Every screen you will see, before you see it.

This is the SPLITSTEEL sitting on paper: the set-up, then every screen the kit shows in the order it shows them, then the objects it leaves behind and how the halves are placed for your heirs. The screens are not drawings. They were recorded by driving the real program, build **`6c8c2740`**, through a complete sitting; the website replays the same frames, and the test suite regenerates them so they cannot drift from the code.

Before you sit down

On the table

- The Raspberry Pi with the SPLITSTEEL card, and its power supply
- Any HDMI screen and a USB keyboard
- Two casino dice, two colours, so first and second stay distinct
- Two USB sticks, any size; they become R and B
- The three printed cards: dice card, ARITHMETIC CARD, SEED GRID CARD (field manual pages 11 and 12; the boxed kit ships them printed)
- Pencil and paper

Not in the room

- No network lead and no Wi-Fi hardware on the machine
- No phone on the table, no camera that can see the screen
- Nobody who does not need to be there

For afterwards

- Steel plates, the punch jig and letter punches, or an engraver
- Two M-DISCs and a drive that burns them
- Two ordinary computers, one for each half
- Two hiding places in two buildings

The rules

- **Practice first.** [3] at the menu is the whole sitting with toy values, nothing at stake.
- **Either half alone is nothing.** Both halves together are the key.
- **The two halves never meet** on one computer or in one hiding place.
- **Power off with** [p], never by pulling the plug. Wait for the green light to stop.
- **Never type a seed into a website.** Not this one, not any.

The seed in these screens is a published demonstration value: **`critic next cloud athlete balcony timber gasp draft paddle silk doll glass`**. It must never hold money.

EPISODE 01

Power on

Power on, and the machine checks itself before it lets you in.

```
 ____ ____  _     ___ _____ ____ _____ _____ _____ _
/ ___||  _ \| |   |_ _|_   _/ ___|_   _| ____| ____| |
\___ \| |_) | |    | |  | | \___ \ | | |  _| |  _| | |
 ___) |  __/| |___ | |  | |  ___) || | | |___| |___| |___
|____/|_|   |_____|___| |_| |____/ |_| |_____|_____|_____|

the Pi is a blender  -  steel is the vault


Starting up. This can take a few minutes - the machine is small
and it checks itself before it lets you in. Leave it be.

Nothing on this computer talks to anything: no wi-fi, no bluetooth,
no network. Nothing you type is ever written to the card. When the
power goes off, everything it knew is gone.

The menu will appear by itself. There is nothing to press.
```

SCREEN 01

Power on. The Pi checks itself for a minute or two and the menu appears by itself. Nothing on this machine talks to anything, and nothing typed is ever written to the card.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
MAIN MENU

integrity: wordlist verified - 10 official vectors pass
wizard build 6c8c2740   boot: quiet   reached the menu 41 s after power-on

   [1] build a vault        words -> pad + ciphertext
   [2] recover              pad + ciphertext -> words
   [3] practice             the whole sitting, toy values
   [?] help                 new to this? start here
   [p] power off            the safe way to finish - and the ONLY safe
                            way to remove the card. Wait for the light.

   First time with this kit? Do [3] practice before anything real: the whole
   sitting with toy values, and nothing on the table that matters.
choose:1
```

SCREEN 02

The menu. The build code under the title is the hash of the program itself; the manual and the website tell you what it should read. On a kit there is no shell to quit to, only [p] to power off.

You type **1** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BEFORE ANYTHING

This machine must be a blender: no network lead, no Wi-Fi hardware,
no camera that can see this screen, no phone on the table.

Nothing you type is ever written to disk. Power off ends everything.
Is the room clean and the machine air-gapped? [y/n]y
```

SCREEN 03

The air-gap question. The Pi has no radios and no network lead, but the room matters too: no camera on the screen, no phone on the table.

You type **y** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
THE USB STICKS

Each half gets its own USB stick, written one at a time so that
both halves can never end up on the same one.

  2 removable drives are plugged in. Good.
     /dev/sda1  (KINGSTON, 15.5 GB)
     /dev/sdb1  (SANDISK, 31.0 GB)

  Leave them in for now. When it is time to write, I will ask
  you to unplug all but one.
press enter to continue - the screen will then clear
```

SCREEN 04

Before a single die is rolled the wizard counts the sticks, so nobody finds out forty minutes in that they brought one.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - THE SEED

Where do the words come from?

   [1] I already have a seed   type in the words I have
   [2] make a brand new one    if the seed I have might be weak or seen
choose:2
```

SCREEN 05

Two ways in: type the words you already have, or mint a brand new seed. This sitting mints one.

