COMS30048 hand-out: how to get the most out of this unit

1. Objective

Put simply, after completing this unit you *should* be able to understand *and* apply concepts relating to

1. implementation techniques, e.g., multi-precision arithmetic
2. implementation attack and countermeasure techniques, e.g., timing attacks, constant-time implementation
3. cryptographic protocols and systems, e.g., TLS

set within the more general context of cryptology.

2. Organisation

- *Everything* is driven via the Blackboard-based unit web-site at

  http://www.ole.bris.ac.uk

  which links to all relevant (internal *and* external) resources. It is worth investing time to familiarise yourself with it *now*, so, e.g., you are aware of the resources available and can therefore capitalise on them *later*.

- At a high(er) level, the unit is delivered as a set of themes (or parts)

  Theme #1 ⇒ "implementation challenges"
  Theme #2 ⇒ "security challenges (i.e., attacks and countermeasures)"
  Theme #3 ⇒ "use-cases, examples, and case-studies"

  by the following members of (academic) staff

  Dr. Daniel Page ⇒ Lecturer and Unit Director
  Dr. David Bernhard ⇒ Lecturer

  plus a wider team who act in Teaching Support Roles (TSRs), e.g., as lab. demonstrators.

- At a low(er) level, the unit involves the following[1] activities

  lecture slot ⇒ synchronous, i.e., timetabled
  ⇒ in-person

  lab. slot ⇒ synchronous, i.e., timetabled
  ⇒ in-person

  More concretely, and bar selected exceptions, activities during each slot can be described as follows:

  lecture slot ↦
  - we provide an explanation of some technical topic(s),
  - you get help and feedback via n-to-m, collective discussion,
  - the slot is synchronous, meaning it will appear in your personal timetable.

  lab. slot ↦
  - we provide some hands-on (e.g., implementation or experimentation) tasks,
  - you get help and feedback via 1-to-1, personal discussion,
  - the slot is synchronous, meaning it will appear in your personal timetable.

[1] http://www.bristol.ac.uk/timetables/TimetablePDF.pdf?unit=COMS30048

3. Assessment

- In general, and in somewhat formal terms, two styles of assessment

$$\text{formative assessment} \mapsto \left\{ \begin{array}{l} \text{typically carried out } \textit{during} \text{ the learning process, intended to } \textit{improve} \\ \text{student performance (e.g., identify difficulties), so is normally not credit bearing} \\ \text{and offers qualitative feedback} \end{array} \right.$$

$$\text{summative assessment} \mapsto \left\{ \begin{array}{l} \text{typically carried out } \textit{after} \text{ the learning process, intended to } \textit{monitor} \\ \text{student performance (i.e., assign a mark to each member of and/or rank the} \\ \text{cohort), so is normally credit bearing and offers quantitative feedback} \end{array} \right.$$

  could each be delivered in various modes.

- For this unit specifically,
  - there is no formative assessment: the primary sources of help and feedback are 1) engagement during the lecture and lab. slots, plus 2) a set of dedicated feedback sessions during week 18,
  - summative assessment is captured by

$$\begin{array}{rcll} \text{summative coursework assignment} & \rightsquigarrow & \text{TB2, week 24} & \\ & \mapsto & \text{100\% weight} & \simeq \text{ 20CP} \end{array}$$

4. Help!

The following content attempts to offer informal help with respect to this unit. Keep in mind that various more formal, UoB-wide policies both exist and may apply: various pertinent examples, e.g., the UoB Student Agreement and Acceptable Behaviour Policy, are collected at

https://www.bristol.ac.uk/secretary/student-rules-regs

4.1. Common questions

I have a question: who can I ask it to, and how can I ask it? Asking questions is vitally important. Do not let the who or how delay or prevent you asking: there is no "incorrect" approach. That said, the most effective approach is somewhat dependant on the question type. Our preference is that you adopt the following guidelines, therefore.

