      # is the read value the version byte
      if (VERSION_BYTE === $byte) {
        # put the read byte in the input buffer
        $__INPUTS[$name][BUFFER] = $byte;

        # this was successful
        $result = true;
      } else {
        $line = "";

        # consume empty lines
        while (!input_eof($name) && (false !== $line) && (0 === strlen($line))) {
          $line = input_readln($name);

          # handle the byte that was initially read
          if (false !== $line) {
            $line = trim($byte.$line, "\n\r");
            $byte = "";
          }
        }

        # check if we found the armor header
        if (ARMOR_HEADER === $line) {
          $__INPUTS[$name][ARMOR] = true;

          # this was successful
          $result = true;
        }
      }
    }
  }
```

Learnings

~/github/v02enc — vi v02enc — zsh — 100×35

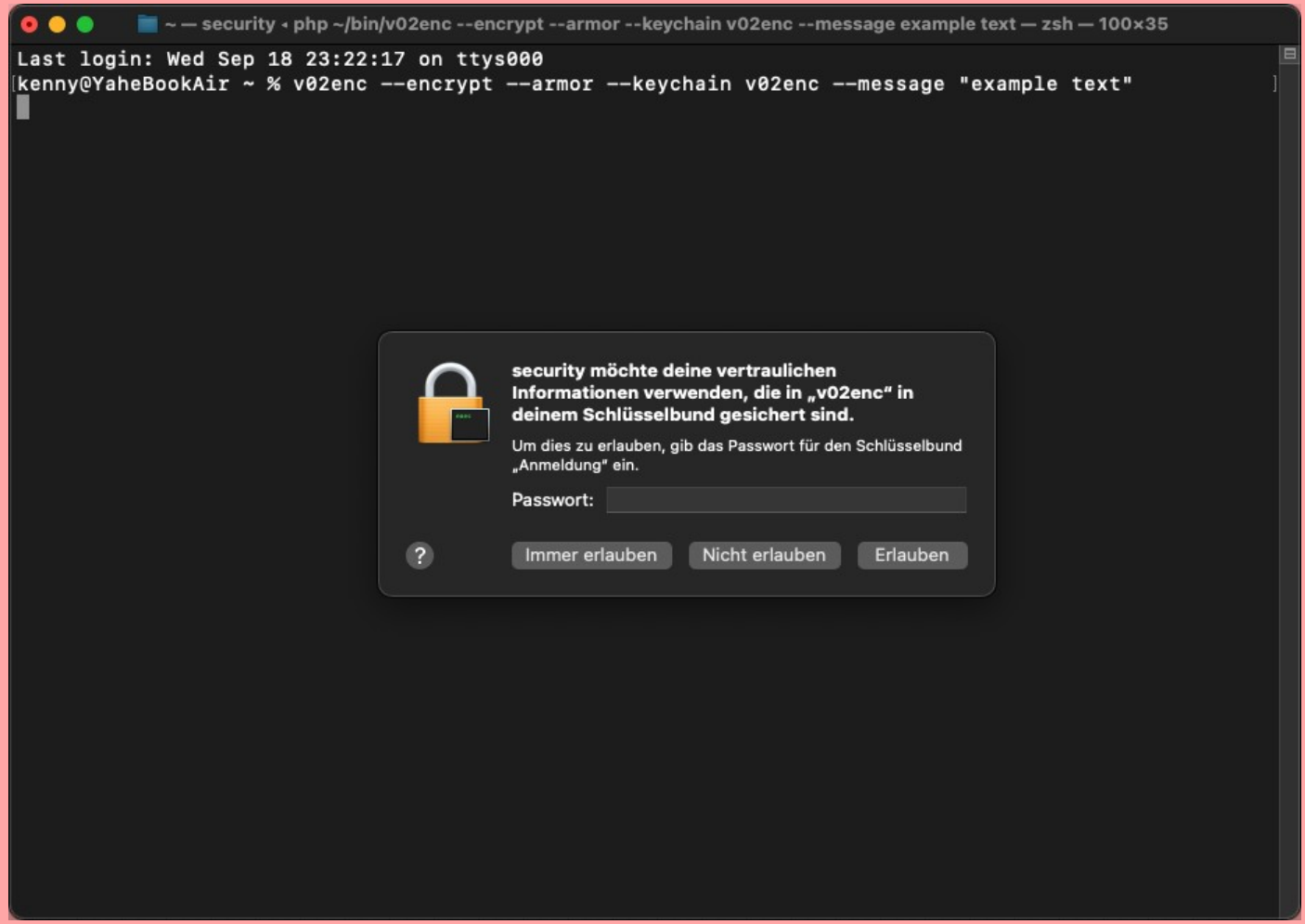
```
        if (input_isarmor($name)) {
          # read next line
          $tmp = input_readln($name);
          if (false !== $tmp) {
            # ignore empty line
            if (0 < strlen($tmp)) {
              # check if we found the armor footer
              if (0 === strcmp($tmp, ARMOR_FOOTER)) {
                # set the input to end-of-file