You type **2** and press enter.

EPISODE 02

A brand new seed

Mint a seed from your dice and this machine together, and check the arithmetic by hand on the cards.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED

This makes a wallet that has never existed before. It is for someone
whose current seed might be weak or might have been seen - a device
with a bad random number generator, a phrase typed into a website, a
backup that was photographed.

  This is a bigger thing than backing up a seed you already have.
  Everything you own will depend on the next few minutes. The
  arithmetic here is standard and tested against the official
  vectors, but no outside party has reviewed this program.
Make a new seed? [y/n]y
```

SCREEN 06

Minting a wallet that has never existed is a bigger thing than backing one up, and the wizard says so before it starts.

You type **y** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - HOW LONG

   [1] 12 words   128 bits. Ample. About 36 dice rolls.
   [2] 24 words   256 bits. Twice the rolls, same method.
choose [enter = 12]:
```

SCREEN 07

Twelve words is 128 bits and ample. Twenty-four is the same method with twice the rolls.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - WHERE THE RANDOMNESS COMES FROM

   [1] your dice AND this machine, mixed   recommended
       About 36 rolls. The machine commits to its number
       first, on screen, before you roll - so it cannot
       steer the result. The two are combined, and the
       answer is good if EITHER source is good. Safe if
       this card was tampered with. Safe if your dice are
       loaded. Same effort as dice alone.
       You still trust that the words shown are the ones the
       numbers make - which you check by hand, afterwards.

   [2] your dice only
       About 36 rolls. Trusts nothing but your dice being
       fair, and your arithmetic. Nothing else at all.

   [3] this machine only   quick
       Instant, no dice. The generator is sound - Linux
       will not hand out random numbers before it has
       gathered enough entropy, so it cannot quietly give
       you a weak one. But you cannot check that from
       outside: you are trusting that whoever flashed this
       card did not swap the program. We cannot yet promise
       more than that - the card is not reproducible from
       source byte for byte, so there is no published number
       you could check it against. Still far better than
       keeping a seed you already doubt.

  A seed invented by a hardware wallet is not one of these
  three. That is the whole reason this step exists: make a
  new one here, then move your money to it.
choose:1
```

SCREEN 08

Dice and machine mixed is the recommendation: the result is good if either source was good, so a tampered card or loaded dice each fail alone.

You type **1** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - THE MACHINE COMMITS FIRST

This is the machine's half. It is fixed now, before you touch a die.

THE MACHINE'S NUMBER  - write it in grid A of the SEED GRID CARD, box for box

   1      2      3      4
  6DCE   ACDC   3EB3   F515
   5      6      7      8      check
  6F05   65C2   F485   0AAE   FE58

  Write this down. Later you can check the arithmetic yourself,
  on the printed table, and prove this machine did not
  choose your seed for you.
press enter when it is written down - then roll
```

SCREEN 09

The machine's half is drawn and shown before any die is rolled, so it cannot steer the result after seeing your dice. Copy it into grid A of the SEED GRID CARD, box for box.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - NOW YOUR DICE

  The dice half is cast.
  Write it in grid B of the SEED GRID CARD, box for box, check group too.

   1       2       3       4
  5E1C    0473    B9A2    E8D1

   5       6       7       8
  370F    6A5C    2D94    081F

   check
  73C4

press enter to continue - the screen will then clear
```

SCREEN 10

Your half is cast, with its check group. Copy it into grid B of the SEED GRID CARD.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - MIXED

  A combined with B, exclusive-or, gives C - THE NEW SEED, AS HEX.
  Good if either source was good. Both would have to be bad, at
  the same time, for this to be weak.

   A  the machine's number              B  your dice
   1      2      3      4               1      2      3      4
  6DCE   ACDC   3EB3   F515            5E1C   0473   B9A2   E8D1

   5      6      7      8      check    5      6      7      8      check
  6F05   65C2   F485   0AAE   FE58     370F   6A5C   2D94   081F   73C4

   C  the new seed  =  A combined with B
   1      2      3      4
  33D2   A8AF   8711   1DC4

   5      6      7      8      check
  580A   0F9E   D911   02B1   8D9C

  Write all three grids onto the SEED GRID CARD, box for box.
  Grids A and B should already be there. With all three on paper
  you can prove the arithmetic yourself, next.
press enter to continue - the screen will then clear
```

SCREEN 11

A combined with B gives C, the new seed. Both would have to be bad, at the same time, for this to be weak. All three grids go onto the card.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - CHECK THE ARITHMETIC

You have three numbers on paper: the machine's, your dice, and the
seed. The seed should be the first two combined with exclusive-or.

