32144 Technology Research Preparation

Week 8 Tutorial 7 Overview	
Topics Covered:	Choosing a Research Method Learning from the implementation of existing research methods Developing Your Research Method
Points:	6
Date Due:	Week 8 – In Class
Submission	In-class contribution to discussions

Week 08 Tutorial 07 Preparation

1. **UNDERSTANDING YOUR RESEARCH MODELS AND METHODS** – Provide answers to the following questions.

   a. What is the title of your Research Proposal…?

   Research proposal title: Mathematical solutions for Data Breach Prevention

   NB: Please list a few options to discuss with your tutor and breakout group to obtain feedback on.

   b. What is the Research Paradigm that your proposed Research Project will implement?

   Research Paradigm: Mixed research paradigm, however with an overwhelming majority of quantitative research methodologies.

   NB: Please choose the item that best describes your own proposal's research model/ paradigm*

   NB: Please refer to Week 7 Lecture Slides for definitions of terms, or discuss with your tutors.

   NB: If you are unsure of the meaning of other terms not covered by the Week 7 Lecture, please refer to the: SAGE Encyclopedia of Research Design

   c. What is the main research question you are addressing in your research proposal?

   Research Question: For the various fields in data breach prevention such as cryptography and anomaly detection, which mathematical models are ideal for practical implementation and how can they be extended upon?.

   NB: Please provide a description of your main research question. If you are dealing with a complex topic, you may wish to answer (d) below before providing a response to this question.

   d. Can your main research question be broken down into research sub-questions (or objectives).? List all sub-questions below (provide at least two).

   Research Sub-Questions: Which is the optimal approach to the post-quantum cryptography (lowest time complexity for encrypting, resistant to quantum algorithms etc)

   How can one expand upon ML models for spam filtering using new

innovations in AI?

NB: Please provide a description of your research sub-questions.

Week 08 Tutorial 07 Preparation Cont.

2. **COMPLETE THE FOLLOWING TABLE** – Using your research question and sub-questions, complete the following table describing the relationship between your sub-questions and related themes, the purpose of these themes and how they structure the research, and the anticipated outcome that you anticipate will result from the implementation of your research proposal.

   NB: Example responses are provided below. Please delete and provide your own.

Research Sub-Questions *List below your response to 1(d). That is , list the sub-questions that you will address in your research proposal.*	**Related Theme/s** *List and, if possible, expand on the related research themes that you have identified in your literature review. Map each theme to your research sub-questions and note any gaps.*	**Purpose of Theme** *Explain **WHY** the themes identified are significant to resolving the sub-questions listed.*	**Anticipated Outcomes** ***WHAT** are the anticipated outcome/s (the solutions, findings, or knowledge contribution) that result from the investigation – and **HOW** will they benefit/ support your stakeholder/s.*
Which is the optimal approach to the post-quantum cryptography ?	• lowest time complexity for encrypting • resistance to quantum algorithms	• Lower time complexity makes the solution more practical, hence more likely to be a standardised solution in the industry • Quantum resistance is the desired property intrinsic to the question; it is the crux of the problem itself	• Solution for cryptography that can be practially employed when quantum computing is available • Solution can be implemented by companies with lower amounts of financial and computational resources
How can one expand upon ML models for spam filtering using new innovations in AI?	• Improving model accuracy • Lowering time complexity of decision making	• Lower time complexity by using more efficient AI models is an advancement for practical spam filters	• Eventual demise of phishing attacks

NB: Please refer to Week 7 Lecture Slides for definitions of terms, or discuss with your tutors.

NB: If you are unsure of the meaning of other terms not covered by the Week 7 Lecture, please refer to the: SAGE Encyclopedia of Research Design.

Week 08 Tutorial 07 Preparation Cont.

3. **IDENTIFY ONE (OR MORE) EXEMPLAR RESEARCH ARTICLE/S BASED ON THE RELEVANCE AND APPROPRIATENESS OF THE ARTICLE'S RESEARCH MODEL & METHODS TO YOUR OWN WORK** – Prior to your tutorial you are required to identify and read a research article that utilises the same or similar research method that you may utilise to execute your research project.

Article Reference Details: Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017). Post-quantum RSA. *IACR Cryptology EPrint Archive*, *2017*, 351.

NB: Please use APA referencing

4. **ASSESS YOUR EXEMPLAR RESEARCH MODEL/ METHODS PAPER/S** – Once you have identified your exemplar research articles and assessed that they provide a potential and relevant research method, which you may utilise to execute your research project, provide responses to the questions below.

Research Paradigm: Quantitative

NB: Please choose the item that best describes the research model.

NB: Please refer to Week 7 Lecture Slides for definitions of terms, or discuss with your tutors.

NB: If you are unsure of the meaning of other terms not covered by the Week 7 Lecture, please refer to the: SAGE Encyclopedia of Research Design.

Application Domain: Application in essential cryptography that will be required to prevent data breaches once quantum computing is sufficiently developed.

NB: Please provide a brief summary of the application domain

Is the Application Domain the same or similar enough to your own research domain?: The application is a subset; it addresses one of the research sub-questions derived from the topic (that of the post-quantum cryptography problem).

NB: Please choose the item that best describes the similarity of the research article's domain to your own.