                $__INPUTS[$name][EOF] = true;
              } else {
                # decode the line
                $tmp = base64_decode($tmp, true);
                if (false !== $tmp) {
                  # the new block is enough to reach the $length
                  if (strlen($result)+strlen($tmp) >= $length) {
                    # how many bytes to take from the new block
                    $count = $length-strlen($result);

                    # write bytes to result
                    $result .= substr($tmp, 0, $count);

                    # update the input buffer
                    $__INPUTS[$name][BUFFER] = substr($tmp, $count);
                  } else {
                    $result .= $tmp;
                  }
                } else {
                  # decode errors have priority
                  $result = false;
                }
              }
            }
          } else {
```

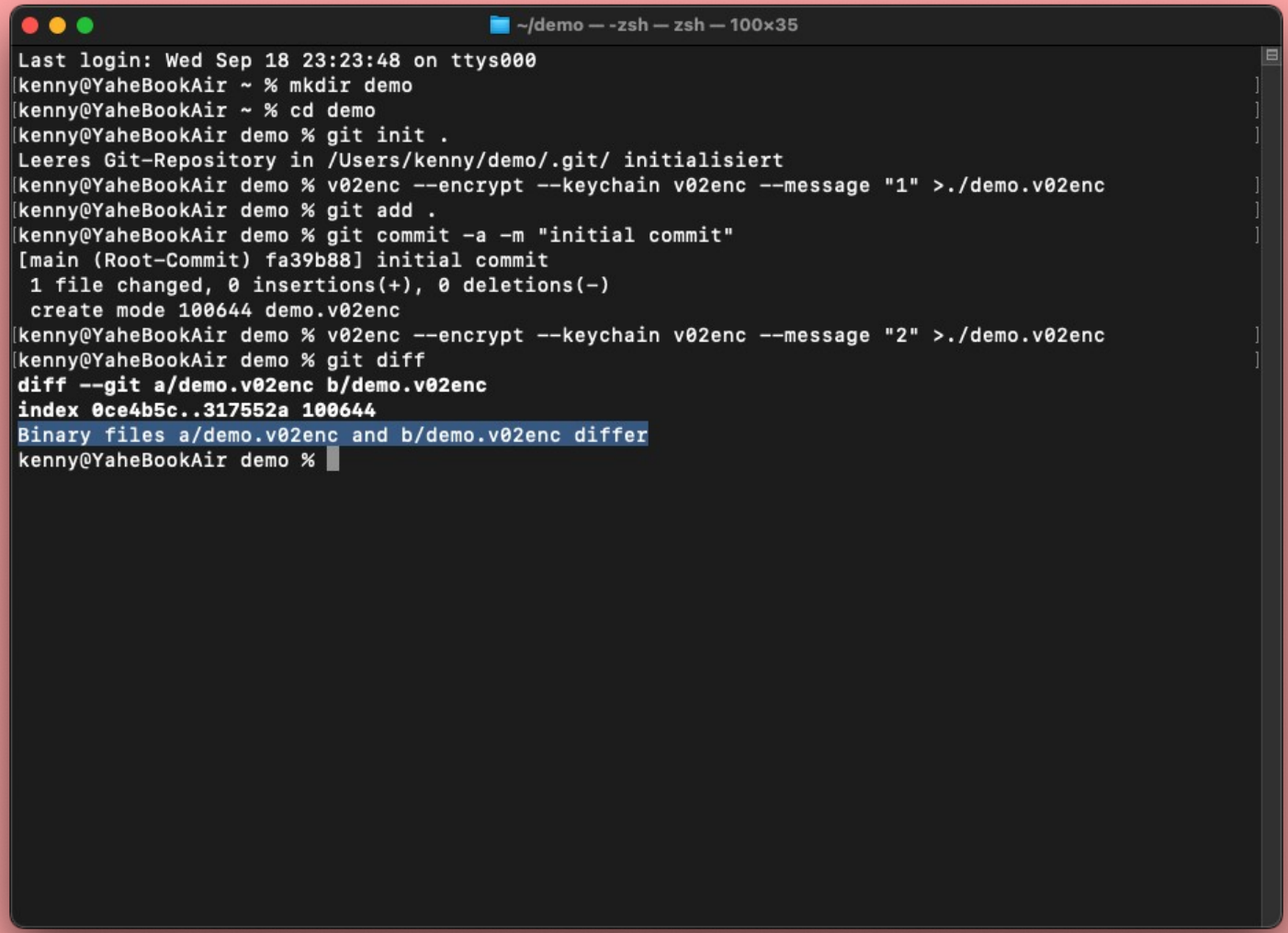
Learnings

Learnings

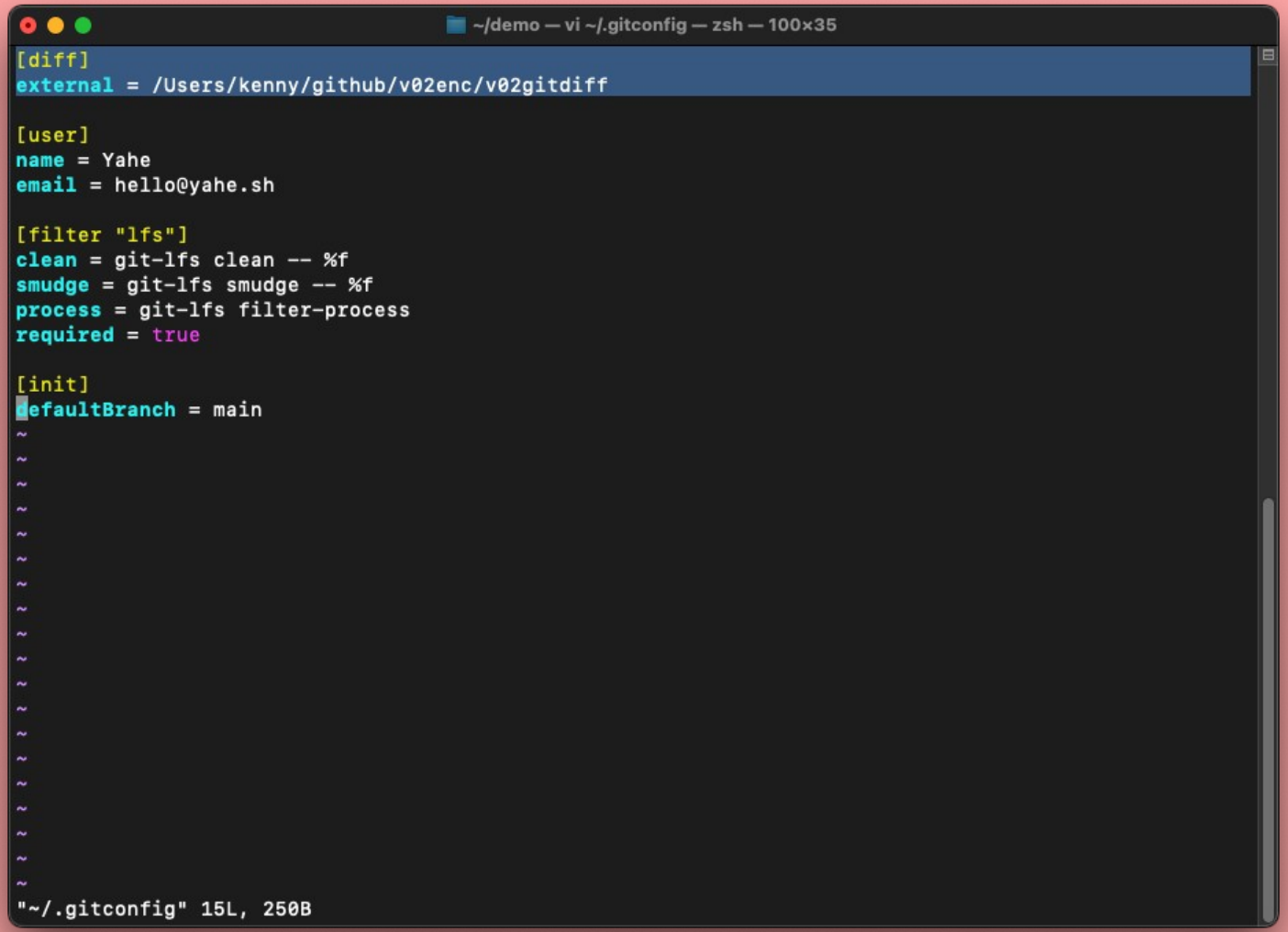

~ — security ‹ php ~/bin/v02enc --encrypt --armor --keychain v02enc --message example text — zsh — 100×35
Last login: Wed Sep 18 23:22:17 on ttys000
kenny@YaheBookAir ~ % v02enc --encrypt --armor --keychain v02enc --message "example text"