Checking that yourself is what takes this program off the trust path.
Until you do, you are taking its word that it used the number it
showed you.

You will need two cards in your hand:
   the SEED GRID CARD    grids A, B and C, written box for box
   the ARITHMETIC CARD   the 16 x 16 table you read them against

  Both are in the kit box, in the field manual (page 11 and the page
  after it) and on the website. Use the printed table, never a screen:
  a table this machine drew is a table it could bend.

   [1] I have both - check every group now   8 lookups, about four minutes
   [2] I need to get them - I will check later from my paper
choose:1
```

SCREEN 12

Now you check the machine, not the other way round. It asks for the SEED GRID CARD you have filled in and the printed ARITHMETIC CARD, and says where to find them.

You type **1** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - CHECK THE ARITHMETIC

  The lit box in A is the row on the table, the lit box in B the
  column; where they meet is that box of C. Type its four characters.
  Move freely: a box number jumps there, b goes back, v checks all 8.

   A  the machine's number              B  your dice
   1      2      3      4               1      2      3      4
  [6DCE] [ACDC] [3EB3] [F515]          [5E1C] [0473] [B9A2] [E8D1]
   5      6      7      8      check     5      6      7      8      check
  [6F05] [65C2] [F485] [0AAE] [FE58]   [370F] [6A5C] [2D94] [081F] [73C4]

   C  the new seed  =  A combined with B
   1      2      3      4
  [????] [????] [????] [????]
   5      6      7      8      check
  [????] [????] [????] [????] [8D9C]
  where A1 and B1 meet:33d2
```

SCREEN 13

For each lit box: the A character is the row on the printed table, the B character the column, and where they meet is C. Box 4 is mistyped here on purpose: it goes red and is retyped.

You type **33d2** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - THE ARITHMETIC

  All 8 groups agree.

   A  the machine's number              B  your dice
   1      2      3      4               1      2      3      4
  [6DCE] [ACDC] [3EB3] [F515]          [5E1C] [0473] [B9A2] [E8D1]
   5      6      7      8      check     5      6      7      8      check
  [6F05] [65C2] [F485] [0AAE] [FE58]   [370F] [6A5C] [2D94] [081F] [73C4]

   C  the new seed  =  A combined with B
   1      2      3      4
  [33D2] [A8AF] [8711] [1DC4]
   5      6      7      8      check
  [580A] [0F9E] [D911] [02B1] [8D9C]

  You have now checked, by hand, that the seed really is the
  machine's number combined with your dice. This program did not
  choose your wallet for you, and you did not have to take its
  word for it.
press enter to continue - the screen will then clear
```

SCREEN 14

All eight groups agree. The program did not choose your seed, and you did not have to take its word for it.

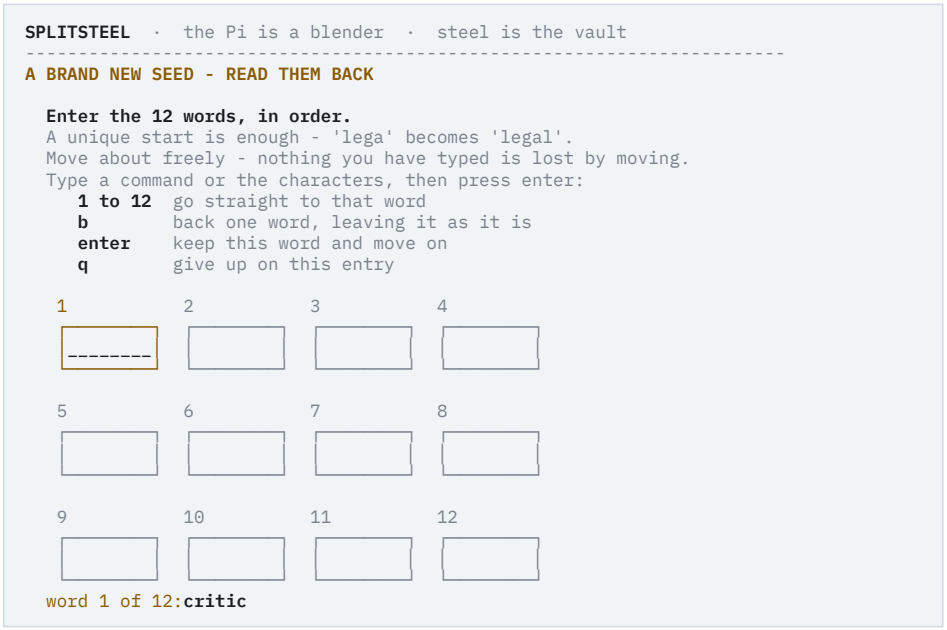
You press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
A BRAND NEW SEED - THE WORDS

  from your dice mixed with this machine

    1 critic       2 next         3 cloud        4 athlete
    5 balcony      6 timber       7 gasp         8 draft
    9 paddle      10 silk        11 doll        12 glass

  Write these down now, on paper, in order.
  The last word is not free - part of it is a checksum over
  all the others, which is how a wallet knows the phrase is
  whole. Copy it exactly like the rest.
press enter when every word is written down
```

SCREEN 15

The seed as its twelve words. These are written on paper and read back in the next screen, the same way every entry on this machine is read back.

