FIT2093 Introduction to Cybersecurity - 2023

Assignment 1: Investigating an Application of **Cryptography**

Purpose	*Cryptography can be used in many applications to solve cybersecurity problems. The goals of this assignment are to explore in more depth how cryptography can be used for the security of an application of your interest, to apply cryptography effectively in practice, and learn about vulnerabilities that can arise if it is used incorrectly.*
Your task	*Prepare a group report and both group and individual video presentations for a chosen cryptography topic. This is followed by a set of individual practical tasks on different aspects of cryptography to be done via Moodle*
Value	**30**% of your total marks for the unit
Page / Time Limit	Group **Report: 10 pages** (not including references) **Group Video** Presentation: up to **6 minutes** **Individual Video** Presentation: up to **5 minutes**
Due Date	**7 April 2023 11:55 pm Melbourne time**
Submission	Part 1: ● Group Report as a **pdf** via Moodle assignment submission. ● Group and individual videos as **mp4**s via Moodle assignment submissions. ● Turnitin will be used for similarity checking of all written submissions. Part 2: ● Complete the untimed quiz in the Moodle assessments section.
Assessment Criteria	*Part 1: See the assessment criteria given in section 1 below.* *Part 2: See the assessment criteria in the document titled "Assignment 1, Part 2: Submission Guidelines Document" on Moodle.*
Late Penalties	● 10% deduction per calendar day or part thereof for up to one week ● Submissions more than 7 calendar days after the due date will receive a mark of zero (0) and no assessment feedback will be provided.
Support Resources	See appendix 1 and 2 for how to search and advice on good research sources
Feedback	Feedback will be provided on student work via: ● general cohort performance ● specific student feedback ten working days post submission

Overview of the assignment

Form a **group of 2~3** among classmates in your tutorial session, and choose the group leader, who will make the group submissions.
Note: If you are unable to find a group to join (e.g. by talking to other students in your tutorial session), please contact your tutor ASAP, and your tutor will find a group for you to join.

In **Part 1** of the assignment (weight: 20% of your unit mark), your group is to prepare a **group report** on the literature to compare approaches of using cryptography in a security application of your group's choice. Examples of security application topics are given in **Appendix 1**. Your report structure will follow the sections given in the `Assignment details' section below. Your team will also prepare a 6-minute **group video** about the key findings while each team member **individually** will prepare a 5-minute reflective **individual video** about the work.

After this, in **Part 2** of the assignment (weight: 10% of your unit mark), each student will individually complete the **practical tasks** on Moodle, to improve your understanding of how to use cryptography effectively for security, and how vulnerabilities can be exploited by attackers to break security if cryptography is not used correctly.

Part 1 Assessment criteria

- Group Report - full marks 100 (weight: 10% of the unit marks)

Item	Criterion	Marks
Group Report	Quality and depth of understanding of the **security application** protocol/system and its applied **cryptographic** techniques	20
	Quality of discussion and depth of understanding of protocol/system **performance/usability** results	20
	Quality of discussion and depth of understanding of application protocol/system security **vulnerabilities** or **analysis** results	20
	Quality and depth of **critical analysis** and **comparison** of results in the reviewed papers in the context of the security application	20
	Presentation **quality** and **clarity** of all sections	20

- Group Video - full marks 100 (weight: 5% of the unit marks)

Item	Criterion	Marks
Group Video	Quality of description of the **security application** protocol/system and its applied **cryptographic** techniques	20
	Quality of discussion on the **performance/usability** results	10
	Quality of discussion on the protocol/system's security **vulnerabilities** or **analysis** results	20
	Quality of **critical analysis** and **comparison** of results in the reviewed papers in the context of the security application	20
	Presentation **clarity** and **creativity**	30

- Individual Video - full marks 100 (weight: 5% of the unit marks)

Item	Criterion	Marks
Individual Video	Description and quality of your **individual contributions** to the group work	30
	Quality and appropriateness of description of real-world **scenario**	10
	Quality and appropriateness of key **threats** and **countermeasures** for that real-world scenario	20
	Clarity and appropriateness of descriptions of **privacy** and **ethics** issues related to the application	20
	Overall video **presentation clarity** and **creativity**	20

Assignment details

Assignment 1 consists of two parts: Part 1 literature review and Part 2 practical exercises. Part 1 is further divided into 3 subparts containing a group report, a group presentation and an individual presentation. Part 2 is an individual exercise which should be completed entirely on your own. This assignment is worth **30%** of the total unit marks.

