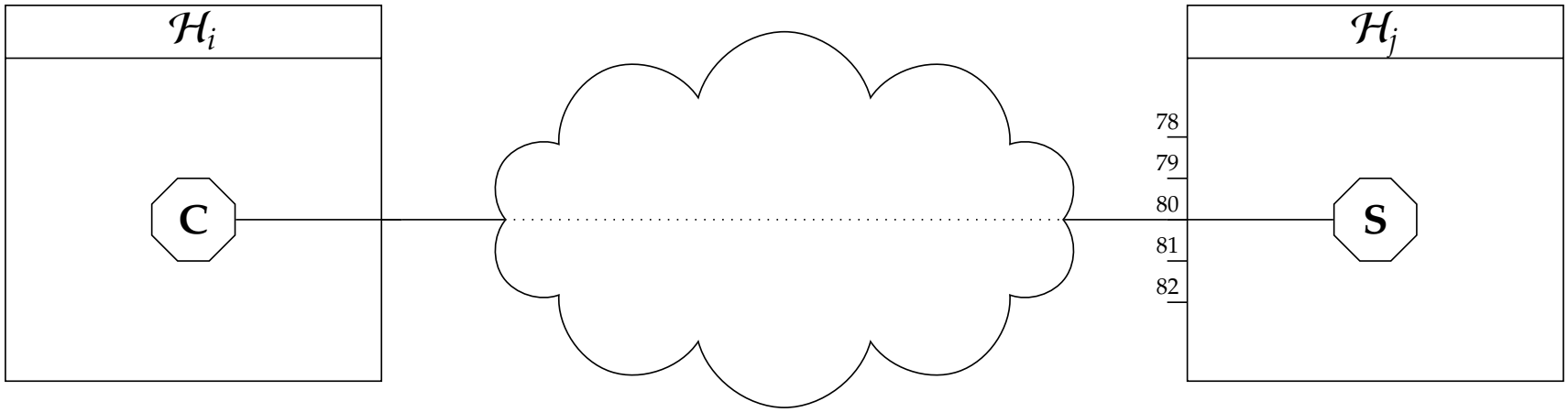
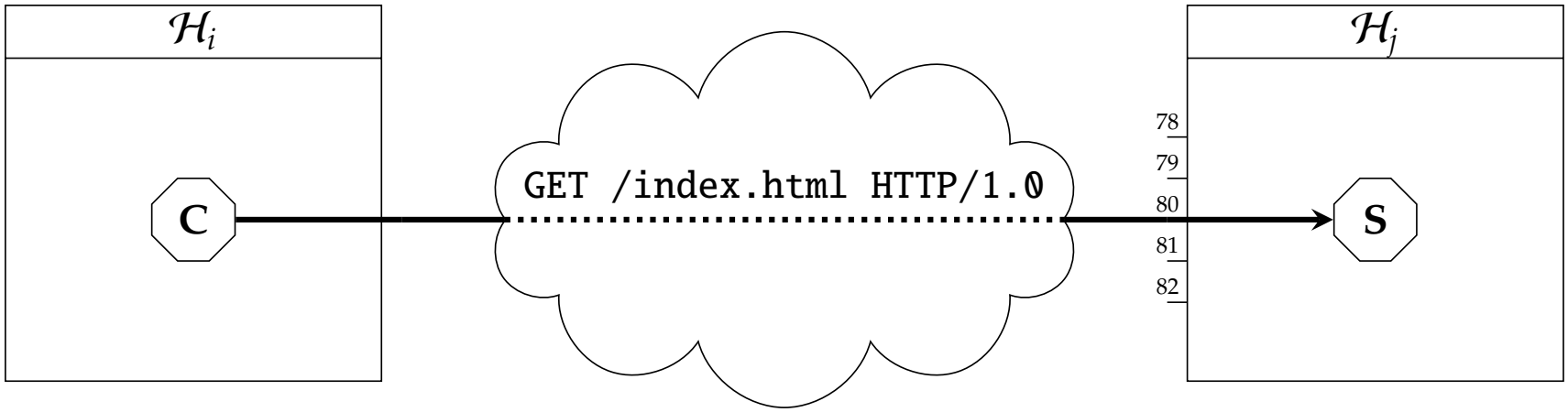
- Agenda: a somewhat technical introduction to the coursework assignment, i.e.,
  - overview of the assignment motivation and content,
  - answer any FAQs,
  - answer any non-FAQs,

  with the overarching goal of clarity, and enabling early progress.