security möchte deine vertraulichen Informationen verwenden, die in „v02enc“ in deinem Schlüsselbund gesichert sind.
Um dies zu erlauben, gib das Passwort für den Schlüsselbund „Anmeldung“ ein.
Passwort:
?
Immer erlauben
Nicht erlauben
Erlauben

Learnings

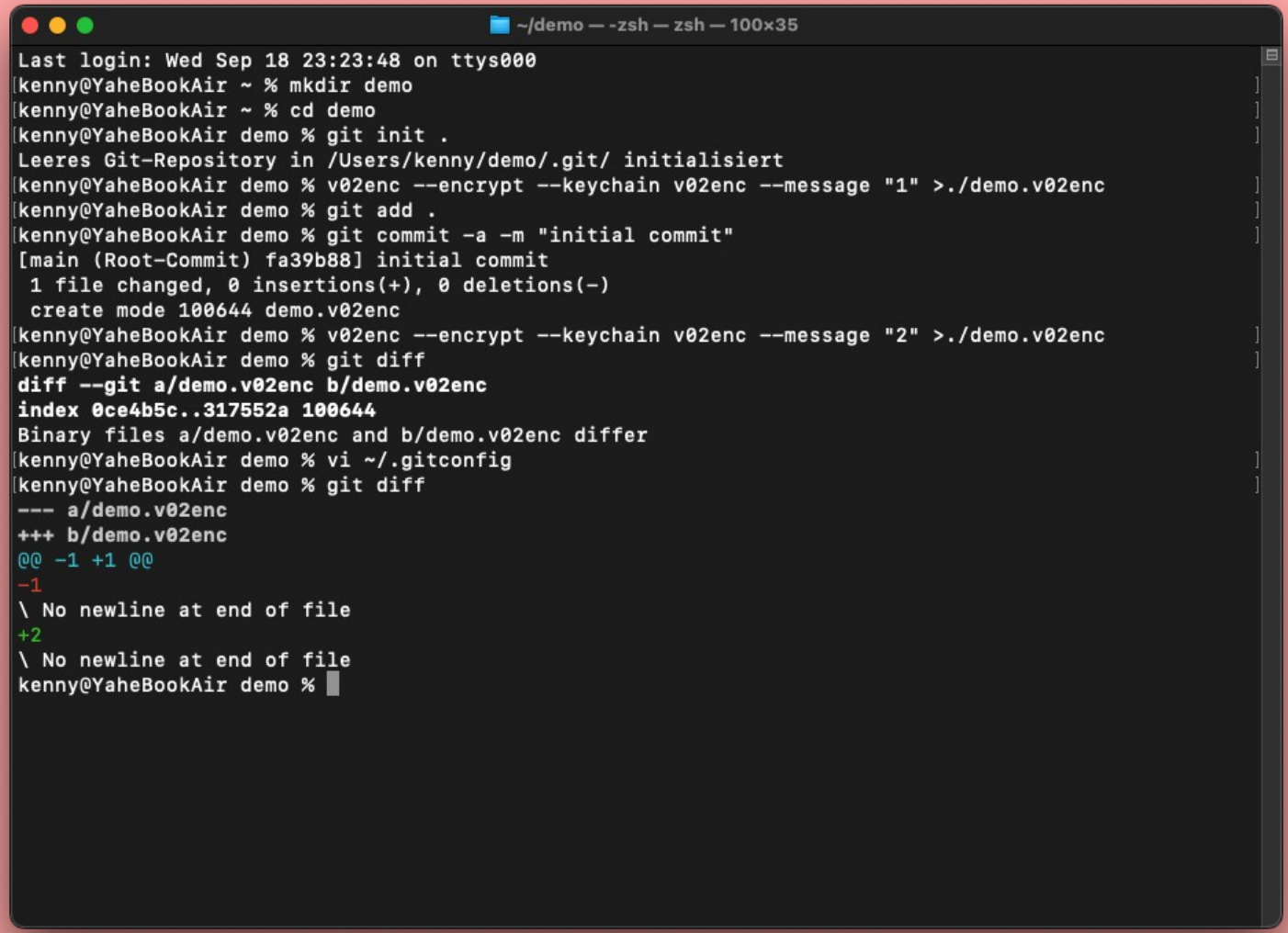
Learnings


~/demo — -zsh — zsh — 100×35
Last login: Wed Sep 18 23:23:48 on ttys000
kenny@YaheBookAir ~ % mkdir demo
kenny@YaheBookAir ~ % cd demo
kenny@YaheBookAir demo % git init .
Leeres Git-Repository in /Users/kenny/demo/.git/ initialisiert
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "1" >./demo.v02enc
kenny@YaheBookAir demo % git add .