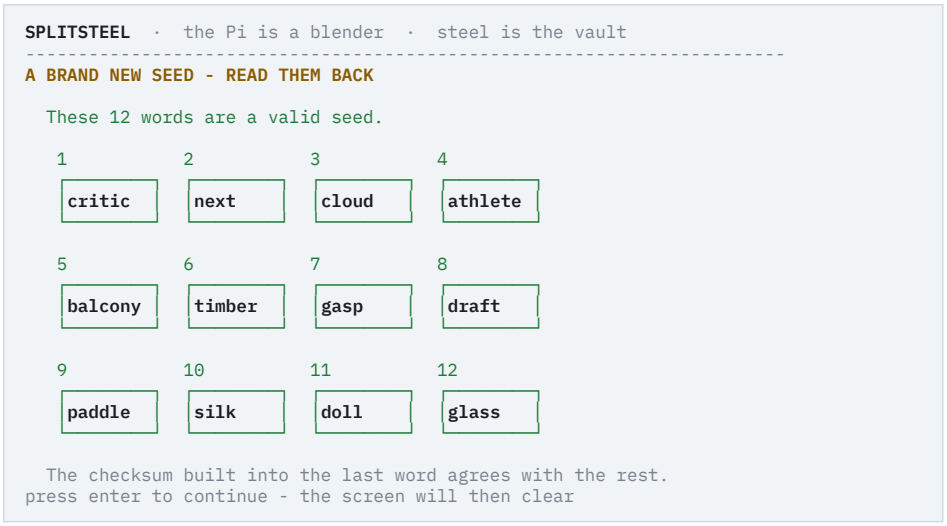
You press enter.



SCREEN 16

The words typed back from your paper, in the same grid as everything else. The checksum in the last word catches a slip.

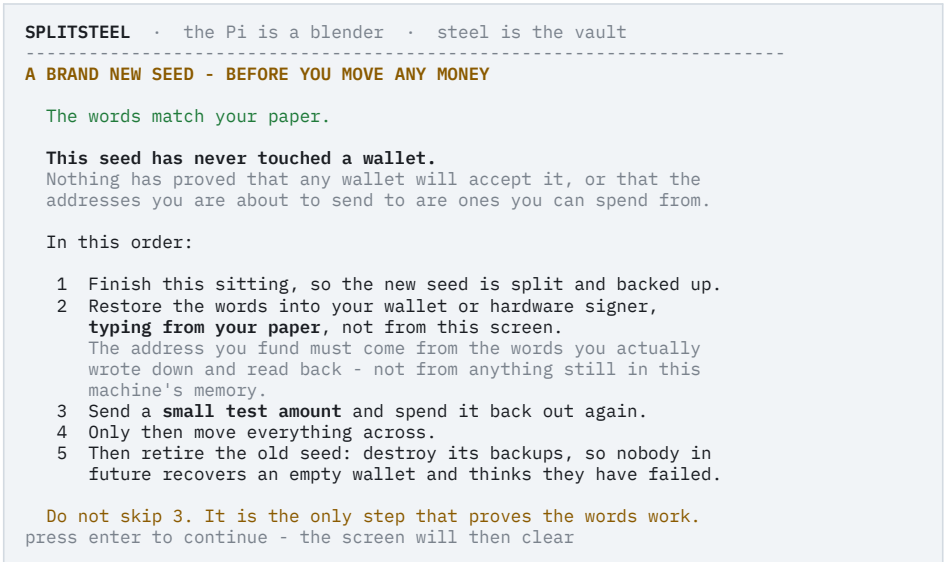
You type **critic** and press enter.



SCREEN 17

Twelve words, read back exactly. The paper is right.

You press **enter**.



SCREEN 18

A new wallet is tested before it holds anything: a small amount in and back out first, and the old seed retired only after everything has moved.

You press **enter**.