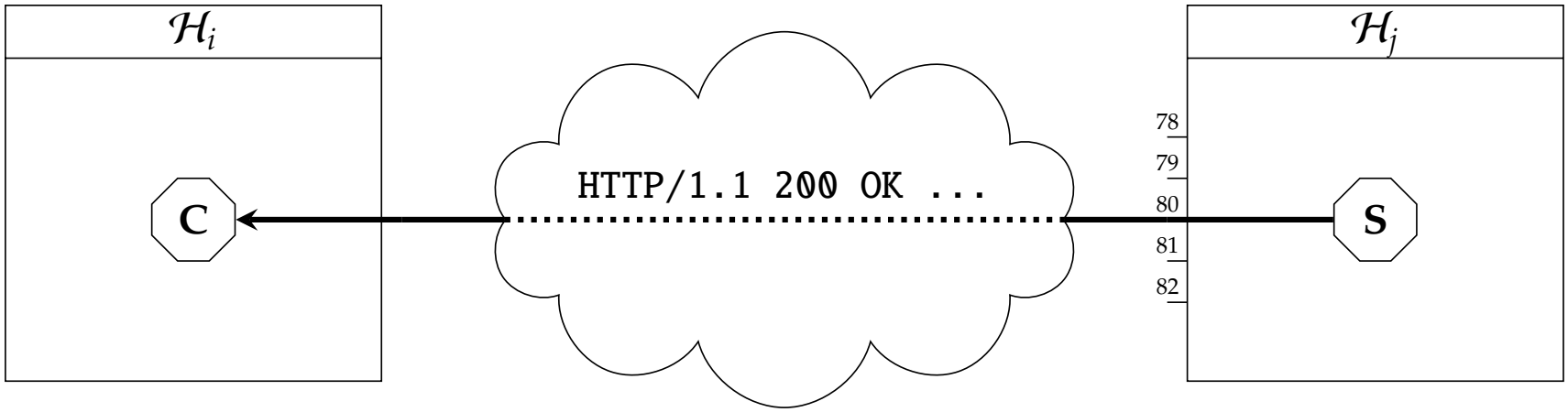
- Problem: confidential (bulk) communication, per



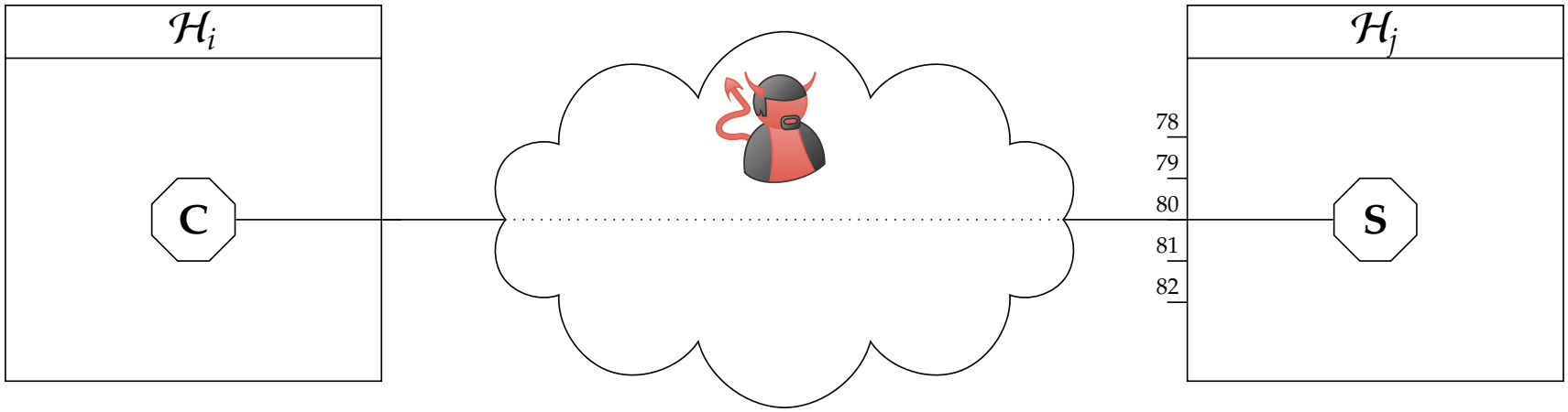
- Problem: confidential (bulk) communication, per