The first type would be a *specific* question, i.e., one which is specific or even personal to you; examples of this type might include "my implementation for question X in lab. worksheet Y does not work correctly; can you help me debug it?". For this type, the best mechanisms are 1) ask it during a lab. slot, or 2) ask it using an email, ideally to the member of academic staff delivering the relevant part of the unit. The second type would be a *generic* question, i.e., one for which discussion or an answer might benefit everyone; examples of this type might include "I cannot understand the concept in week X, lecture slot Y, slide Z; can you explain it in more detail?" or "you said X, but what about Y: could that be an option in situation Z?". For this type, the best mechanisms are 1) ask it during an lecture slot, 2) ask it using the forum, which is accessible via the unit web-site. With respect to the forum, keep in mind that:

- UoB maintains and, in certain cases, enforces a policy related to acceptable behaviour.
- The forum supports peer-based learning, e.g., student-to-student, as well as student-to-staff discussion.
- We respond to questions first-come, first-served, and best-effort basis: try to be patient, especially during busy and out-of-hours (i.e., outside the working week and/or term time) periods.

What should I do and when; how should I organise my time? The short answer is that *you* have to find a way of working that suits *your* circumstances and preferences. Put another way, the unit is deliberately as flexible as possible: various approaches will be viable as a result, but it is unlikely any specific approach will suit everyone.

As an aside, note that all units are subject to a policy[2] intended to calibrate your expected workload. Put simply, any unit associated with x Credit Points (CPs) expects an average investment of $10 \cdot x$ hours of

[2] See https://www.bris.ac.uk/unit-programme-catalogue/WorkloadStatement.jsa?orgCode=COMS.

effort to obtain an average mark. We are (very) careful to align with this expectation, calibrating the unit accordingly. However, using average as a qualifier is important: the reality could legitimately differ from this expectation on a per student basis, and so for you specifically. For example, maybe 1) you find the unit harder than others, so need to invest more effort to get the same mark, or 2) manage your overall workload (when considering other units), so compromise by accepting a lower mark by investing less effort.

Can you recommend a textbook for this unit? Unlike some others units, we deliberately avoid recommending a single textbook for this unit. Our rationale is that multiple suitable textbooks exist, and there is no definitively best choice: each instance uses a different approach or style to some extent, so may be a better choice, e.g., 1) to match the requirements of a given student, or 2) as a result of a offering a different perspective of a given topic. Instead, *every* set of lecture slides concludes by citing a list of relevant textbooks (and other, e.g., online, resources) you can use to enhance or solidify your understanding.

Do I need to attend a slot X, or all versus some of a slot Y? On one hand, no: unlike some others units, we do not operate an attendance reward or non-attendance penalty for this unit. In that sense, therefore, and modulo the impact it could have on your learning, you can opt to attend or not attend as much or as little of any slot as you want or need to.

On the other hand, yes: engagement with and attendance at activities related to this unit are clearly important to your learning outcomes. In more detail, various patterns of behaviour are strong indicators of an underlying problem; these often result in failure of the unit, and might carry-forward to produce failures in *other*, subsequent units. In a general sense, and based on the observed behaviour and academic performance of students, if you

- do not attend the lecture slots,
- do not attend the lab. slots,
- do not read/watch the teaching material provided,
- read/watch *only* the teaching material provided,
- consider the functional quality of your work alone,
- start the coursework assignment(s) late,
- fail the coursework assignment(s),
- fail the exam

then there is a problem. It is important to identify if, when, and why such cases apply to you: irrespective of what the underlying problem is, we can and will do everything we can to help you solve it. However, we can only do so *if* 1) you actually talk to us[3], and 2) you do so early enough to formulate and implement a solution: asking for help 1 day before a deadline is, for example, less ideal than $n > 1$ days before that deadline.

Why do I need to register my attendance at slot X? There is no negative implication nor penalty for not registering or forgetting to register attendance: this is a mechanism put in place simply to 1) allow engagement monitoring, e.g., to identify students who may need additional support, and 2) satisfy the visa requirements of certain students. Note that we cannot and so will not retroactively register attendance for you, if, for example, you forget to do it yourself.

How do I register my attendance at slot X? Either

1. download, install, and use the native app[4] available for Android and iOS, or
2. directly use the web-based app available at

   https://check-in.bristol.ac.uk

noting the latter is also linked to via the `Attendance` menu item on the left-hand side of the Blackboard-based unit portal.

The lab. slot in my personal timetable differs from student X: why, and what is the difference between them? There is no difference between them: they exist simply to cope with the cohort size and room capacity. Although there are $n > 1$ lab. slots for the *unit* per week, we only expect *you* to attend 1 of them (which is shown in your personal timetable).