EPISODE 03

The pad and the ciphertext

Cast the pad from your dice; the wizard works out the ciphertext. Two halves, written down exactly.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - CAST THE PAD

The pad is YOUR dice, never this machine. If you have already rolled
it at the table with the printed card, choose hex entry.

   [1] enter dice rolls, the wizard maps them
   [2] enter the pad as hex, already rolled
choose:1
```

SCREEN 19

The pad is your dice, never the machine. It is the other random number, the one the seed hides behind.

You type **1** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
CAST THE PAD - DICE

  The pad is cast.

   1       2       3       4
  2D94    081F    5E1C    0473

   5       6       7       8
  B9A2    E8D1    370F    6A5C

   check
  73C4
press enter to continue - the screen will then clear
```

SCREEN 20

The pad is cast, with the check group the wizard works out from it.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - WRITE THE PAD

THE RED PAD  - half the secret, write it exactly, check group too
   1      2      3      4
  2D94   081F   5E1C   0473
   5      6      7      8      check
  B9A2   E8D1   370F   6A5C   73C4

This goes on the keeper plate and the spare. No labels, ever.
written down, with its check group? press enter
```

SCREEN 21

The RED half. Write it exactly, check group too. This goes on the keeper plate and its spare, and carries no label, ever.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - THE CIPHERTEXT

THE BLUE CIPHERTEXT  - the other half, write it exactly, check group too
   1      2      3      4
  1E46   A0B0   D90D   19B7
   5      6      7      8      check
  E1A8   E74F   EE1E   68ED   FE58

Now the SPOT CHECK. Everything so far has been done by this machine.
This is the one step that does not trust it - you do the arithmetic
yourself, from the XOR table on your printed card, and it grades you.

Use the table on the CARD, not on any screen. A dishonest machine
could show you a doctored table; a printed card cannot be changed.

Haven't got the card? It is page 11 of the field manual -
the page headed "Print this page and take it to the table", with the
dice card and the 16x16 XOR table on it. You will find the manual:

   on any SPLITSTEEL stick or disc:  manual/
   on the website:                   the field manual download
   or the recipe page, which prints the table on its own

Print it on another computer and come back. This machine deliberately
will not show you the table - a table it drew is a table it could bend.
Do the spot check now? (strongly recommended) [y/n]y
```

SCREEN 22

The BLUE half: the seed combined with the pad. Either half on its own is a random number. Then the spot check, done from the printed card and never from a screen.

You type **y** and press enter.

EPISODE 04

The checks

The spot check proves the machine's arithmetic against your printed card. The round trip proves your paper.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - SPOT CHECK 1 OF 3

Find the pair on the XOR table on your card: the PAD character
gives the row, the CIPHERTEXT character gives the column. Read off
where they meet, and type it in.

   RED PAD                                BLUE CIPHERTEXT
   1      2      3      4                 1      2      3      4
  [2D94] [081F] [5E1C] [0473]            [1E46] [A0B0] [D90D] [19B7]
   5      6      7      8      check      5      6      7      8      check
  [B9A2] [E8D1] [370F] [6A5C] [73C4]     [E1A8] [E74F] [EE1E] [68ED] [FE58]

  character 10 of 32 - the second character of the lit box, box 3
     pad        E
     ciphertext 9
     row E, column 9 gives:7
```

SCREEN 23

Three characters picked at random. The RED PAD character is the row, the BLUE CIPHERTEXT character the column, and you read where they meet off the printed table.

You type **7** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - SPOT CHECK RESULT

  OK   character 10  you said 7, this machine says 7
  OK   character 21  you said 0, this machine says 0
  OK   character 26  you said 9, this machine says 9

  All three agree.
  The arithmetic on this machine matches the arithmetic on your card.
  You are no longer taking its word for anything.
press enter to continue - the screen will then clear
```

SCREEN 24

Your table and the machine agree, so the machine's arithmetic is the arithmetic on your card.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
READ IT BACK

  re-enter the RED PAD, from your own writing
  Four characters per box, in the order they appear on the object.
  Move about freely - nothing you have typed is lost by moving.
  Type a command or the characters, then press enter:
     1 to 9   go straight to that box
     b        back one box, leaving it as it is
     enter    keep this box and move on
     q        give up on this entry

   1      2      3      4
  [____] [    ] [    ] [    ]

   5      6      7      8
  [    ] [    ] [    ] [    ]

   check
  [    ]
  box 1 of 8:2d94
```

SCREEN 25

Each half goes in box by box from the paper. The check box at the end catches a misread character and says which column of the paper to look at.

You type **2d94** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - ROUND-TRIP RESULT

    1 critic       2 next         3 cloud        4 athlete
    5 balcony      6 timber       7 gasp         8 draft
    9 paddle      10 silk        11 doll        12 glass

MATCHES the seed you started with.
And they match the paper seed in front of you, word for word? [y/n]y
```

SCREEN 26

The twelve words come back exactly. The paper is right.