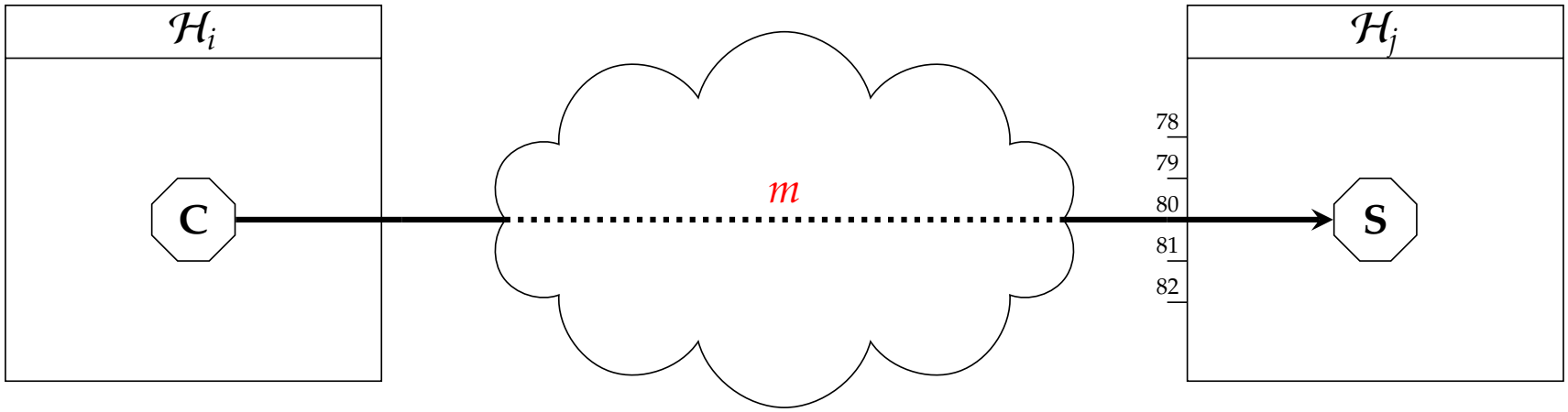
- Problem: confidential (bulk) communication, per