kenny@YaheBookAir demo % git commit -a -m "initial commit"
[main (Root-Commit) fa39b88] initial commit
1 file changed, 0 insertions(+), 0 deletions(-)
create mode 100644 demo.v02enc
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "2" >./demo.v02enc
kenny@YaheBookAir demo % git diff
diff --git a/demo.v02enc b/demo.v02enc
index 0ce4b5c..317552a 100644
Binary files a/demo.v02enc and b/demo.v02enc differ
kenny@YaheBookAir demo %

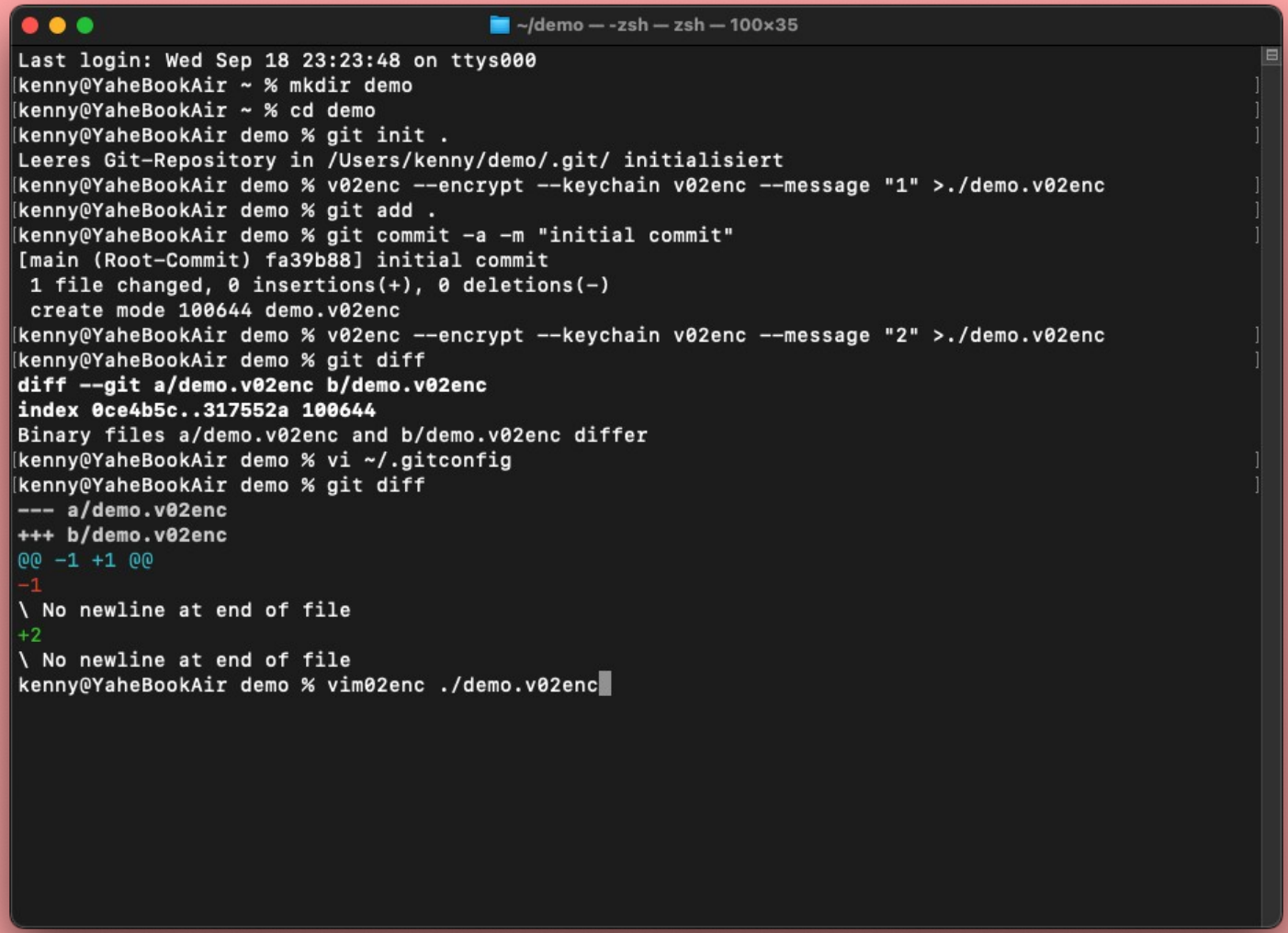
Learnings


~/demo — vi ~/.gitconfig — zsh — 100×35