Are the lab. worksheets assessed? No, the lab. worksheets are *not* assessed. Therefore, note that 1) there is no requirement to submit anything, e.g., via Blackboard, and 2) there is no negative implication nor penalty if you want (e.g., for revision) or need (e.g., because you have fallen behind) to work on tasks in the worksheet for week $j \neq i$ during week i: there will be help available in *any* of the lab. slots.

[3] The meaning of "us" here is the most general possible; see for example http://cssbristol.co.uk/wellbeing.

[4] https://www.bristol.ac.uk/students/support/it/software-and-online-resources/registering-attendance

4.2. General advice

Accept the fact that teaching and learning is *not* adversarial. In all aspects of your time at UoB, our view is that adopting a "staff versus students" attitude is counterproductive. Rather, your academic achievement is a shared aim. Clearly topics of disagreement will arise, we will sometimes make mistakes, and we will sometimes deliberately challenge you to elicit some outcome. Even so, it is fundamentally important you trust that we will make our best effort to serve your best interests: we *want* you to do well. This is the essence of collegiality[5], which extends beyond staff-student into student-student interaction. Put simply, treating your peer group as form of "competition" rather than source of help and inspiration is equally counterproductive. We *all* need help, and your peer group will often be best placed to provide it; your time at UoB will will be enriched if you value and so act on this fact, for example through engagement with the CSS[6] and beyond.

Consider an example: ignoring the above can lead to students mistaking "I find X hard" for "X is *too* hard" or even for "you have *made* X too hard unnecessarily". The fact X is included in the unit implies that, in our view, there is value in you mastering it: it is *not* included for our benefit or amusement, nor with any intent to trick or demoralise you. Obviously we will *help* you master X using the most effective approaches we can, but, even so, sometimes X *is* hard so demands a significant effort on your (and our) part.

Take ownership of your own academic experience. Although a rich literature[7] underpins this point, the blunt, more colloquial fact is that we will not "spoon feed" you with respect to your education. We will provide appropriate material and support, but *you* must take advantage of it; doing so demands that you take responsibility for (or "own") your academic experience, which can then be described as facilitated rather than controlled by us. On one hand this may be intimidating, and *will* require motivation, organisation, and independence on your part. On the other hand it will be more fulfilling, and, ultimately, more effective in the longer term.

Embrace the challenge. This unit will attempt to emphasise

$$\text{problem definition} \rightsquigarrow \text{synthesis of ideas} \rightsquigarrow \text{solution}s$$

within many of the activities you engage in. Some students are confused by or even dislike this emphasis, so why do we adopt it? Or, rather, why do we ask you to formulate ideas (versus just do what we we specify) and why highlight a need for solution*s* (versus one solution)?

1. The term synthesis relates to combining different aspects of your ideas and research, and that of others, to produce new ideas. In other words, we want you to be comfortable with absorbing existing, background knowledge and skills, then using that background to formulate your own solutions to a problem.
2. It is rare that a only single solution to a given problem exists; often, multiple valid (i.e., functionally correct) solutions will exist, each representing a trade-off with respect to some quality metric(s). Likewise, it is rare a solution is produced without some amount of iteration. More often, successive cycles of

   $$\text{design},\ \text{implement},\ \text{evaluate},\ \textit{re}\text{design},\ \textit{re}\text{implement},\ \textit{re}\text{evaluate},\ \ldots,$$

   using the quality metric(s) to progressively approach a solution that is fit for purpose.
3. In both of the above, failure is *not* negative provided you learn from it. For example, the failure of one design to meet a quality metric might be a necessary step (e.g., providing useful information) toward a redesign that does. The same is true with respect to *your* learning, in the sense that adversity (e.g., failure, problems, bugs, etc.) can/should offer crucial learning experiences if the correct mindset is employed.

Likewise, it favours

$$\text{(deep) understanding of underlying concepts} > \text{(shallow) understanding of ad hoc solutions},$$

via exploration of and experimentation with said concepts set within a context of concrete, ideally *real* (or at least useful) examples and activities. Same question: *why*?