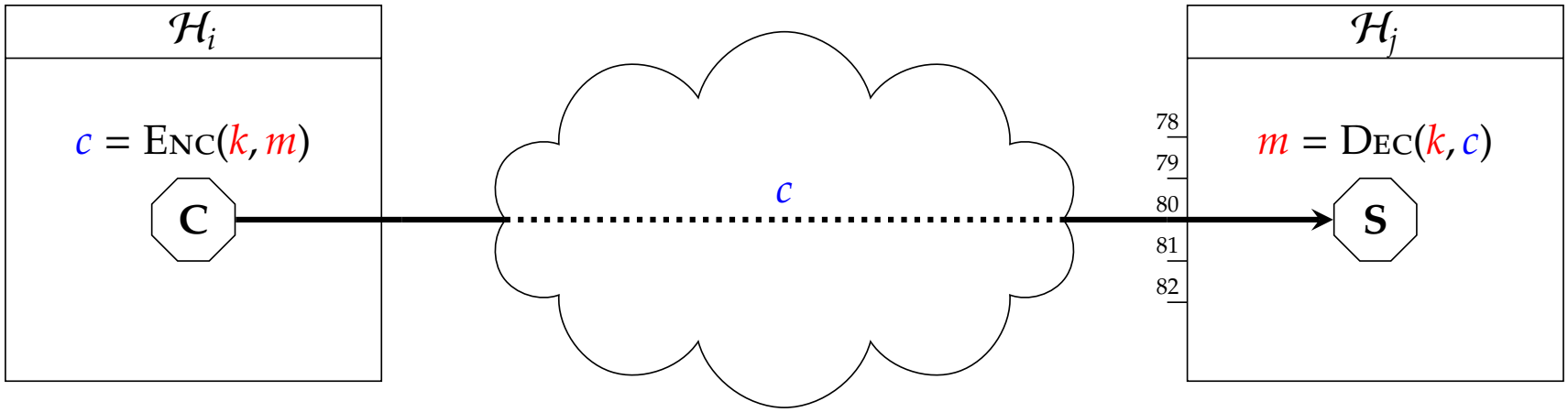
- Problem: confidential (bulk) communication, per



- Problem: confidential (bulk) communication, per



- Problem: confidential (bulk) communication, per



- Solution: **encryption** using a **block cipher**, i.e.,

$$\begin{array}{lcccccc} \text{Enc} & : & \{0,1\}^{n_k} & \times & \{0,1\}^{n_b} & \rightarrow & \{0,1\}^{n_b} \\ \text{Dec} & : & \{0,1\}^{n_k} & \times & \{0,1\}^{n_b} & \rightarrow & \{0,1\}^{n_b} \end{array}$$

such that $\text{Dec}(k, c = \text{Enc}(k, m)) = m$.

- Structure: using Verilog,

stage 1	$\Rightarrow$	implement support for ENC
stage 2	$\Rightarrow$	implement ENC using combinatorial approach
stage 3	$\Rightarrow$	implement ENC using iterative approach
stage 4	$\Rightarrow$	implement ENC using piplined approach