You type **y** and press enter.

EPISODE 05

The sticks

Each half onto its own stick, one at a time, read back and labelled. Then what is left to do.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
--------------------------------------------------------------------------------
BUILD THE VAULT - WRITE THE RED STICK

Plug in ONE stick: the one that will carry the PAD.
Unplug every other USB stick first.

  This is the rule that makes the whole scheme safe: with one
  stick in the machine, both halves cannot land on the same one.

   [1] it is plugged in, and it is the only one
   [2] skip the USB copy of this half
choose:1
```

SCREEN 27

One stick at a time, with every other stick unplugged, so both halves can never land on the same one. The half, the plate files and the recovery tools go on, then it is read back.

You type **1** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
--------------------------------------------------------------------------------
BUILD THE VAULT - THE RED STICK IS WRITTEN

  Written and verified.
  Every file was read back and matched its checksum, and the
  half was re-derived from the stick to confirm the check group.

  Now, before you do anything else:

     Write  R  on this stick in permanent marker.
     R = pad. It is safe to label: a half on its own is nothing.

     Then unplug it.
press enter when it is labelled and unplugged
```

SCREEN 28

Read back and verified. Label it R or B in marker: a half on its own is nothing, so the label is safe. Then unplug it before the other one goes in.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
--------------------------------------------------------------------------------
BUILD THE VAULT - WRITE THE BLUE STICK

Plug in ONE stick: the one that will carry the CIPHERTEXT.
Unplug every other USB stick first.

  This is the rule that makes the whole scheme safe: with one
  stick in the machine, both halves cannot land on the same one.

   [1] it is plugged in, and it is the only one
   [2] skip the USB copy of this half
choose:1
```

SCREEN 29

One stick at a time, with every other stick unplugged, so both halves can never land on the same one. The half, the plate files and the recovery tools go on, then it is read back.

You type **1** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
--------------------------------------------------------------------------------
BUILD THE VAULT - THE BLUE STICK IS WRITTEN

  Written and verified.
  Every file was read back and matched its checksum, and the
  half was re-derived from the stick to confirm the check group.

  Now, before you do anything else:

     Write  B  on this stick in permanent marker.
     B = ciphertext. It is safe to label: a half on its own is nothing.

     Then unplug it.
press enter when it is labelled and unplugged
```

SCREEN 30

Read back and verified. Label it R or B in marker: a half on its own is nothing, so the label is safe. Then unplug it before the other one goes in.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BUILD THE VAULT - THE SITTING IS DONE

On the table you now have the pad and the ciphertext, each with a
check group. What remains, in order:

   OPEN  START-HERE.html  ON EACH STICK.
   It is a page that opens with a double-click on any computer and
   walks that half through to finished: burning the disc, making
   the plate, and where to put it. You do not have to remember any
   of what follows - it is all on that page, per half.

   THE TWO STICKS MUST NEVER MEET.
   Take R to one computer and B to a different one, and keep it that way.
   Either stick alone is nothing. Both on one computer is your
   whole seed on that computer.

   1  punch or engrave the keeper plates: one pad, one ciphertext
   2  make the spare pair on your chosen medium
   3  run RECOVER on this wizard reading only off the finished objects
   4  only then destroy the old paper seed
   5  split the copies: no hiding place holds both halves
   6  wipe or destroy this SD, power off, post the heirs' letter

   7  send a small test amount to the NEW wallet and spend it
      back out, then move everything across
   8  only then retire the OLD seed: destroy its plates, discs
      and paper, so nobody later recovers an empty wallet
      and thinks they have failed

When you are finished with this machine, choose  p  at the menu to
power off. Do not pull the plug.
press enter to clear the screen
```

SCREEN 31

What is left is physical. START-HERE.html on each stick walks that half through to its plate and its disc. The two sticks never meet on one computer.

You press **enter**.

EPISODE 06

Power off

The only safe way to finish, and the only safe way to take the card out.

```
Powering off. Nothing was ever stored.

The screen will go blank in a moment. That is NOT the end.

  RED light    = the plug is in. It never goes off. Ignore it.
  GREEN light  = the card is busy. Watch this one.