[diff]
external = /Users/kenny/github/v02enc/v02gitdiff
[user]
name = Yahe
email = hello@yahe.sh
[filter "lfs"]
clean = git-lfs clean -- %f
smudge = git-lfs smudge -- %f
process = git-lfs filter-process
required = true
[init]
defaultBranch = main
"~/.gitconfig" 15L, 250B

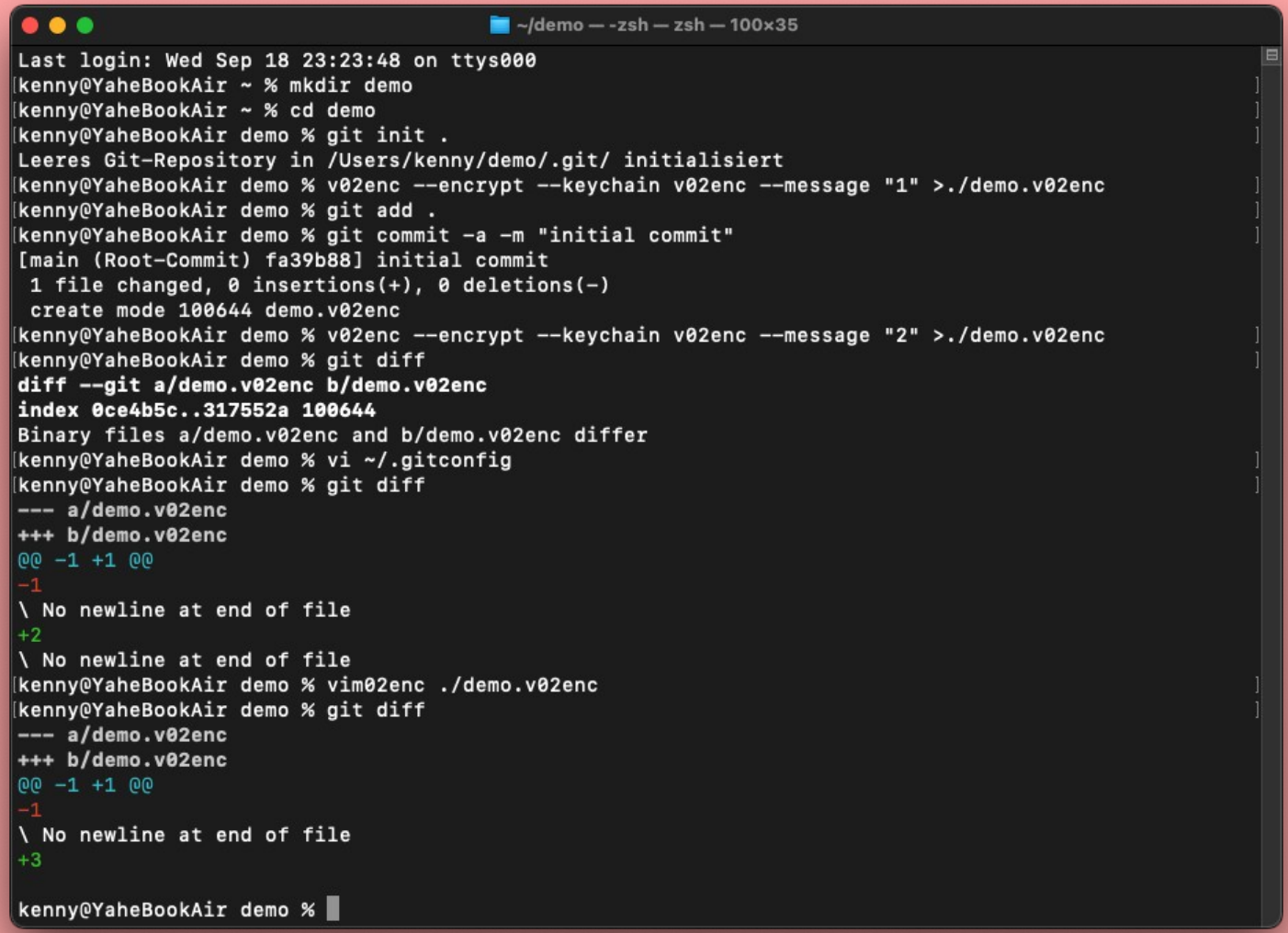
Learnings


~/demo — -zsh — zsh — 100×35
Last login: Wed Sep 18 23:23:48 on ttys000
kenny@YaheBookAir ~ % mkdir demo
kenny@YaheBookAir ~ % cd demo
kenny@YaheBookAir demo % git init .