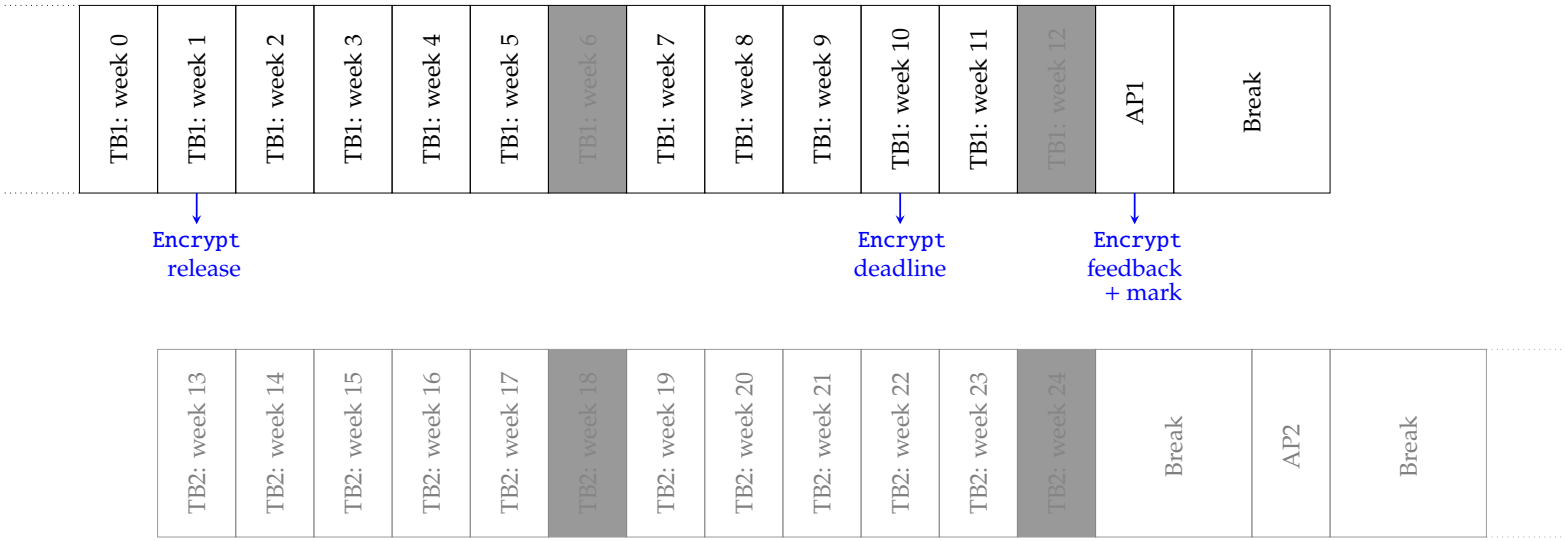
noting that, crucially,

1. a detailed design for ENC,
2. test vectors for ENC, i.e., sample inputs and outputs, and
3. a skeleton implementation plus build system,

are *all* provided.

- Question: "*when* should I start; *when* should I invest effort"?

- Question: "*when* should I start; *when* should I invest effort"?
- Answer: basically, recall that



and so *could* start ≃ week 5, whereas *should* start ≃ week 7.

- Question: "*how* should I start; *how* should I invest effort"?

- Question: "*how* should I start; *how* should I invest effort"?
- Answer: basically,
  - attempt to complete relevant lab. worksheet(s),
  - work step-by-step through stages, e.g.,
    1. invest in understanding problem and, e.g., tools, workflow, etc.,
    2. produce an on-paper design,
    3. implement the design,
    4. test the implementation,
  - note that said stages are only *somewhat* dependent, e.g.,

$$\text{stage 1} \rightsquigarrow \text{stage 2}$$

but

$$\text{stage 2} \not\rightsquigarrow \text{stage 3, 4}$$

- Question: "I'm concerned about academic integrity, and, e.g., plagiarism"?!

- Question: "I'm concerned about academic integrity, and, e.g., plagiarism"?!
- Answer:
  1. an accessible overview can be found at

     https://www.bristol.ac.uk/students/support/academic-advice/academic-integrity

  2. the more detailed policy can be found, e.g., via Sec. 3 of

     https://www.bristol.ac.uk/academic-quality/assessment/codeonline.html

  3. we do apply (semi-)automatic tools to identify potential transgression.

- Question: "the assignment description is *how* many pages"?!

- Question: "the assignment description is *how* many pages"?!
- Answer: keep in mind that the bulk of those pages capture
  1. various diagrams,
  2. various appendices (which offer additional detail and, e.g., a fully-worked example),

  meaning the central content is *much* shorter (i.e., ~ 4 pages)!

- Question: "there are lab. worksheets at the same time, i.e., should I do *both*"?

- Question: "there are lab. worksheets at the same time, i.e., should I do *both*"?
- Answer: no, not necessarily, in the sense each such worksheet says

> During the period of time aligned with this lab. worksheet, there is an active (or open) coursework assignment for the unit. You could address this fact by dividing your time between them. However, our (strong) suggestion is to view the former as of secondary importance (or optional, basically), and instead focus on the latter: since it is credit bearing, the coursework assignment should be viewed as of primary importance. Put another way, focus exclusively on completing the latter before you invest any time at all in the former.

Conclusions (1)

- Take away points: the assignment is designed to (ideally) balance

1. short-term challenge:

intellectual	:	demands *thinking* versus simply *doing*
technical	:	stresses formative understanding of some concepts, resources, etc.
definitional	:	some aspects are partially defined, or go beyond taught content
logistical	:	demands effective planning and time management
	⋮	

2. long-term outcome:

rewarding	:	simulate (limited) experience of *real* versus explanatory task
useful	:	hands-on vehicle for exploring (and understanding) taught content
	⋮	

in the sense that the former aren't negative, *provided* the latter are true.

Questions?

References