Pull the plug only when the GREEN light has been off for a slow
count of ten. On this board that is a good half-minute after
the screen goes blank. Pulling it sooner is how the card gets damaged.
```

SCREEN 32

Power off from the menu, never by pulling the plug. The red light stays on; wait until the green one has been off for a slow count of ten.

EPISODE 07

Recover

The bad day: two objects, both halves typed box by box, the words back, and one question before you finish.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
BEFORE ANYTHING

This machine must be a blender: no network lead, no Wi-Fi hardware,
no camera that can see this screen, no phone on the table.

Nothing you type is ever written to disk. Power off ends everything.
Is the room clean and the machine air-gapped? [y/n]y
```

SCREEN 33

The air-gap question. The Pi has no radios and no network lead, but the room matters too: no camera on the screen, no phone on the table.

You type **y** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
RECOVER - FROM THE OBJECTS

One pad copy and one ciphertext copy, in a private room, on a blender.

  RED marks the pad and BLUE the ciphertext, on a stick or a disc alike.
  Plates carry no mark, and it does not matter: the arithmetic comes
  out the same either way round, so enter two plates in any order.
how many words? [12/15/18/21/24, enter=12]:12
```

SCREEN 34

The bad day. One pad copy and one ciphertext copy, on a blender. RED marks the pad and BLUE the ciphertext on a stick or a disc; plates carry no mark, and the order does not matter.

You type **12** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
READ IT BACK

  the RED PAD, read from the object in front of you
  Four characters per box, in the order they appear on the object.
  Move about freely - nothing you have typed is lost by moving.
  Type a command or the characters, then press enter:
     1 to 9   go straight to that box
     b        back one box, leaving it as it is
     enter    keep this box and move on
     q        give up on this entry

   1       2       3       4
  ┌────┐  ┌────┐  ┌────┐  ┌────┐
  ____
  └────┘  └────┘  └────┘  └────┘

   5       6       7       8
  ┌────┐  ┌────┐  ┌────┐  ┌────┐
  └────┘  └────┘  └────┘  └────┘

   check
  ┌────┐
  └────┘
  box 1 of 8:2d94
```

SCREEN 35

Each half goes in box by box from the paper. The check box at the end catches a misread character and says which column of the paper to look at.

You type **2d94** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
RECOVER - THE WORDS

    1 critic       2 next         3 cloud        4 athlete
    5 balcony      6 timber       7 gasp         8 draft
    9 paddle      10 silk        11 doll        12 glass

Write them down before you go on - the next screen clears this one.
press enter to continue - the screen will then clear
```

SCREEN 36

The words are back. Write them down before the screen clears.

You press **enter**.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
------------------------------------------------------------------------
RECOVER SUCCEEDED - ONE QUESTION BEFORE YOU FINISH

You have your words back - the two halves rebuilt the wallet.

Before you do anything with them, this program needs to know one
thing, because the safe next step is completely different depending
on the answer: what kind of machine did you just do this on?

   [1] a dedicated blender - never been online, will be wiped
       (a kit Pi like this one)
   [2] an everyday computer, or I am not sure
       (a laptop or PC that has been on the internet)
choose 1 or 2:1
```

SCREEN 37

One question before you finish, because the safe next step depends entirely on what kind of machine just saw both halves.

You type **1** and press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
--------------------------------------------------------------------------
RECOVER - THE SEED IS STILL SAFE

  Good - nothing untrusted has seen it.
  The only machine that has seen both halves is this one, and it
  goes no further.

   1  Write the words on a scrap of paper.
   2  Put them into a wallet on a device that has NOT been on the
      internet - a hardware wallet (Trezor, Ledger and the like,
      bought new) is safest. Never a website, never a wallet on a
      phone or PC that browses the web. Confirm the balance is what
      you expected, then move the funds to a wallet you control.
      New to this? Choose [?] help at the menu first.
   3  Burn the scrap.
   4  Wipe or destroy this SD card.
   5  Put the two objects back in different buildings.
press enter to clear the screen
```

SCREEN 38

On a dedicated blender the seed is still private: into a hardware wallet, never a website, confirm the balance, move the funds, burn the scrap, wipe the card.

You press enter.

EPISODE 08

Help for heirs

Written for someone who has never done any of this. The words are the money.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
--------------------------------------------------------------------------
HELP - START HERE IF THIS IS NEW TO YOU

If you have inherited this, or just do not know your way around
crypto, that is completely normal. Read this once - it is short, and
it is the difference between keeping the money and losing it.

The words this machine gives you ARE the money.
Like cash, or a key to a safe: whoever has them owns everything
inside, at once, with no way to get it back. So:

  THE RULES THAT KEEP YOU SAFE
   - Never type the words into a website. No real service needs them.
   - Never send them to anyone - not by email, message, or photo.
   - Never type them because someone helping you over the phone or
     chat told you to. That is the commonest way people are robbed.
   - A real helper never needs to take the words away or keep a copy.
     They can guide you while YOU hold the paper.
   - In any doubt, stop. The money is safe as long as the words are.
     Nothing about this is urgent, whatever anyone tells you.
press enter for the next page
```

SCREEN 39

The heir's first screen. The words are the money; never type them into a website, never send them to anyone, and nobody real ever needs to take them away.