Part 1 : Investigating a Security Application of Cryptography

In this part, your task is to work in a group to investigate a security application of cryptography. Your group will review the cybersecurity literature to research and compare approaches/algorithms/mechanisms in a security application of your group's choice.

Submissions Requirement:

(a) Group Report

Group leader submits Part 1 **Group Report** via Moodle on behalf of the group.

- **Report File Format.** You must submit the report as a **pdf** file. The maximum page limit for the report is **10 pages (not including references)**. You may use any way of generating a pdf output report. A possible way could be to use Microsoft Word (*ask Google for examples of showing different things*) or you may use LaTeX with the free Overleaf[1] web-hosted editor in Springer LNCS format.

- **Report Contents.** Research the literature on your chosen security application of cryptography and write a group report on your findings. Your report should cite and critically discuss and compare at least **two** relevant (*and credible, e.g. highly cited or published in a reputable journal or conference*) research papers from the research literature. In addition to these research paper sources, you can also cite other references (e.g. books).

  You can find relevant research papers and their citation numbers by searching using search engines customised for finding research papers, such as Google Scholar (scholar.google.com) or Microsoft Academic (academic.microsoft.com). Please refer to the Reference section in this document.

  Note: *You* ***must*** *cite any sources you used in writing your report (see academic integrity warning at the end of this document for more information).*

- **Report Structure.** Your report should contain the following sections:
  - **Group Names & Photos:** Name of your team, Names and student ID Numbers of the team members, Photos of team members
  - **Introduction:** An introduction to the chosen security application of cryptography and the security goals that the application requires/aims to achieve. Include a list of the main (2 or more) research papers you reviewed, and an overview of the contents of the rest of the report.

[1] https://www.overleaf.com/latex/templates/springer-lecture-notes-in-computer-science/kzwwpvhwnvf

- **Application Protocol/System Description**: Description of your chosen application protocol/system and its methods of applying the Cryptographic techniques to that chosen security application, including
  - types of cryptographic mechanisms used in your chosen application (e.g. encryption, signature or other cryptographic protocol), the main protocol steps or system stages, and how the cryptographic algorithms are used in the application.
  - threat/attack model: what are the assumptions about different parties involved in the application protocol/system, what are the main threats/attacks that the application protocol/system was designed to protect against.
  - any unusual/novel aspects or impacts of the cryptographic mechanisms used.

- **Application Protocol/System Performance & Usability Results**: A summary of the methods and results you found in your reviewed research papers (and/or other sources) about the performance and/or usability of your chosen security application protocol/system. You may use tables, graphs, screenshots, visualisations, etc. as appropriate to clearly illustrate and compare the results in your reviewed papers.

- **Application Protocol/System Security Vulnerabilities or Security Analysis Results:** A summary of the results you found in your reviewed research papers (and/or other sources) about security vulnerabilities or other security analysis results about your chosen security application protocol/system and any countermeasures proposed against the vulnerabilities. You may use tables, graphs, screenshots, visualisations, etc. as appropriate to clearly illustrate and compare the results in your reviewed papers.

- **Critical Analysis of Results:** A critical comparison and discussion of the results reported in the papers you reviewed (and any other sources) and their implication for security and practicality/usability of the cryptographic protocols/techniques for your chosen security application problem. You may consider aspects and relevant metrics such as security, accuracy, time requirements, memory requirements, cost/size/usability of hardware needed, etc. Your discussion may also point out areas where you think further improvements are needed to improve the practicality of the protocol/system in your chosen security application.

- **References**: list all references used in writing your report.

(b) Group Video Presentation

Group leader submits a group **Video** (in **mp4** format) of **up to 6 minutes** in total via Moodle that summarises the content in the group report. Each team member should take turns presenting in the video, with **facial video** as inset. The video should include all the sections in the Group report:

- The chosen security application/protocol and its applied cryptographic techniques
- Two performance/usability/vulnerabilities/security results from the papers reviewed in the report
- Your critical comparison and conclusions on the results obtained in those papers in terms of their security, usability, and practicality for your chosen security application.

You can use any video recording software, such as Zoom or Panopto, to record the video.