Leeres Git-Repository in /Users/kenny/demo/.git/ initialisiert
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "1" >./demo.v02enc
kenny@YaheBookAir demo % git add .
kenny@YaheBookAir demo % git commit -a -m "initial commit"
[main (Root-Commit) fa39b88] initial commit
1 file changed, 0 insertions(+), 0 deletions(-)
create mode 100644 demo.v02enc
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "2" >./demo.v02enc
kenny@YaheBookAir demo % git diff
diff --git a/demo.v02enc b/demo.v02enc
index 0ce4b5c..317552a 100644
Binary files a/demo.v02enc and b/demo.v02enc differ
kenny@YaheBookAir demo % vi ~/.gitconfig
kenny@YaheBookAir demo % git diff
--- a/demo.v02enc
+++ b/demo.v02enc
@@ -1 +1 @@
-1
\ No newline at end of file
+2
\ No newline at end of file
kenny@YaheBookAir demo %

Learnings


~/demo — -zsh — zsh — 100×35
Last login: Wed Sep 18 23:23:48 on ttys000
kenny@YaheBookAir ~ % mkdir demo
kenny@YaheBookAir ~ % cd demo
kenny@YaheBookAir demo % git init .
Leeres Git-Repository in /Users/kenny/demo/.git/ initialisiert
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "1" >./demo.v02enc
kenny@YaheBookAir demo % git add .
kenny@YaheBookAir demo % git commit -a -m "initial commit"
[main (Root-Commit) fa39b88] initial commit
1 file changed, 0 insertions(+), 0 deletions(-)
create mode 100644 demo.v02enc
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "2" >./demo.v02enc
kenny@YaheBookAir demo % git diff
diff --git a/demo.v02enc b/demo.v02enc
index 0ce4b5c..317552a 100644
Binary files a/demo.v02enc and b/demo.v02enc differ
kenny@YaheBookAir demo % vi ~/.gitconfig
kenny@YaheBookAir demo % git diff
--- a/demo.v02enc
+++ b/demo.v02enc
@@ -1 +1 @@
-1
\ No newline at end of file
+2
\ No newline at end of file
kenny@YaheBookAir demo % vim02enc ./demo.v02enc

Learnings


~/demo — -zsh — zsh — 100×35
Last login: Wed Sep 18 23:23:48 on ttys000
kenny@YaheBookAir ~ % mkdir demo
kenny@YaheBookAir ~ % cd demo
kenny@YaheBookAir demo % git init .
Leeres Git-Repository in /Users/kenny/demo/.git/ initialisiert
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "1" >./demo.v02enc
kenny@YaheBookAir demo % git add .
kenny@YaheBookAir demo % git commit -a -m "initial commit"
[main (Root-Commit) fa39b88] initial commit
1 file changed, 0 insertions(+), 0 deletions(-)
create mode 100644 demo.v02enc
kenny@YaheBookAir demo % v02enc --encrypt --keychain v02enc --message "2" >./demo.v02enc
kenny@YaheBookAir demo % git diff
diff --git a/demo.v02enc b/demo.v02enc
index 0ce4b5c..317552a 100644
Binary files a/demo.v02enc and b/demo.v02enc differ
kenny@YaheBookAir demo % vi ~/.gitconfig
kenny@YaheBookAir demo % git diff
--- a/demo.v02enc
+++ b/demo.v02enc
@@ -1 +1 @@
-1
\ No newline at end of file
+2
\ No newline at end of file
kenny@YaheBookAir demo % vim02enc ./demo.v02enc
kenny@YaheBookAir demo % git diff
--- a/demo.v02enc
+++ b/demo.v02enc
@@ -1 +1 @@
-1
\ No newline at end of file
+3
kenny@YaheBookAir demo %

Questions?