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 LaTeX 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

I was so damn amazed by the power of Emacs. So damn powerful!

This is just another testing text. To test [1]. Yet another El-Gamal [2], [3].

- *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

5 Implementation

Implementation process will be discussed here.

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 Dr. Zeyar for his amazing lectures throughout the semester, as well as assigning us a challenging but rewarding project like this. In addition, we would show our gratitude to Masdar Institute for creating the world-class research environment.

References

[1] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over gf(p) and its cryptographic significance (corresp.)," *Information Theory, IEEE Transactions on*, vol. 24, no. 1, pp. 106–110, 1978.

[2] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *Information Theory, IEEE Transactions on*, vol. 31, no. 4, pp. 469–472, 1985.

[3] ——, "A subexponential-time algorithm for computing discrete logarithms over," *Information Theory, IEEE Transactions on*, vol. 31, no. 4, pp. 473–481, 1985.

Fadwa Bin Ishaq is a second year master student at Masdar Institute.

Yanan Xiao is a first year master student at Masdar Institute. For his undergraduate, he spent three years in information security related area, mainly computer networks. Right now he is with Dr. Chi-Kin Chau to earn his MSc degree. His research interests are wireless networks, embedded systems and all kinds of algorithms. When he does not have much research workload, he usually takes some tea while reading books.

Maryam Al Mehrezi is a first year master student at Masdar Institute.