(c) Individual Video Presentation

In this part, you will work individually to reflect on your own contributions and your understanding of Part 1 Group Work, and submit a **video** of **up to 5 minutes** of presentation (*to be provided in due course on the Moodle Assessments page*).

Your video should cover the following points:

- **Your contributions**: give a summary of your contributions in the group report
- **Application Protocol Security Vulnerabilities & their impact.**
    - Find and describe a **real-world scenario** (*which can be a system or an application, e.g. an online book shop*) which is relevant to the security application considered by your group.
    - Explain the main relevant **security threats** in your scenario and their **risks** (likelihood of successful attack and potential damage from attack), and how the security vulnerabilities discussed in the group report can **impact** your chosen scenario.
    - Suggest the **mitigation** mechanisms used in your security application to address the threats and discuss any underlying **assumptions**, and how they reduce the relevant threat risk.
    - **Privacy**: discuss how the security application chosen by your group affects individual privacy, or give your reasons why privacy is not an issue
    - **Ethics**: discuss how the security application chosen by your group relates to ethical issues, or give reasons why ethics is not relevant

  Note: Your chosen real-world scenario should **differ** from the scenarios chosen by your group members.

Part 2 : Practical Crypto Attack / Exercises on Sagemath and Openssl

In this part, you will work individually to perform practical tasks to improve your understanding of cryptography and its pitfalls. Detailed submission instructions and assessment criteria for this part of the assignment are provided in a separate document on Moodle, titled “Assignment 1, Part 2: Submission Guidelines Document”. The Part 2 task details can be found in the “Assignment 1 Part 2: Submission (Unit Weight: 10%)” Moodle quiz.

Appendices

Reminders

Dos and Don’ts

Do	Don’t
Cite the reference of your sources including generative AI following the guideline as below	No group work in Part 1 individual video and Part 2 practical exercises
Photos should be placed on the report	
Your **face** should be shown clearly in the videos	

WARNING (Academic integrity): It is an academic requirement that your submitted work be original. Zero marks will be awarded for the whole submission if there is any evidence of plagiarism or contract cheating (i.e. paying another person to complete the assessment task). It is fine to use code or other material from various sources in your report. However, any material that you obtain from some source (e.g. website, book, paper, article) **must be cited** in the appropriate place in your report **and listed in the references section** of your report. Please also note that students must not work on this assignment with members of other assignment groups, and significant similarities between assignments submitted by different groups (other than those due to the same cited starting source code / dataset) will be investigated for evidence of plagiarism.

REMARK (Guidelines on Use of AI tools in the Assignment): ChatGPT or other AI tools may be used for study purposes, to learn about your topic, and to develop your assignment. However, similar to citation requirements for other references (see “Academic Integrity” statement above), you **must include a clear declaration of all generative AI tools used** (e.g. ChatGPT, DALL-E, Grammarly, voice-to-text), **how and where you have used them**. In particular, you should be aware that output of AI tools may not be factually correct and you should therefore critically evaluate the output generated by such tools for claim accuracy and appropriateness to the topic, using reliable sources, before incorporating such output in your assignment (e.g. an example declaration may be: ‘ChatGPT was used to generate an initial structure for the Introduction and Conclusion. I then edited this to correct factual inaccuracies, add citations to support claims, and strengthen the connection to my chosen topic and the ideas from other references that I referred to’).

Where to get help

What can you get help for?

English language skills

if you don’t feel confident with your English.

- Talk to English Connect: https://www.monash.edu/english-connect

Study skills

If you feel like you just don’t have enough time to do everything you need to, maybe you just need a new approach

- Talk to an academic skills advisor: https://www.monash.edu/learnhq/consultations

Things are just really scary right now

Everyone needs to talk to someone at some point in their life, no judgement here.

- Talk to a counsellor: https://www.monash.edu/health/counselling/appointments (friendly, approachable, confidential, free)

Things in the unit don’t make sense

Even if you’re not quite sure what to ask about, if you’re not sure you won’t be alone, it’s always better to ask.

- Ask in the forums or email your tutor:

  Teaching team: https://lms.monash.edu/course/view.php?id=155649&section=1

  Consultation: https://lms.monash.edu/mod/resource/view.php?id=11630825

I don’t know what I need

Everyone at Monash University is here to help you. If things are tough now they won’t magically get better by themselves. Even if you don’t exactly know, come and talk with us and we’ll figure it out. We can either help you ourselves or at least point you in the right direction.