Summary of Research Methodology: Research model is referencing previous literature to inspire innovative ideas to improve RSA, and then conduct a computer simulation (controlling the key size) to determine the efficacy of the proposed idea (control & randomization)

NB: Please provide a brief summary of the research methodologies utilised

Why are the Research Methodologies relevant/ appropriate to your Research Proposal? Mathematics is quantitative by nature, hence an appropriate research method would use quantitative research methodologies to evaluate the efficacy of a model. Though this is a focus, small quantities of qualitative reseach methods should be employed to link results to practicality. The article does not mention this, however this is a part of the scope of our research proposal.

NB: Please prepare a few brief statements the reasons why the research methodologies utilised in the paper you have sourced are relevant and appropriate to your Research Proposal.

Week 08 Tutorial 07 In-Class Activities

1. **DEVELOPING YOUR RESEARCH METHOD**– Answer the following questions, and use the matrix to identify questions or concerns that you have about your developing research model and methodologies. Discuss them as a group or share common concerns.

   a. Check all that apply to your developing research model and methodology.

		Quantitative	☒	Qualitative	☐
Requirement	Question	Hypothesis	☐	Interest	☒
	Method	Control & randomization	☒	Curiosity & reflexivity	☐
	Data collection	Response	☒	Viewpoint	☐
	Outcome	Dependent variable	☒	Accounts	☐
Ideal	Data	Numerical	☒	Textual	☐
	Sample size	Large (power)	☒	Small (saturation)	☐
	Context	Eliminated	☒	Highlighted	☐
	Analysis	Rejection on null	☒	Synthesis	☐

NB: Please refer to Week 7 Lecture Slides for definitions of terms, or discuss with your tutors.

NB: If you are unsure of the meaning of other terms not covered by the Week 7 Lecture, please refer to the: SAGE Encyclopedia of Research Design.

2. **USING THE RESEARCH ARTICLE TO FURTHER EXPLORE METHODS** – Rate the level of relevance and appropriateness of the research article to your own research model and method? Briefly describe how – in what way – your research methods differ from those in the article…?

Articles Level of Relevance and Appropriateness to Your Own Research Proposal:

Partially relevant, research model is referencing previous literature to inspire innovative ideas to improve RSA, and then conduct a computer simulati(controlling the key size)todetermine the efficacy of the proposed idea (control & randomization)

NB: Please choose the item that best describes the level of relevance or appropriateness to your own proposal's research model and methodologies.

In What Way will Your Research Methods Differ from those described in the Article?

Click or tap here to enter text.

NB: Please describe how your own research methods may differ relative to the article you have sourced.

Week 08 Tutorial 07 In-Class Activities Cont.

3. **DEVELOPING YOUR DATA COLLECTION METHODS**– Answer the following questions, and use the matrix to identify questions or concerns that you have about your developing research model and methodologies.

a. Check all that apply to your developing data collection methods.

QUANTITATIVE	☒	QUALITATIVE	☒
Experiments	☒	**Observations**: recording what you have seen, heard, or encountered in detailed field notes	☒
Computer Simulation and Agent-Based Models	☒	**Interviews**: asking people questions in one-on-one conversations	☐
Controlled observations	☐	**Focus groups**: asking questions and generating discussion among a group of people	☐
Surveys: paper, kiosk, mobile, questionnaires	☐	**Surveys**: distributing questionnaires with open-ended questions	☐
Longitudinal studies	☐	**Secondary research**: collecting existing data in the form of texts, images, audio or video recordings, etc.	☐
Polls and Telephone interviews	☐		☐

b. Copy and paste the table that you have completed as part of your tutorial preparation activities and add an additional column as shown in the example below.

By adding this column, describe the type of data collection techniques that you will need to implement in your research to respond to your research sub-questions. ***Describe WHAT data collection methods and the type of data required to meet your anticipated outcome/s and HOW they will answer the research sub-question.***

Research Sub-Questions *List below your response to 1(d). That is , list the sub-questions that you will address in your research proposal.*	**Related Theme/s** *List and, if possible, expand on the related research themes that you have identified in your literature review. Map each theme to your research sub-questions and note any gaps.*	**Purpose of Theme** *Explain **WHY** the themes identified are significant to resolving the sub-questions listed.*	**Anticipated Outcomes** ***WHAT** are the anticipated outcome/s (the solutions, findings, or knowledge contribution) that result from the investigation – and **HOW** will they benefit/ support your stakeholder/s.*	**Supporting Data Collection Methods** *Describe **WHAT** data collection methods and the type of data required to meet your anticipated outcome/s and **HOW** they will answer the research sub-question.*
Which is the optimal approach to the post-quantum cryptography ?	• lowest time complexity for encrypting • resistance to quantum algorithms	• Lower time complexity makes the solution more practical, hence more likely to be a standardised solution in the industry • Quantum resistance is the desired	• Solution for cryptography that can be practially employed when quantum computing is available • Solution can be implemented by companies with lower amounts of	• Computer simulations with controlled key sizes • hypothesis testing on the mean time required among a sample of simulations

		property intrinsic to the question; it is the crux of the problem itself	financial and computational resources	
How can one expand upon ML models for spam filtering using new innovations in AI?	• Improving model accuracy • Lowering time complexity of decision making	• Lower time complexity by using more efficient AI models is an advancement for practical spam filters	• Eventual demise of phishing attacks	• hypothesis testing on the mean time required among a sample of simulations