Assessment Brief: Key Exchange Protocol Attacks

Assessment Title and Weighting

Coursework, 30% of the total grade.

Description of the Assessment Task

This is a group assignment where you will collaborate with one, two or three more students (up to maximum of 5 in a group on special request) in your class to produce a technical paper on Key Exchange Protocol attacks. A key exchange protocol is a method that generates a cryptographic key over a public and insecure medium such as the Internet. Diffie-Hellman (D-H) and RSA are two of the most widely used key exchange protocols. However, D-H and RSA are susceptible to specific attacks including, but not limited to, a man-in-the-middle attack and a timing attack, respectively. In this coursework, you will (1) explain one attack technique on D-H, (2) explain one attack technique on RSA, (3) implement D-H and RSA, (4) apply the attack techniques to attack D-H and RSA, (5) explain how to defend D-H and RSA from these attacks, (6) apply the defensive techniques to defend D-H and RSA, (7) compare and contrast the attacks on D-H and RSA, and (8) compare and contrast the methods you applied to defend D-H and RSA from these attacks.

You should organise your technical paper as follows:

- Title of your paper, author names, affiliations and University of Aberdeen student ID.
- Abstract, maximum 150 words.
- Introduction section.
- Related work section.
- Methods section:
- Results section.
- Discussion section.
- Conclusion and future work section.
- Authors contribution section.

Use of GenAI

Please review the information provided for students on Academic Integrity and Use of GenAI tools in the Course Assessment folder. If the use of GenAI tools is permitted, please read the guidance on how to acknowledge the use of GenAI tools (https://abdn.site/cad-genai-acknowledgements).

The permitted level of GenAI tool use is detailed below:

GenAI Level 0 – Not Permitted

You should not use generative artificial intelligence (GenAI) tools in your assessment. This includes (but not limited to): MS Copilot, ChatGPT, DALL-E, GitHub Copilot, Google Gemini, Perplexity AI, Deepseek, etc.

Assessment Criteria

After completing this coursework, the student will be able to:

- Explain the Diffie-Hellman and RSA key exchange protocols.
- Explain two attack methods on Diffie-Hellman and RSA.
- Explain two defensive techniques to protect Diffie-Hellman and RSA from these attacks.
- Implement the Diffie-Hellman and RSA key exchange protocols.
- Apply two attack methods on Diffie-Hellman and RSA.
- Apply two defensive techniques to protect Diffie-Hellman and RSA.
- Compare and contrast two attack methods on Diffie-Hellman and RSA.
- Compare and contrast two defensive methods for Diffie-Hellman and RSA.

Grading Criteria

All assessments are graded using the University's Common Grading Scale (CGS), which uses 23 points and 7 band descriptors from A to G. A full description of how each band is defined is available in the guidance on the Common Grading Scale (https://abdn.site/common-grading-scale). Please note that the grade awarded represents the standard of the work overall. Your assignment will be graded using the following criteria:

Band	Description
A	Work, which is largely and predominately characterised by evidence of the following: 1. Outstanding knowledge and understanding of concepts and theories 2. Superior skill and judgement in solving problems. 3. A consistently high standard of accuracy in reasoning and calculation 4. Ability to express arguments with a high level of precision. 5. Possibly signs of creative ability.
B	Work, which is largely and predominately characterised by evidence of the following: 1. Sound knowledge and understanding of most concepts and theories. 2. Ability to solve problems similar in general character to ones seen previously. 3. Reasoning and calculation generally accurate and correctly presented.
C	Work, which is largely and predominately characterised by evidence of the following: 1. Competence in understanding central concepts and theories. 2. Ability to produce standard lines of argument and calculations in problem solving. 3. Few totally fallacious arguments or inaccurate calculations.
D	Work, which is largely and predominately characterised by the following: 1. Ability shown in performing routine calculations and producing short logically correct arguments in familiar situations. 2. Limited understanding of the theory.
E	Work, which is largely and predominately characterised by the following: 1. An insecure grasp of basic concepts leading to nonsensical reasoning. 2. Ability to calculate correctly only in very restricted areas.
F	Work, which is largely and predominately characterised by the following: 1. A lack of knowledge and understanding of the basic theory thus making it impossible to produce reasoned argument or accurate calculations.

Submission Guidelines

By submitting your assignment you accept that your work is your own work and does not breach the University of Aberdeen Code of Practice on Student Discipline (https://abdn.site/student-discipline).

Please note that text-matching software such as Turnitin and/or SafeAssign will be used, where applicable.

Technical paper

You will format your paper using the IEEE conference proceedings style, double-column page, minimum 6 pages and maximum 8 pages. All tables and figures must be labelled, captioned and included within the paper. The paper must be written in English and carefully read and agreed by all authors. References will be formatted using the IEEE referencing style. The references section and author contribution sections are excluded from the page limit. Save your paper as one PDF file, and submit the PDF file to the coursework submission page.

Code

You can use any programming language such as Java, Python or C++ to implement D-H and RSA, implement the attacks on D-H and RSA, and implement the defensive methods to protect D-H and RSA from the attacks you implemented. Put all your code in one ZIP file and submit the ZIP file to the coursework submission page.

Extensions

You should apply for an extension by emailing your request (using your UoA email address) to uoa-ji-enquiries@abdn.ac.uk (mailto:uoa-ji-enquiries@abdn.ac.uk). Students should also include any supporting evidence where possible e.g medical letter. Please read the policy at Extensions and Late Submission of Work (https://www.abdn.ac.uk/staffnet/teaching/key-education-policies-for-students-11809.php#panel13739) for full details.