Appendix 1. Choice of topics

You can pick any topic from:

- Cryptography in Mobile Phone networks
- Cryptography in WiFi networks
- Cryptography in Blockchains (Consensus protocols, cryptocurrencies, privacy-preserving cryptocurrencies, smart contracts, …)
- Cryptography in Database encryption and/or authentication
- Cryptography in Cloud (Infrastructure, data, applications..)
- Cryptography in Web security (e.g. SSL/TLS protocol)
- Cryptography in Virtual Private Networks (e.g. IPSec protocol)
- Cryptography in SSH secure login protocol
- Cryptography in Bluetooth wireless networks
- Cryptography in Trusted Execution Environments (e.g. SGX)
- Cryptography in Secure Messaging Apps (e.g. Signal protocol)
- Cryptography in Credit Card / EFTPOS payment systems
- Cryptography in Multi-factor authentication systems (e.g. Okta, Yubikey)
- Cryptography in Public transport systems (e.g. myki)
- Cryptography and AI / machine learning

For any other topic, please discuss with your tutor so we can ensure it is of equal difficulty.

Appendix 2 - Reference Page: Important tips for online resources

Online seminars in Monash's Cybersecurity Lab's website:
https://www.monash.edu/it/ssc/cybersecurity/seminars

Google Scholar's citation ranking:
https://scholar.google.com.au/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography

Research paper database:
DBLP http://dblp.uni-trier.de/ provides a very good starting point!

Some Good Journals:

- IEEE Transactions on Information Forensics and Security
    - http://dblp.uni-trier.de/db/journals/tifs/ (by IEEE Xplore)
- IEEE Transactions on Dependable and Secure Computing
    - http://dblp.uni-trier.de/db/journals/tdsc/ (by IEEE Xplore)
- Journal of Cryptology
    - http://dblp.uni-trier.de/db/journals/joc/ (by SpringerLink)

IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)

- https://tches.iacr.org/

Some Good Conferences:

- Crypto
    - http://dblp.uni-trier.de/db/conf/crypto/ (by SpringerLink)
- EuroCrypt
    - http://dblp.uni-trier.de/db/conf/eurocrypt/ (by SpringerLink)
- AsiaCrypt
    - http://dblp.uni-trier.de/db/conf/asiacrypt/ (by SpringerLink)
- ACISP
    - http://dblp.uni-trier.de/db/conf/acisp/ (by SpringerLink)
- ACNS
    - http://dblp.uni-trier.de/db/conf/acns/ (by SpringerLink)
- Theory of Cryptography Conference (TCC)
    - http://dblp.uni-trier.de/db/conf/tcc/ (by SpringerLink)
- International Conference on Practice and Theory of Public-Key Cryptography (PKC)
    - http://dblp.uni-trier.de/db/conf/pkc/ (by SpringerLink)
- RSA Conference Cryptographers' Track (CT-RSA)
    - http://dblp.uni-trier.de/db/conf/ctrsa/ (by SpringerLink)
- Financial Cryptography and Data Security (FC)
    - http://dblp.uni-trier.de/db/conf/fc/ (by SpringerLink)
- European Symposium on Research in Computer Security (ESORICS)
    - http://dblp.uni-trier.de/db/conf/esorics/ (by SpringerLink)
- ACM Conference on Computer and Communications Security (CCS)
    - http://dblp.uni-trier.de/db/conf/ccs/ (by ACM)
- ACM Asia Conference on Computer & Communications Security (ASIACCS)
    - http://dblp.uni-trier.de/db/conf/asiaccs/ (by ACM)