[5] http://en.wikipedia.org/wiki/Collegiality

[6] http://cssbristol.co.uk

[7] In short and formal terms, you might encounter units that adopt a teaching-centered paradigm or a learning-centered paradigm. The former is more traditional in higher education, usually comprising of a lectures whose focus is on information delivery (which will, by definition, be somewhat detached from the context it is used in) by a lecturer to largely passive students. In contrast, the latter has students learn in a more active manner by actually doing things in a given lecture (facilitated by a lecturer); doing so is more naturally aligned with concrete use-cases, and often blends acquisition of knowledge and skills. There is no right and wrong here: each paradigm has a valid format and purpose, so might reasonably be employed within this, and other units to suit different requirements.

Note that the preference for real versus "toy[8]" examples should be obvious: they are simply more interesting, more compelling, and more useful. Indeed, for many people, the ability to understand and explain the world (or artefacts in it, e.g., computers) is reason enough to study it. Such advantages are not without a cost, however: some concepts and most real examples will typically have an inherently higher degree of technical detail. As such, and in combination with the first point above, a fundamental understanding of the underlying concepts

1. acts as a means of cope with (i.e., avoid being "lost in") this detail,
2. supports innovation (versus simply reproduction): when faced with a non-trivial problem without a known solution, you cannot expect to "hack together" or "copy-and-paste" something suitable!

Avoid treating instances of overlap and repetition at face value. In some cases, you may encounter a given topic multiple times; this can occur in intra-unit (e.g., two lectures within the same unit cover the same topic) *or* intra-unit (e.g., two lectures within two, different units cover the same topic) forms, either way implying some degree of overlap and hence repetition. Uncontrolled instances of this are clearly unattractive: it is simply a waste of time, for both you *and* us. Typically this would hint at a problem in our curriculum design, that you should highlight (e.g., in any unit feedback, of via the SSLC) so we can address it.

However, keep in mind that there *are* instances where some controlled form of repetition is either necessary or useful:

- it could be that the repetition is by design, e.g., to highlight the importance of a topic, and thus prompt revision to ensure a strong understanding,
- it could be that a single topic is considered differently, from different (even deliberately contrasting) perspectives or for different purposes; it might *seem* like repetition at face value, but the differences suggest otherwise,
- for an open unit the topic cannot be assumed background for what is likely a mixed cohort.

Be aware of what teaching material is available. We provide a diverse range of teaching material, designed to cater for various teaching and learning styles. For example, you may get access to

- lecture slides,
- lecture videos, including those captured by Re/Play (née Mediasite),
- lecture handouts,
- extended sets of notes,
- suggested reading lists,
- problem sets for use as revision,
- problem sets (i.e., lab. worksheets) for use in lab. slots.

Be aware of what feedback is available. You will receive information about the work you have done, or, equally, are current doing, via a number of mechanisms; this is true whether or not that work is assessed. For example, you may

- get a personal (or general), hand-written marking report (e.g., on a printed hard-copy, or electronically),
- get a personal auto-generated marking report (e.g., via an auto-marker provided, or electronically),
- get a verbal marking report (e.g., during a viva),
- present your work to an audience (e.g., via a poster, or oral presentation),
- discuss your work in a lecture slot (e.g., recapping a coursework solution, or solving example problems),
- discuss your work in a lab. slot (e.g., with a lab. demonstrator),
- discuss your work on a forum (e.g., via Blackboard),
- discuss your work in a tutorial (e.g., a personal tutorial, or a problem class),
- discuss your work in a meeting (e.g., office hours, or scheduled appointment).

It is important to understand two points. First, *all* of the above are forms of feedback: each may have both positive and negative features, but do not mistake the first one, which is the traditional norm, as the *only* valid instance. Second, some of the above will be *available* to you. This fact is true whether or not you access them, and even though some may be harder to access than others (e.g., scheduling a meeting with someone to ask a question may be harder than using an online forum). Put another way, take care not to confuse your lack of need for or access to some form of feedback for it being unavailable.

Understand how to ask effective questions and interpret answers. Getting the help you need can hinge on asking an effective question: it can help a *lot* if you clearly articulate detail such as 1) what are you trying

[8] http://en.wikipedia.org/wiki/Toy_problem

to achieve, 2) what platform (e.g., hardware and/or software) are you using, 3) what problem have you encountered (e.g., does X not work as expected, do you not understand Y), and 4) what have you tried so far to resolve it. Fundamentally, it is a mistake to treat the person you are asking as a perfect "oracle[9]" of some sort: better to accept you engage in a conversation that you can get some insight, advice, and help from, and thus learn from, rather than *simply* get the/an answer from. For example, it might make no sense to offer a complete solution if, by doing so, we deem you will not learn anything. Instead, we might offer a suggestion of what you could do as a step toward producing a solution of your own. Keep in mind the following classes of question, and the rationale for how we might interpret them:

Question you ask	:	"I don't understand X" or "Y doesn't work"
Problem we see	:	Insufficient synthesis (or connection of concepts)
Solution	:	Instead ask "I read W and X; I think I understand Y, but I don't see how to apply Z" or "the description says W, but I can't tell whether that means X or Y because Z"
Question you ask	:	"Can I assume X"
Problem we see	:	A missed chance to explore alternatives
Solution	:	Instead ask *yourself* "*if* I assume X, what will positive impact could this have?" or "*if* I assume X, what will negative impact could this have?", then reassess whether it is *reasonable* to assume X
Question you ask	:	"Is approach X the correct one for problem Y"
Problem we see	:	A belief there is a single correct way to solve Y, or fear of even *trying* an X
Solution	:	First 1) list a set of possibilities, 2) list a set of metrics, 3) use 1) to rank 2), *then* ask "does this analysis seem robust, or am I missing something"

Understand nuanced terminology in written questions. Although it is difficult to be perfectly consistent, written questions within the context of this unit will often use terminology which hints at how to produce and/or what is expected from a solution. Some examples include:

- If a question that asks for a "block diagram" of some X, this is typically hinting the solution can be at a level of abstraction suited to the context, i.e., it can potentially ignore detail at a low level of abstraction. If X is a combinational logic design, for example, then the solution might be expressed in terms of 1) logic gates, and/or 2) pertinent building block components, e.g., multiplexers, but *not* transistors: the latter would be too low a level of abstraction, and the solution too complex therefore.
- If a question that asks you to "specify" some X, this is typically hinting the solution involves a precise, formal rather than a imprecise, discussed element.
- If a question that asks you to "explain" some X, this is typically hinting the solution would focus on describing and explaining the form and/or function of X (e.g., how X delivers the required function, why it is correct).
- If a question that asks you to "justify" or "evaluate" some X, this is typically hinting the solution would focus on evidenced reasoning the form and/or function of X (e.g., why the form of X is as presented, what alternatives exist, how those alternatives compare).
- If a question that asks for a "brief" solution, this is typically hinting it should aim to be clear and concise, e.g., a paragraph at most; it would not necessarily need to expand on, e.g., the possibility for alternative approaches, trade-offs, etc.

Understand the fact that we do not control *everything* you experience. To some extent, the staff associated with this unit act as the obvious "public face" and thus first point of contact. However, delivery of *any* unit depends on a wide range of support services. For example, consider the following:

- You will attend lectures slots in lecture theatres *throughout* UoB, not *just* in MVB; these are managed centrally by the Learning Facilities Management (LFM) group. You can contact them via

  https://www.bristol.ac.uk/directory/learning-facilities

  e.g., if there is a problem with room temperature.

[9] http://en.wikipedia.org/wiki/Oracle

- You will attend lab. slots in the MVB Linux lab(s). (e.g., MVB-1.15 or MVB-2.11); these are managed centrally by the Faculty IT Support Team, which forms a subset of IT Services. You can contact them via

  https://www.bristol.ac.uk/it-services

  e.g., if there is a problem with some hardware and/or software, or you cannot access your account.
- You will access teaching material via the Blackboard online learning environment; this is managed centrally by the Digital Education Office (DEO). You can contact them via

  https://www.bristol.ac.uk/digital-education

  e.g., if Blackboard is unavailable or does not function correctly.
- Your exam timetable (i.e., when and where *written* exams are: note this does not include coursework or non-written "exams" such as vivas) is managed by the Exam Office. You can contact them via

  http://www.bristol.ac.uk/directory/exams

It is important to understand two points. First, we can and will help resolve any problems you encounter with the support services listed above. That said, however, it may be easier if you make *direct* contact with them: often we will simply pass the problem to the appropriate contact, which you could do yourself. Second, keep in mind that we may little or even no control over some of the support services. For example, members of staff are *users* of Blackboard in largely the same way you are. Put another way, it is useful (for us) if you separate the delivery of the unit (i.e., teaching) from the delivery of support services. This will mean, for example, that feedback concerning the latter cannot be misattributed to the former (or vice versa).