

# RSA and El-Gamal Cryptosystems

Fadwa Bin Ishaq, Yanan Xiao, *Student Member, IEEE* Maryam Al Mehrezi

**Abstract**—In this paper we discuss the RSA and El-Gamal cryptosystem. Alongside we introduce our way of implementing them in Python and C.

**Keywords**—RSA, EL-Gamal, Implementation, Public Key, Cryptosystem

## 1 INTRODUCTION

THIS demo file is intended to serve as a “starter file” for IEEE Computer Society journal papers produced under L<sup>A</sup>T<sub>E</sub>X using IEEEtran.cls version 1.7 and later. I wish you the best of success.

mds  
January 11, 2007

### 1.1 Subsection Heading Here

Subsection text here.

## 2 PUBLIC KEY CRYPTOSYSTEM

PKCS

### 2.1 More Details

Some problems with this template...I mean, the subsubsection part.

## 3 RSA

This is just another testing case.

## 4 EL-GAMAL

El-Gamal

## 5 IMPLEMENTATION

Implementation process will be discussed here.

- Fadwa Bin Ishaq, Yanan Xiao and Maryam Al Mehrezi are with the Department of Electrical Engineering and Computer Science, Masdar Institute of Science and Technology, Masdar City, Abu Dhabi, UAE, 54224.  
E-mail: {fbinishaq,yxiao,malmehrezi}@masdar.ac.ae

## 6 CONCLUSION

Conclusion and Contributions.

### APPENDIX A

#### PROOF OF THE FIRST ZONKLAR EQUATION

Appendix one text goes here.

### APPENDIX B

#### SOME RELATED MATH STUFF WILL BE DISPLAYED HERE

Appendix two text goes here.

### ACKNOWLEDGMENTS

The authors would like to thank...

### REFERENCES

- [1] H. Kopka and P. W. Daly, *A Guide to L<sup>A</sup>T<sub>E</sub>X*, 3rd ed. Harlow, England: Addison-Wesley, 1999.



**Michael Shell** Biography text here.

**John Doe** Biography text here.

**Jane Doe** Biography text here.