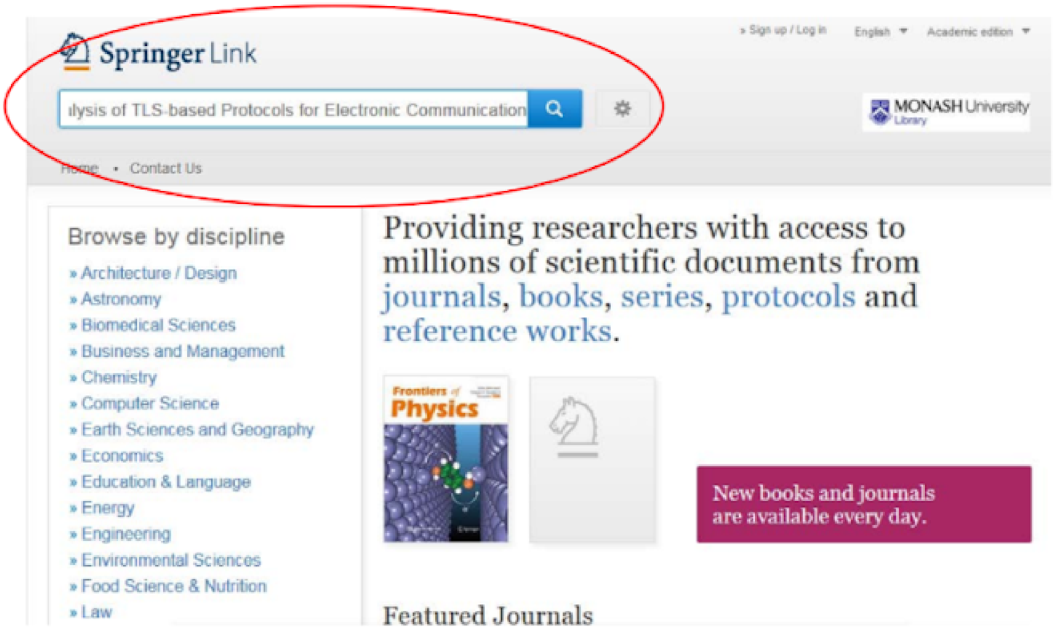
- USENIX Security Symposium (USENIX Security)
    - o http://dblp.uni-trier.de/db/conf/uss/ (by USENIX, open access)

Note: Exclude those affiliated workshops

- Network and Distributed System Security Symposium (NDSS)
    - o http://dblp.uni-trier.de/db/conf/ndss/ (by Internet Society, open access)
- IEEE Symposium on Security and Privacy (IEEE S&P)
    - o http://dblp.uni-trier.de/db/conf/sp/ (by IEEE Xplore)
- IACR CHES
    - o https://www.iacr.org/publications/access.php

How to download papers from IEEE, ACM and SpringerLink online library (through Monash account)?

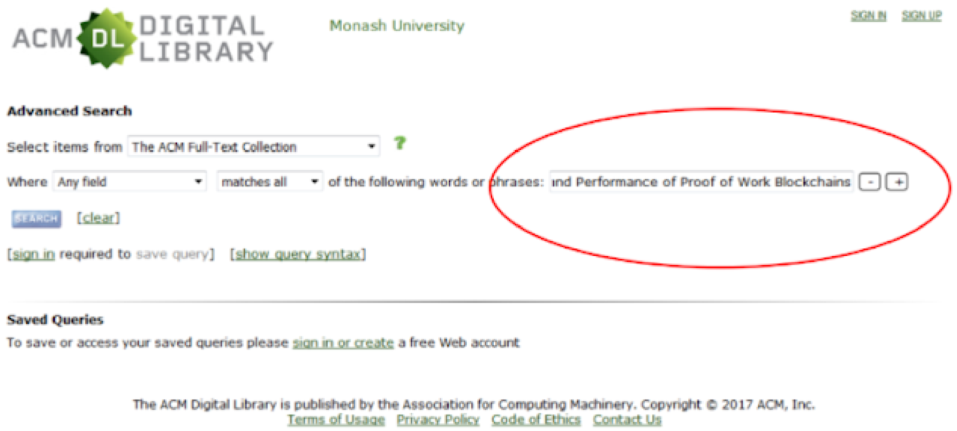
1. Go to Monash Online Library:
http://guides.lib.monash.edu/c.php?g=219820&p=1453413
2. Select the online sources (ACM digital library , IEEE Xplore or SpringerLink)
3. Use your Monash username/password to login
4. Type the paper title in the Search box



ılysis of TLS-based Protocols for Electronic Communication

Providing researchers with access to millions of scientific documents from journals, books, series, protocols and reference works.

New books and journals are available every day.



Advanced Search

Select items from The ACM Full-Text Collection ▾ ?

Where Any field ▾ matches all ▾ of the following words or phrases: ınd Performance of Proof of Work Blockchains

[sign in required to save query] [show query syntax]

Saved Queries

To save or access your saved queries please sign in or create a free Web account

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2017 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Change log

All changes to the assignment will be listed here with the time of the change (in Melbourne time):