



SDI Review Form 1.6

| | |
|--------------------------|---|
| Journal Name: | <u>British Journal of Mathematics & Computer Science</u> |
| Manuscript Number: | Ms_BJMCS_21889 |
| Title of the Manuscript: | Cryptanalysis and Improvement on an E-mail Protocol |
| Type of the Article | Original Research Article |

General guideline for Peer Review process:

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty**', provided the manuscript is scientifically robust and technically sound.

To know the complete guideline for Peer Review process, reviewers are requested to visit this link:

(<http://www.sciencedomain.org/page.php?id=sdi-general-editorial-policy#Peer-Review-Guideline>)



SDI Review Form 1.6

PART 1: Review Comments

| | Reviewer's comment | Author's comment <i>(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)</i> |
|--|--|---|
| <u>Compulsory</u> REVISION comments | | |
| <u>Minor</u> REVISION comments | <ul style="list-style-type: none">• All references mentioned in the paper are not the latest ones. There could be more work carried out in the related area from 2010 to 2015 which needs further investigation.• Usage of standard format for listing references is advisable.• Careful reading of the script before final submission is advised (man-the-middle attack used instead of man-in-the-middle attack) | 1, Yes, we have done 2, Yes, we have done 3, Yes, we have done |
| <u>Optional/General</u> comments | <ul style="list-style-type: none">• The literature survey is well documented.• The proposed method provides forward secrecy, overcomes replay attack, sender impersonation attack and confidentiality in the mail content is achieved. | |