RSA and El-Gamal Cryptosystems

Yanan Xiao, *Student Member, IEEE* Maryam Al Mehrezi

Abstract—We present our analysis of RSA and ElGamal cryptosystem with great detail. We show that there are some attacks on RSA. The mathematical foundation of ElGamal cryptosystem, namely discrete logarithm problem is discussed. Basic structure of our implementation codes is also mentioned.

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 Cryptosystem

n nvKJASHF [1].

4.1 Background

Discrete logarithm problem will be discussed here.

4.2 Basic El-Gamal Encryption

Well, I really want to finish those stuff as soon as possible. In this way I have to abort something else.

4.3 Generalized El-Gamal Encryption

Life is so damn hard. Isn't it? Just another

4.4 El-Gamal in Digital Signature

4.5 Some Possible Attacks

5 Implementation

Implementation process will be discussed here. Let the hunt begin [2].

5.1 RSA

5.2 El-Gamal

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.

• *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: {yxiao,malmehrezi}@masdar.ac.ae

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] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[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.

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.