JC3012 (2025-26): Network Security Technology

Detailed marking scheme

Below is a detailed marking scheme for each section in your technical report.

A: **Abstract** (**5%**)

1. The aim of the technical report is described. - 1%
2. A method to attack Diffie-Hellman is listed. - 1%
3. A method to attack RSA is listed. - 1%
4. A method to defend Diffie-Hellman from the attack is listed. - 1%
5. A method to defend RSA from the attack is listed. - 1%

B: **Introduction section** (**5%**)

1. The method to attack Diffie-Hellman is described clearly. - 1%
2. The method to attack RSA is described clearly. - 1%
3. The method to defend Diffie-Hellman from the attack is described clearly. - 1%
4. The method to defend RSA from the attack is described clearly. - 1%

a. Items 1 to 4 listed above must tie to the methods listed in the abstract. If not, then for each mismatch subtract 1%.

5. A list of tasks performed is given. - 1%

C: **Related Work section** (**10%**)

1. Two papers that presented attack and defense methods on Diffie-Hellman are summarised clearly. – 4% (2% per paper)

a. These papers do not have to be recent ones.
b. These papers should be published in a peer-reviewed conference or journal.

2. Two papers that presented attack and defense methods on RSA are summarised clearly. – 4% (2% per paper)

c. These papers do not have to be recent ones.
d. These papers should be published in a peer-reviewed conference or journal.

3. The similarities and differences between the attack and defense methods in the technical report and the reviewed papers are summarised clearly. – 2%

D: **Methods section** (**40%**)

1. Two attack methods on Diffie-Hellman are compared and the reason(s) for selecting the attack method is described clearly. – 7.5%
2. Two attack methods on RSA are compared and the reason(s) for selecting the attack method is described clearly. – 7.5%
3. Two defense methods on Diffie-Hellman are compared and the reason(s) for selecting the defense method is described clearly. – 7.5%
4. Two defense methods on RSA are compared and the reason(s) for selecting the defense method is described clearly. – 7.5%
5. Metrics for evaluating the attack method on Diffie-Hellman are described clearly. – 2.5%
6. Metrics for evaluating the attack method on RSA are described clearly. – 2.5%

7. Metrics for evaluating the defense method on Diffie-Hellman are described clearly. – 2.5%
8. Metrics for evaluating the defense method on RSA are described clearly. – 2.5%

E: **Evaluation section** (**30%**)

1. Visuals such as line plots, bar charts, tables, etc. are used to present results for Diffie-Hellman. – 7.5%
2. Visuals such as line plots, bar charts, tables, etc. are used to present results for RSA. – 7.5%
3. Results from executing the attack and defense methods on Diffie-Hellman are summarised clearly. – 7.5%
4. Results from executing the attack and defense methods on RSA are summarised clearly. – 7.5%

F: **Discussion section** (**5%**)

1. Strengths and weaknesses of the attack method are described clearly. – 2.5%
2. Strengths and weaknesses of the defense method are described clearly. – 2.5%

G: **Conclusion and future work section** (**5%**)

1. Findings from the Evaluation section are summarised clearly. – 2%
2. Another attack and defense method on Diffie-Hellman is summarised clearly. – 1.5%
3. Another attack and defense method on RSA is summarised clearly. – 1.5%