You press enter.

```
SPLITSTEEL  ·  the Pi is a blender  ·  steel is the vault
--------------------------------------------------------------------------
HELP - WHAT TO DO WITH THE WORDS

To reach the money, the words go into wallet software on a device
that has not been on the internet - a hardware wallet (a small
dedicated device such as a Trezor or Ledger, bought new and sealed)
is the safest choice. Never put them into a wallet on an everyday
phone or computer that browses the web.

Once the wallet shows the balance, move it to a wallet that is yours,
then treat these words as spent.

  IF YOU NEED A PERSON TO HELP
   - Best of all: someone you already know and would trust with cash.
   - A solicitor experienced in digital assets.
   - A regulated crypto custody firm - but you approach them; never
     accept an offer that came to you, and they still never need the
     words themselves.
   - Hardware-wallet makers give free setup guides and support. Real
     support helps you use the device and never asks for your words.
     If "support" asks for the words, it is a thief. Walk away.

The full manual, on the disc and the memory stick, says all of this
again with more detail, including how to do it with no computer.
press enter to continue - the screen will then clear
```

SCREEN 40

What to do with the words: a hardware wallet bought new, then move the money and treat these words as spent. Who can safely help, and the one sign of a thief.

You press enter.

AFTER THE SITTING

Two sticks, two numbers on paper. From here on, one half at a time.

The blender is the only machine that ever holds your whole seed. Everything after it handles one half, and a half is a random number, so the computers that make the copies need no trust and no skill. One rule replaces all of that: **the two halves never meet on the same computer.**

- **The sticks.** Each carries one half, its plate files, the recovery tools and START-HERE.html, a page that opens with a double-click and walks that half through to finished. Take R to one computer and B to a different one.
- **The discs.** One M-DISC per half, burned on that half's computer from the files on its stick.
- **The steel.** A keeper plate and a spare for each half, punched with the jig from the plate files, eight groups and the check group. No labels, ever: the plates carry no red or blue and no name, because the arithmetic does not care which is which.
- **Then prove it, then split it.** Run RECOVER on the kit reading only off the finished objects. Only then destroy the old paper seed. Two halves, three copies each, and no hiding place holds both halves. Wipe the SD card, power off, post the heirs' letter.

INHERITANCE

Split the secret, not the trust.

Copies of the same half never add up. Twenty people holding twenty copies of the ciphertext hold nothing between them, which is what makes a split different from a multisig: nobody you give a half to can ever spend, alone or together. The whole design of the inheritance is deciding who could hold one half and also reach the other.

- **Many ciphers.** Spread the ciphertext as widely as is useful: a solicitor, a family member, a hole in the garden, even a dead man's switch in an online account. A hacked account learns a random string and nothing else.
- **Few pads.** Keep the pad copies few, in places only you control, never online, never with anyone who holds a cipher. Once a thief has a pad, every cipher copy in the world is a place they can finish the job.
- **The one rule.** No person, account or place ever holds one half and the whereabouts of the other. A solicitor with a cipher and a sealed letter saying where a pad is holds the whole secret.
- **The after-death path takes two.** The will names where the pad is, and whoever holds the will holds no cipher. A cipher sits with someone who does not know where the pad is. Either alone has nothing. Together, after you, they recover it.

THE BAD DAY

For the person who inherits this.

The wizard has a help screen written for you, and the recovery is two grids typed from two objects. The words it gives you are the money. Nothing about this is urgent, whatever anyone says.

- Read the help screens first: choose [?] at the menu.
- Gather one pad object and one ciphertext object: a red stick or disc and a blue one, or two plates in any order.
- Sit at the kit in a private room, choose [2] recover, and type each half box by box. The check box catches a misread character and says which column of the object to look at.
- Write the words on paper when the screen shows them, before pressing enter.
- Put them into a hardware wallet bought new, never a website, never a phone or PC that browses the web. Confirm the balance, then move everything to a wallet that is yours.
- Burn the scrap, wipe the SD card, and put the two objects back in different buildings until the old wallet is empty.
- Real help never needs your words. If anyone offering support asks for them, they are a thief. Walk away.

This quick start was generated from program build **6c8c2740**. The field manual, with the three printed cards, is splitsteel-field-manual.pdf beside this file.